applied sciences

Special Issue Reprint

RFID(Radio Frequency Identification) Localization and Application

Edited by
Jia Liu

mdpi.com/journal/applsci

MDPI

RFID(Radio Frequency Identification) Localization and Application

RFID(Radio Frequency Identification) Localization and Application

Guest Editor

Jia Liu

Basel • Beijing • Wuhan • Barcelona • Belgrade • Novi Sad • Cluj • Manchester

Guest Editor
Jia Liu
Nanjing University
Nanjing
China

Editorial Office
MDPI AG
Grosspeteranlage 5
4052 Basel, Switzerland

This is a reprint of the Special Issue, published open access by the journal *Applied Sciences* (ISSN 2076-3417), freely accessible at: https://www.mdpi.com/journal/applsci/special_issues/RFID_Localization_Application.

For citation purposes, cite each article independently as indicated on the article page online and as indicated below:

Lastname, A.A.; Lastname, B.B. Article Title. *Journal Name* **Year**, *Volume Number*, Page Range.

ISBN 978-3-7258-2311-6 (Hbk)
ISBN 978-3-7258-2312-3 (PDF)
https://doi.org/10.3390/books978-3-7258-2312-3

Contents

About the Editor

Jia Liu

Dr. Jia Liu (Associate Professor) works at the Department of Computer Science and Technology at Nanjing University. His research mainly focuses on RFID technology, including protocols and systems. Dr. Liu holds 16 patents and has published 70 peer-reviewed conference/journal papers, including USENIX NSDI, ACM MOBICOM, ACM MOBISYS, ACM SIGMOD, and USENIX ATC. He has received numerous accolades, including 10 ICIM Scientific and Technological Developments, Special Gold Medal at the 46th Geneva's Invention Expo, and ACM SIGBED China Rising Star. Dr. Liu developed an RFID mobile localization system that has been widely deployed in Singapore and over 20 provinces in China.

Preface

RFID technology is transforming various sectors, from smart industries and logistics to healthcare and security. The reprint of the Special Issue on RFID Localization and Application of the journal Applied Sciences, compiles ten papers that present the latest advancements and applications in RFID research. The reprint provides a comprehensive overview of RFID technology, offering insights into its diverse applications and theoretical advancements, specifically including: supply chains and logistics, security and authentication, localization and motion capture, protocol optimization, and environmental sensing and simulation. The reprint aims to inspire further research and development by presenting cutting-edge findings and innovative solutions in RFID. The motivation for this reprint is to highlight significant strides in RFID technology. It is intended for researchers, engineers, practitioners, and students interested in exploring the latest developments and practical implementations of RFID. We extend our gratitude to the authors for their pioneering research, the reviewers for their valuable feedback, and the editorial team of Applied Sciences for their support. Special thanks are also extended to the institutions and funding agencies that supported the research.

Jia Liu
Guest Editor

applied sciences

MDPI

Editorial

RFID (Radio Frequency Identification) Localization and Application

Jia Liu

State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China; jialiu@nju.edu.cn

1. Introduction

RFID (Radio Frequency Identification) technology has witnessed widespread adoption across diverse industries and sectors due to its versatility and ability to provide real-time tracking, monitoring, and data capture [1,2]. By attaching an RFID tag to an object, the RFID reader can communicate with the tag, making tagged objects identifiable and traceable for item-level intelligence. With global tag usage exceeding 44.8 billion in 2023 [3], RFID has become the most prevalent smart terminal in the era of Internet of Things.

This Special Issue of "RFID (Radio Frequency Identification) Localization and Application" highlights significant strides and emerging trends within the dynamic field of Radio Frequency Identification (RFID) technology. The ten papers featured in this issue collectively provide a comprehensive overview of the current state of RFID research, spanning diverse applications and theoretical advancements that push the boundaries of what is possible with this transformative technology, specifically including the following:

Supply Chain and Logistics [4]: RFID's role in optimizing supply chain operations is exemplified through enhanced tracking and inventory management solutions. The digitalization of supply chains, as illustrated by its application to fresh produce, showcases RFID's potential to improve efficiency, reduce waste, and enhance traceability.

Security and Authentication [5]: Novel approaches in RFID-based security systems highlight the integration of biometric data and sophisticated protocols to ensure robust and reliable authentication. These developments are crucial for applications requiring high security, such as access control and user verification.

Localization and Motion Capture [6,7]: Advanced techniques for real-time locating systems and wireless motion capture have been explored, with applications ranging from healthcare to smart environments. Innovations in this area promise to enhance accuracy and reduce costs, making RFID an indispensable tool for precise indoor positioning and activity sensing.

Protocol Optimization [8–11]: Efficient tag identification and communication protocols are critical for maximizing the performance of RFID systems. Research in dynamic query protocols and multi-group tag searching addresses the need for faster and more reliable identification processes, especially in complex and high-density environments.

Environmental Sensing and Simulation [12,13]: The application of RFID in environmental sensing and the development of simulation models for radio signal propagation reflect the expanding scope of RFID technology. These studies provide valuable insights into optimizing RFID system design and deployment in various settings.

2. Challenges

Despite impressive advancements, several challenges and knowledge gaps persist in the field of RFID technology. These include the following:

Scalability and Interoperability: Ensuring that RFID systems can scale effectively and interoperate with other technologies remains a critical challenge. The diverse applications

Citation: Liu, J. RFID (Radio Frequency Identification) Localization and Application. *Appl. Sci.* **2024**, *14*, 5932. https://doi.org/10.3390/app14135932

Received: 26 June 2024
Accepted: 5 July 2024
Published: 8 July 2024

of RFID necessitate solutions that are flexible and adaptable to different environments and requirements.

Security and Privacy: While significant progress has been made in RFID security, ongoing research is needed to address emerging threats and enhance privacy protections. The integration of advanced cryptographic techniques and biometric data requires continuous innovation to stay ahead of potential vulnerabilities.

Cost and Complexity: Reducing the cost and complexity of RFID systems, particularly in localization and motion capture, is essential for broader adoption. Simplified solutions that maintain high performance without the need for extensive infrastructure will drive the expansion of RFID applications.

3. Future Work

Looking ahead, several areas warrant further exploration to continue advancing RFID technology:

Integration with Emerging Technologies: The convergence of RFID with IoT, AI, and machine learning holds tremendous potential. Future research should focus on how these technologies can be synergistically integrated to create smarter, more autonomous systems.

Advanced Security Measures: Ongoing research into sophisticated security protocols and privacy-enhancing techniques is crucial. As RFID technology becomes more pervasive, ensuring robust protection against unauthorized access and data breaches will be paramount.

Environmental Impact and Sustainability: Investigating the environmental impact of RFID systems and exploring sustainable practices in their design and deployment will become increasingly important. Research into eco-friendly materials and energy-efficient operations can contribute to more sustainable RFID solutions.

Application-Specific Innovations: Tailoring RFID solutions to specific industry needs, such as healthcare, retail, and smart cities, will drive further advancements. Collaborative efforts between academia and industry can foster the development of customized applications that address unique challenges and opportunities in these sectors.

4. Conclusions

In conclusion, the papers in this Special Issue reflect the vibrant and rapidly evolving landscape of RFID technology. By addressing existing gaps and exploring new frontiers, the research presented here sets the stage for future innovations that will continue to transform industries and improve societal outcomes. We look forward to seeing how these advancements will shape the future of RFID and inspire ongoing research and development in this exciting field.

Funding: This research was funded by the National Natural Science Foundation of China grant number 62072231, the Fundamental Research Funds for the Central Universities, and the Collaborative Innovation Center of Novel Software Technology and Industrialization.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chen, X.; Liu, J.; Huang, H.; Sun, Y.E.; Zhang, X.; Chen, L.J. Revisiting Cardinality Estimation in COTS RFID Systems. In Proceedings of the ACM MobiCom, 29th Annual International Conference on Mobile Computing and Networking, Madrid, Spain, 2–6 October 2023.
2. Yang, L.; Chen, Y.K.; Li, X.Y.; Xiao, C.W.; Li, M.; Liu, Y.H. Tagoram: Real-time Tracking of Mobile RFID Tags to High Precision using COTS Devices. In Proceedings of the ACM MobiCom, 20th Annual International Conference on Mobile Computing and Networking, Maui, HI, USA, 7–11 September 2014.
3. RFID Journal. Available online: https://www.rfidjournal.com/shipment-of-rain-rfid-tag-chips-surged-to-44-8-billion-in-2023 (accessed on 7 July 2024).
4. Menanno, M.; Savino, M.; Accorsi, R. Digitalization of Fresh Chestnut Fruit Supply Chain through RFID: Evidence, Benefits and Managerial Implications. *Appl. Sci.* **2023**, *13*, 5086. [CrossRef]

5. Huang, Y.; Fu, B.; Peng, N.; Ba, Y.; Liu, X.; Zhang, S. RFID Authentication System Based on User Biometric Information. *Appl. Sci.* **2022**, *12*, 12865. [CrossRef]
6. Tan, P.; Tsinakwadi, T.; Xu, Z.; Xu, H. Sing-Ant: RFID Indoor Positioning System Using Single Antenna with Multiple Beams Based on LANDMARC Algorithm. *Appl. Sci.* **2022**, *12*, 6751. [CrossRef]
7. Wang, X.; Wang, X.; Yan, Y.; Liu, J.; Zhao, Z. RF-Access: Barrier-Free Access Control Systems with UHF RFID. *Appl. Sci.* **2022**, *12*, 11592. [CrossRef]
8. Wang, X.; Tian, X.; Su, S.; Gu, R.; Hu, C.; Liu, H.; Liu, J. A Filter-Based and Parallel Unknown Tag Identification Protocol in Open RFID Systems. *Appl. Sci.* **2022**, *12*, 11349. [CrossRef]
9. Peng, J.; Zhang, L.; Fan, M.; Zhao, N.; Lei, L.; He, Q.; Xia, J. An Admission-Control-Based Dynamic Query Tree Protocol for Fast Moving RFID Tag Identification. *Appl. Sci.* **2023**, *13*, 2228. [CrossRef]
10. Yan, N.; Chen, H.; Lin, K.; Li, Z.; Liu, Y. Fast and Effective Tag Searching for Multi-Group RFID Systems. *Appl. Sci.* **2023**, *13*, 3540. [CrossRef]
11. Wang, C.; Wang, Y.; Zhang, Y.; Xu, H.; Zhang, Z. Open-Set Specific Emitter Identification Based on Prototypical Networks and Extreme Value Theory. *Appl. Sci.* **2023**, *13*, 3878. [CrossRef]
12. Straka, T.; Vojtech, L.; Neruda, M. Simulation of Radio Signal Propagation for UHF RFID Technology in an Indoor Environment Using Ray Tracing (Graphics) Method. *Appl. Sci.* **2022**, *12*, 11065. [CrossRef]
13. Ramos, V.; Suárez, O.; Suárez, S.; Febles, V.; Aguirre, E.; Zradziński, P.; Rabassa, L.; Celaya-Echarri, M.; Marina, P.; Karpowicz, J.; et al. Electromagnetic Assessment of UHF-RFID Devices in Healthcare Environment. *Appl. Sci.* **2022**, *12*, 10667. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

applied sciences

MDPI

Article

RF-Access: Barrier-Free Access Control Systems with UHF RFID

Xuan Wang [1], Xia Wang [1,2], Yingli Yan [1], Jia Liu [1,*] and Zhihong Zhao [1,3,*]

[1] State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China
[2] School of Computer Engineering, Jinling Institute of Technology, Nanjing 211100, China
[3] Suzhou City University, Suzhou 215104, China
[*] Correspondence: jialiu@nju.edu.cn (J.L.); zhaozhih@nju.edu.cn (Z.Z.)

Abstract: Traditional RFID-based access control systems use flap barriers to help manage pedestrian access and block unauthorized staff at any entrance, which requires visitors to swipe their cards individually and wait for the opening of the blocking body, resulting in low-frequency pedestrian access and even congestion in places with large passenger flow. This paper proposes a barrier-free access control system (RF-Access) with UHF RFID technology. The main advantage of RF-Access is that it provides non-intrusive access control by removing flap barriers and operations of swiping the card. The visitors just go across the system without any stay at the entrance. Meanwhile RF-Access performs the authentication, which greatly improves time efficiency and quality of service. RF-Access addresses two key issues of the non-intrusive access control: motion direction detection and illegal intrusion detection. In RF-Access, we first propose a dual-antenna system setup together with a time-slot-based model to monitor users' moving directions, which is robust to different environmental factors, such as multi-path effects. Afterwards, we use a tag array to detect illegal intrusion in case attackers do not carry any RFID tags. We implement a prototype of RF-Access with commercial RFID devices. Extensive experiments show that our system can detect the moving direction with 99.83% accuracy and detect illegal intrusion with an accuracy of 96.67%.

Keywords: RFID; access control; mobile sensing

Citation: Wang, X.; Wang, X.; Yan, Y.; Liu, J.; Zhao, Z. RF-Access: Barrier-Free Access Control Systems with UHF RFID. *Appl. Sci.* **2022**, *12*, 11592. https://doi.org/10.3390/app122211592

Academic Editors: Junseop Lee and Subhas Mukhopadhyay

Received: 12 October 2022
Accepted: 11 November 2022
Published: 15 November 2022

1. Introduction

Radio Frequency IDentification (RFID) has been widely used in a variety of applications, such as supply chain management [1,2], warehouse inventory [3,4], objects monitoring and tracking [5,6]. RFID-based access control is one of these applications, which aims to help manage pedestrian access and block unauthorized staff at any entrance. The existing RFID-based access control systems consist of a high-frequency (HF) RFID reader and a blocking body, e.g., flap barriers, which require visitors to swipe their identity cards individually and wait for the opening of the blocking body, resulting in low-frequency pedestrian access and even congestion in places with large passenger flow.

In this paper, we propose a barrier-free access control system (RF-Access) with UHF RFID technology. Compared with HF RFID, UHF RFID has a longer communication range and a higher reading rate, which makes it possible to remove the process of swiping the identity card. In addition, we remove flap barriers from the system, which provides non-intrusive access control: the visitors just go across the system without any stay at the entrance, and meanwhile RF-Access performs the user authentication, which greatly improves time efficiency and quality of service. To achieve this goal, RF-Access needs to address two key challenges: motion direction detection and illegal intrusion detection. In RF-Access, we firstly propose a dual-antenna system setup together with a time-slot-based model to monitor users' moving directions, which is robust to different environmental factors such as multi-path effects. Afterward, we use a tag array to detect illegal intrusion in case attackers do not carry any RFID tags. Experimental results show that the proposed system has good performance. The main contributions of this paper are three-fold.

- We propose a novel barrier-free access control system (RF-Access) with UHF RFID technology. The main advantage of RF-Access is that it provides non-intrusive access control by removing flap barriers and operations of swiping the card, which greatly improves time efficiency and quality of service.
- RF-Access addresses two key issues of non-intrusive access control: motion direction detection and illegal intrusion detection, by using a dual-antenna tag-array system setup together with a time-slot-based model to monitor users' moving directions.
- We implement a prototype of RF-Access with commercial RFID devices. Extensive experiments show that our system can detect the moving direction with 99.83% accuracy and detect illegal intrusion with an accuracy of 96.67%.

The rest of the paper is organized as follows. Section 2 introduces the related work. Section 3 details our access control system RF-Access. Section 4 implements the system and evaluates its performance. Finally, Section 5 concludes this paper.

2. Related Work

Access control systems need to install flap barriers to help manage pedestrian access and block unauthorized staff at any entrance, which can function properly but require visitors to wait for the opening of the blocking body, leading to low-frequency pedestrian access and even congestion in places with large passenger flow. In recent years, studies have shifted to barrier-free access control. TDflex [7] designed a customized sensor to detect tailgating intrusion. Specifically, TDflex uses a non-scanning light source to emit modulated near-infrared light and generate real-time three-dimensional images of the monitoring area by measuring the difference between the lights emitted by the light source and the detection target. Computer vision is another technology for barrier-free access control. For example, HIKVISION [8] produces a binocular intelligent network camera, which is deployed directly above the monitoring area. It adopts binocular stereo vision technology to obtain height information of objects and an intelligent tracking algorithm to analyze the users' behavior trajectory, counting the number of users and detecting access directions. However, vision-based sensing suffers from the impact of environmental factors, including low illumination and non-line-of-sight (the target is blocked by others). Additionally, these solutions cannot figure out the user identity accurately.

In comparison to the above sensing technologies, RFID offers an appealing alternative, with the advantages of unique identification, non-line-of-sight communication, and high reading rates, which makes it the most widely used in the field of access control [9,10]. In recent years, some RFID studies have shifted to study barrier-free access control. Mai et al. [11] deploy a group of infrared intrusion detectors to detect the user's pass in and out, which, however, allows only a single-channel pass at a time. Wang [12] and Fan [13] deploy two sets of infrared switches on both sides of the gates to detect the directions of users but cannot detect an illegal user amongst legal users. He et al. [14] demand the time interval between the illegal pass and the tag last seen to be greater than 3 s, which is too ideal for practical use. Additionally, the existing solutions all use the HF RFID as the authentication approach, which suffers from a short communication range. Namely, each user needs to stop at the entrance to swipe his/her identity card for authentication, which still has the problem of low-frequency pedestrian access. There are a few commercial RFID readers (antennas) that provide us with the function of moving direction estimation, e.g., Impinj xSpan [15]. They use an antenna-array design to perform beamforming, which is able to dynamically scan the moving tags but suffers from the limitations of the large device size and the high system cost. For example, an Impinj xSpan reader costs nearly nearly 3000 [16], which is much higher than the retail price of an RFID-based access control system. Instead, our design uses the existing RFID reader and antennas embedded in the existing access control system, with no need for any extra hardware augmentation.

3. RF-Access

3.1. Overview

RF-Access uses the UHF RFID to perform user authentication. As shown in Figure 1, an RFID reader connects to one or more RFID antennas that locate on one side of the passageway. The user authentication is achieved by querying RFID tags attached to visitors who pass through the gate. If a tag is queried, the reader compares its EPC (tag's ID) with legal IDs stored in the backend server. Only the user with a legal RFID tag (or a tagged badge) will pass the system authentication. Since UHF RFID has a long communication range and a high reading rate, RF-Access does not demand users stop to swipe their identity cards as HF RFID. Instead, the visitors just go through the system without any stay, and meanwhile, RF-Access does the user authentication, which greatly improves time efficiency and quality of service. However, the long communication range makes the motion direction detection difficult. Additionally, since we remove the flap barriers, how we detect illegal intrusion by a user who does not carry any tags is another concern. In what follows, we detail how RF-Access addresses these two issues.

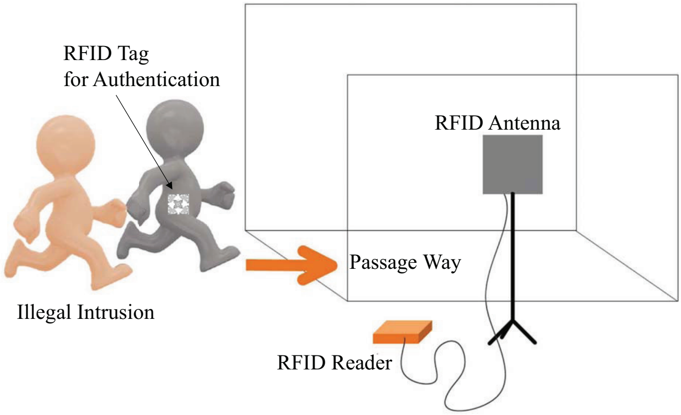


Figure 1. System overview.

3.2. Motion Direction Detection

A barrier-free access control system needs to detect the motion direction (in or out) of each visitor in the passageway. In RF-Access, we first present a signal-based solution and later offer a more robust time-lost model.

3.2.1. Signal-Based Sensing

As shown in Figure 2, as a visitor passes through the access control system (the trajectory can be approximatively treated as a line), the distance between the reader (omnidirectional) antenna and the tag first experiences a decline. After reaching the minimum, the distance increases as the person (tag) moves. If we can observe the distance variances over time, we can use two antennas A and B along the moving direction to check which one reaches the minimal distance first. If A is earlier than B, the motion direction of the tag is from A to B. Otherwise, the direction is B to A. The parameters of RF signals can reflect the distance, such as Received Signal Strength Indicator (RSSI) and the phase value. In the following, we take RSSI as an example to show this solution.

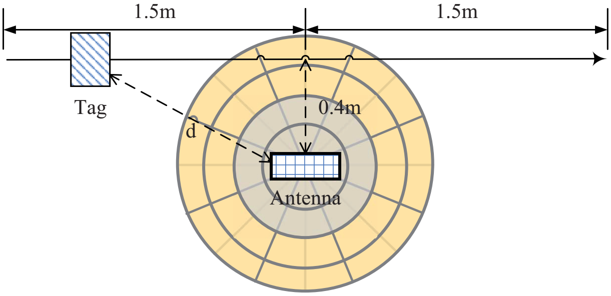


Figure 2. The changes of tag-to-reader distance when a tag moves linearly (omnidirectional antenna in this case).

In an RFID system, RSSI represents the strength of a tag's signals received by the reader. More specifically, a large RSSI value means the power of the tag's response signal is strong and is more likely to be close to the reader. In theory, Friis is a widely used model that reflects the distance between the transmitter and receiver in free space. According to the Friis equation, the power of a tag's response signal can be written as follows [17]:

$$P_R = \frac{P_T G_{TR}^2 G_t^2 \lambda^4 X^2 M}{(4\pi r)^4 \Theta^2 B^2 F_2}, \tag{1}$$

where P_R is the power coupled into the radio-frequency integrated circuit, P_T is the power transmitted by the reader, G_{TR} is the load-matched, free-space gain of the transmitter/receiver antenna (i.e., the reader antenna), G_t is the load-matched, free-space gain of the tag antenna, λ is the carrier-frequency wavelength, X is the polarization mismatch, M is a modulation factor, r is the reader-to-tag separation distance, Θ is the RF tag antenna's on-object gain penalty, B is the path-blockage loss, and F_2 is the monostatic fade margin. RSSI is a logarithmic form of P_R, which can be derived by the following function:

$$RSSI = 10 \times lg(P_R). \tag{2}$$

According to Equations (1) and (2), we can easily conclude that given a reader and a tag, the longer the distance between them, the smaller the RSSI is. As aforementioned, when the tag moves along the x-axis, the distance between the reader antenna and the tag declines first and then increases. Namely, RSSI experiences a contrary change trend. In Figure 3, we plot the theoretical RSSI value when a tag moves along the x-axis ([−1.5 m, 1.5 m]), given the closest distance of 0.4 m. It is clear that RSSI sees a rising trend and after peaking at the maximum, it gradually drops. The peak corresponds to the time when the tag–antenna distance reaches the minimum.

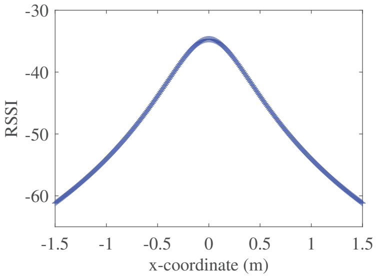


Figure 3. The theoretical RSSI value when a tag moves along the x-axis.

We verify the above theoretical model with a real-world experiment in an open space. As shown in Figure 4, a tag is fixed to a sliding rail and moves at a constant speed of 10 cm/s. Two RFID antennas are 80 cm in height and 40 cm apart from each other. As the tag moves along the sliding rail, we keep measuring the RSSI value of the RF signals backscattered by the tag. The experimental results are shown in Figure 5. It is clear that the RSSI curve generally follows the theoretical model, and two peaks corresponding to two antennas can easily figure out moving in or out—which peaks first means the direction is from this one to the other.

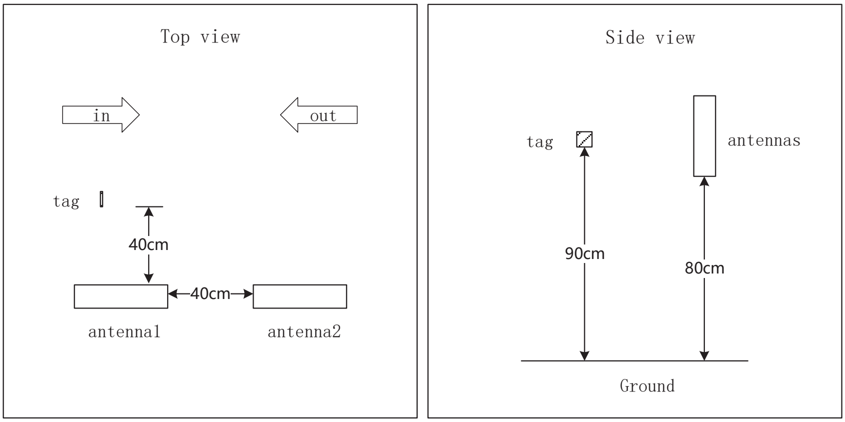


Figure 4. System deployment for the RSSI-based model.

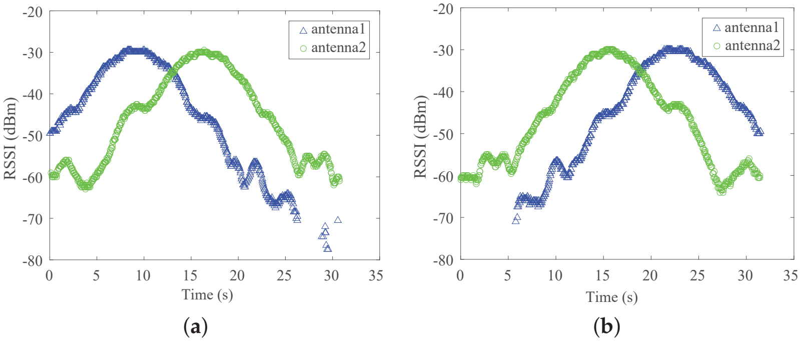


Figure 5. RSSI values with respect to the time; (**a**) moving in; (**b**) moving out.

However, the peak cannot be directly determined by the maximal RSSI value due to thermal noise, which is very likely to give rise to false positives. Instead, we try to fit this RSSI curve and find out the time corresponding to the peak for each antenna.

Given a tag, we collect n responses by the mth antenna and build a tag response matrix following the timestamp order, which is described as: $D^m = \left(D_1^m\ D_2^m\ \cdots\ D_n^m\right)^T$, where D_i^m is a tag's RSSI record, which is actually a triple $D_i^m = \left(e, r_i^m, t_i^m\right)$, where e is EPC (tag ID), r_i^m, t_i^m are the measured RSSI value and corresponding timestamp obtained by the m-th antenna. So, the response matrix of the m-th antenna can be written as follows:

$$D^m = (D_1^m\ D_2^m\ \cdots\ D_n^m)^T = \begin{pmatrix} e & r_1^m & t_1^m \\ e & r_2^m & t_2^m \\ \vdots & \vdots & \vdots \\ e & r_n^m & t_n^m \end{pmatrix} = (E, R^m, T^m), \tag{3}$$

where the timestamp meets $t_i^m \le t_j^m$ $(0 < i < j \le n)$, E is the broadcast of e, R^m is the vector of RSSI values measured by the m-th antenna, and T^m is the vector of timestamps corresponding to R^m. The changing trend of the RSSI curve is approximate to the parabola with the opening downward. We fit the RSSI and timestamp in the response signals of two antennas with a quadratic curve, respectively. Let the second-order coefficient and the first-order coefficient in the fitting results be a and b; the time t_{peak} corresponding to the peak is:

$$t_{peak} = -\frac{b}{2a}. \tag{4}$$

By comparing the time of the two antenna's peaks, we can determine the motion direction.

The signal-based model functions properly in an ideal scenario with modest multipath effects and slow speed. However, in a real indoor scenario, this model is not robust to more general scenarios. In Figure 6, we let a volunteer carrying a tag walk through the system and use the signal-based model to detect the direction. As we can see, since the human body blocks the tag, almost all the tag signals in the second half are absorbed, resulting in the incomplete image of the RSSI, which further affects the detection accuracy. According to the fitting results, we will obtain a wrong result of the direction. The main reason is that RF signals are vulnerable to environmental changes, which motivates us to seek a more robust way.

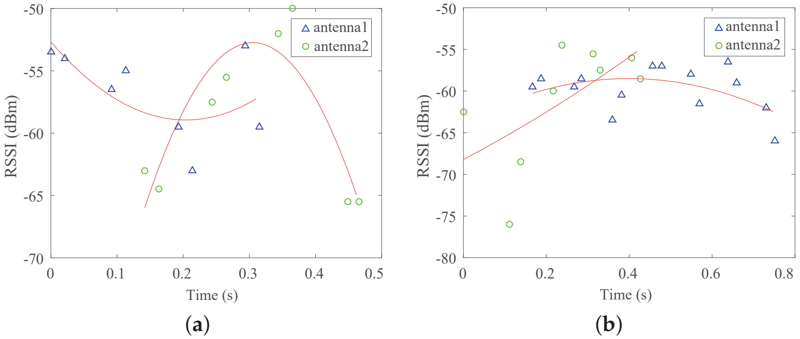


Figure 6. RSSI values collected from a running tagged person: (**a**) moving in; (**b**) moving out.

3.2.2. Time-Slot-Based Sensing

Instead of using RF signals, we attempt to use the application-layer feature—reading records, which are stable and robust to environmental factors. The principle is that when the tag moves from left to right, the left-side antenna is supposed to query the tag earlier than the right-side antenna and vice versa. By observing the timestamps of the reading records of two antennas, it is promising to figure out the moving direction.

An intuitive solution is to check the first seen time by each antenna. This works in theory but is not robust in real scenarios due to the multi-path effects and the blocking impact of the human body. To address this problem, we resort to all reading records. The solution is to split the reading period into many smaller time slots. For each antenna, we check whether there are some reading records within each time slot. If yes, we consider that this antenna hits the time slot, and the time slot is labeled as a busy slot. The mean of all busy slots is treated as the final reading time of an antenna. By comparing the mean of different antennas, we can figure out the direction.

More specifically, for the m-th antenna, we obtain the time-stamp sequence of the reading records $T^m = \left(t_1^m \; t_2^m \; \cdots \; t_n^m\right)$. The time period is:

$$T_s = [\min(T^m), max(T^m)]. \tag{5}$$

The time period T_s can be divided into w small time slots with the length of δ, i.e.,

$$w = \lceil \frac{\max(T^m) - \min(T^m)}{\delta} \rceil \tag{6}$$

The middle x_i of the ith time slot is:

$$x_i = \min(T^m) + (i - \frac{1}{2})\delta. \tag{7}$$

Let the bit vector $B = \{b_1, b_2, ..., b_n\}$ indicate whether each slot is busy. If b_i is equal to 1, the ith slot is busy. Otherwise, the ith slot is idle. We can obtain the mean $\bar{t}^m$ of reading time of the m-th antenna:

$$\bar{t}^m = \frac{1}{\sum(B)} \sum_{i=1}^{n} x_i \times b_i. \tag{8}$$

For two antennas A and B, if $\bar{t}^A < \bar{t}^B$, we know that the moving direction is from A to B and vice versa.

Figure 7 shows the RSSI values when a user moves out with a tag at a constant speed. If the signal-based solution is used, we obtain a wrong answer in this case. For the time slot-based solution, we can obtain $\bar{t}^1$ = 1.78 s and $\bar{t}^2$ = 1.61 s, which means that $\bar{t}^1 > \bar{t}^2$ and further verifies that the moving direction is from antenna 2 to antenna 1, i.e., moving out, where the symbols '$*$' and '$\times$' in Figure 7 indicate that the tag is queried within a time slot by antenna1 and antenna2, respectively.

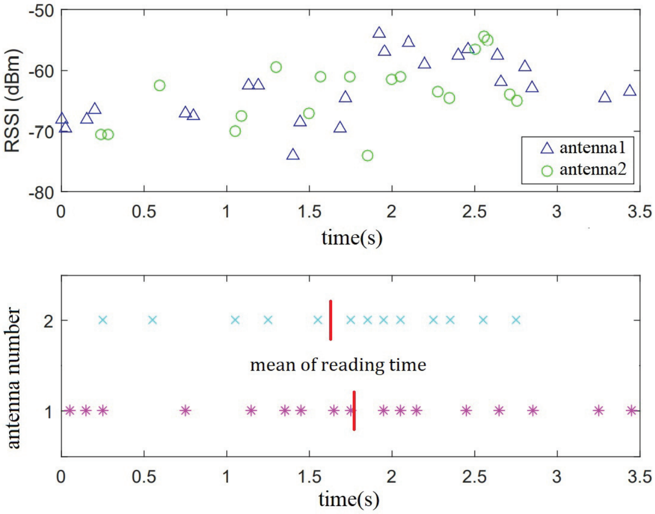


Figure 7. An illustration of time-slot-based detection.

3.3. Tag-Array Based Intrusion Detection

In addition to motion direction detection, intrusion detection is another fundamental function of access control. Illegal intrusion generally falls into two categories: independent intrusion and tailgating intrusion. The former means the attacker individually goes through the access control system, and the latter indicates the attacker closely follows the legal users in the passageway. Since the attacker does not carry any RFID tags, the reader cannot obtain anything from the attacker directly for intrusion detection. RF-Access boils down the issue to a counting-people problem. The idea is to estimate the number of people in the passageway and compare it with that of legal tags queried by the reader. If these two numbers are different, an intrusion event has happened. It is worth noting that if an intruder is detected, the access control system can raise a warning alarm and push this abnormal information to the security guard. The follow-up procedure is application-defined, which is out of the scope of this work.

Since a smart intruder must not carry any tags, we need to design a device-free way to count the number of people. If the intruder carries one or more illegal tags, we can easily figure out the intrusion by reading these tags. In RF-Access, we use a tag array to perform people counting. As shown in Figure 8, we deploy one or more RFID antennas on one side of the passageway and a tag array on the other side. Since the RF signals are vulnerable to the human body, we can take advantage of this inference as the vehicle to people count.

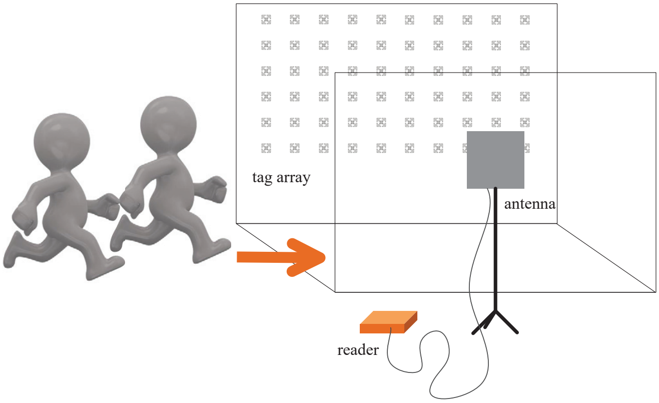
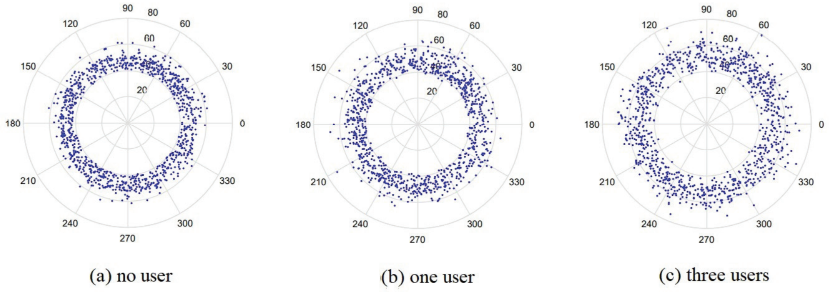


Figure 8. Tag-array-based intrusion detection.

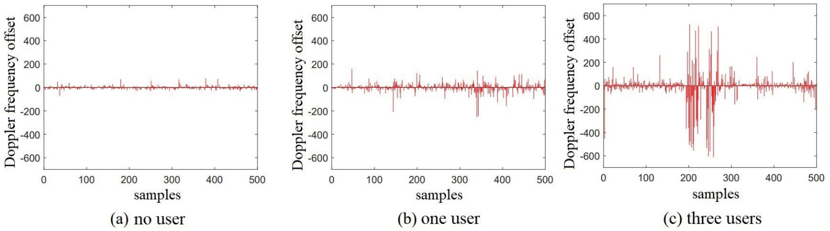
We use a group of experiments to validate this idea. We invite three volunteers to walk through the passageway. To mimic a real attack, we ask for the volunteers to try to be close to each other. Meanwhile, the reader keeps collecting the backscattered signals from all tags. Two parameters are measured, including RSSI and Doppler frequency offset. As shown in Figure 9, 1000 RSSI values obtained from a 6 × 10 tag array are plotted in a polar coordinate system in a random direction, where the radius of each point represents the real RSSI value. We can learn from this figure: (1) When no one walks by, the RSSI distribution forms a thin circle, which indicates that RSSI signals remain relatively stable. (2) RSSI values start to spread out as the number of users increases. The above results demonstrate that there is a potential to use the RSSI distribution to estimate the number of people.

Similarly, we test the Doppler shifts of all tags under different numbers of people. In Figure 10, we randomly select and plot 500 Doppler frequency offset values. Ideally, the Doppler frequency offset should be close to zero when the tag and antenna keep stationary and the Doppler frequency offset increases as the tag moves toward the antenna. However, due to the noise, the Doppler frequency offsets reported by the commercial RFID reader level off at 0 with positive values and negative values, which are shown in Figure 10a. Similar to RSSI, the Doppler frequency offsets become more and more dispersed as the number of people increases.



(a) no user (b) one user (c) three users

Figure 9. Impact of the number of users on RSSI.



(a) no user (b) one user (c) three users

Figure 10. Impact of the number of users on Doppler frequency offsets.

With the signal features, we can treat the counting problem as a classification problem using machine learning. More specifically, we view RSSI as a random variable and use the entropy of RSSI to measure how the RSSI data spread. Assume that the minimum value of RSSI in all samples is r_{min}, and the maximum value is r_{max}. The value domain of RSSI is the interval $[r_{min}, r_{max}]$. Afterward, we divide the interval into N bins with the size Δ of each:

$$N = \lceil \frac{r_{max} - r_{min}}{\Delta} \rceil. \tag{9}$$

Let m_i be the number of RSSI values falling into the ith bin. The probability p_i of an RSSI falling into the ith bin is:

$$p_i = \frac{m_i}{\sum_{i=1}^{N} m_i}. \tag{10}$$

The RSSI entropy in unit time can be calculated as follows:

$$H_R = E[log_b p(M)] = -\sum_{i=1}^{N} p_i \cdot log_b(p_i), \tag{11}$$

where b is the base of logarithm, which is set to two, making the unit of entropy to be *bit*. Thus, the RSSI entropy f_R of the sample is:

$$f_R = H_R/\Gamma, \tag{12}$$

where Γ is the time interval between the first sampling and the last one. For Doppler frequency offsets, we can use the similar method to calculate its entropy.

In addition to the above signal-level features, we observe that the application layer parameters, such as the reading rates, can also be used to conduct counting. With these features, we use the random forest algorithm [18] as the machine learning classifier to conduct counting due to its good classification results on small data sets. We adjust the parameters of the classifier to optimize the estimation accuracy and use the "cross validation method" to evaluate the model. Specifically, the data set is randomly divided into k mutually exclusive subsets with the similar size. We then utilize one subset as the test set and the remaining $k-1$ subsets as the training sets to obtain k groups of training/test sets. We finally obtain k mean values of classification accuracy through carrying out k training and classification tests. Here, we adopt "10-fold cross-validation" with k being 10.

It is worth noting that there are some good solutions to the problem of people counting, such as computer vision [8] and radar [19]. We could choose one of them to conduct people counting and use RFID to identity authentication and estimate moving direction. However, in a barrier-free access control system, this increases the deployment overhead and hardware cost for practical use. Instead, our solution is to use an existing RFID device together with a tag matrix (less than nearly 10) to achieve the same task, which might not be the best choice for people counting alone but is a good solution to the existing access control system.

3.4. Put Things Together

So far, we have discussed motion direction detection and intrusion detection, respectively. Now, we need to put them together to form our access control system RF-Access. As shown in Figure 11, three antennas are installed on one side of the passageway. The two antennas (#1 and #2) are used for moving direction detection. We let antenna #1 slightly face the 'in' direction and antenna #2 face the 'out' direction, which helps the slot-based solution better identify the moving direction. Additionally, the third antenna #3 is used to keep reading the tag array on the other side of the passageway for intrusion detection. These two parts work together to achieve non-intrusive access control without any stay or flap barriers, which greatly improves the passing speed and quality of service.

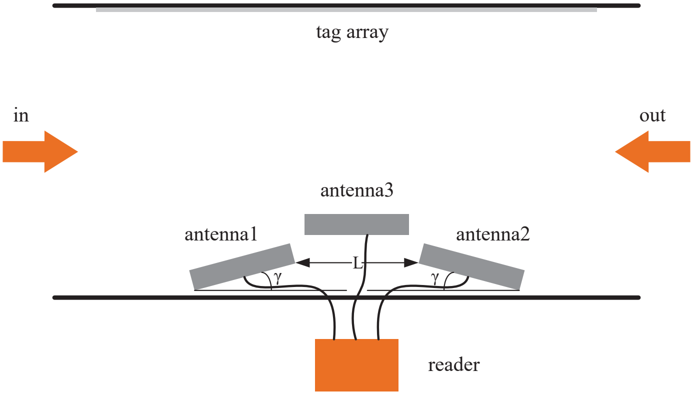


Figure 11. Top view of RF-Access deployment

4. Evaluation

In this section, we implement a prototype of RF-Access and evaluate its performance in terms of motion direction detection and intrusion detection.

4.1. Implementation

Hardware setup. RF-Access uses an enterprise-level commercial reader, Impinj Speedway R420, which has four antenna ports and a high tag reading rate with hundreds of tags per second. The antenna is Laird S9028PCL [20], which is a circularly polarized directional panel antenna and can receive and transmit signals within the 902–928 MHz frequency band. The antenna gain is 9 dBiC, and the beam width corresponding to 3 dB is 70 degrees. A Laird S9028PCL antenna can concentrate energy in the access control passageway for radiation with the far radiation distance.

System deployment. As shown in Figure 12, RF-Access deploys an RFID reader with three antennas and an RFID tag array at a two-way single passageway access control with a width of 80 cm. One reader works at 32.5 dBm power and 924.375 MHz frequency. Two antennas (antenna #1 and antenna #2) are deployed on one side of the passageway with an interval of 40 cm and an incline of 20 degrees to both ends of the passageway, respectively. The third antenna #3 is deployed between the two antennas, facing the other side of the passageway for intrusion detection. A 6×10 tag array is deployed on the other side of the passageway. RF-Access uses Impinj H47 RFID tags with a size of 44 mm × 44 mm. The distance between two adjacent tags is 10 cm. The height of the tags is from 0.4 m to 1.15 m. Antenna #3 faces the center of the tag array, which is 80 cm away from the ground. The antenna continuously records the signal changes from all tags in the array. The passageway is about 1.5 m long.

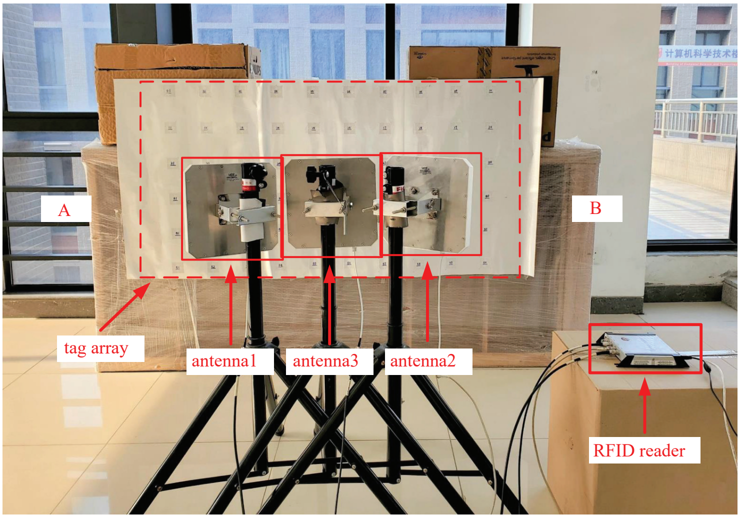


Figure 12. System deployment of RF-Access.

4.2. Detection of Motion Direction

4.2.1. Experimental Methods

We invite some volunteers to conduct experiments in a general indoor environment for evaluating the performance of our system. Volunteers carry Impinj H47 RFID tags that reflect their identities at different locations and then execute traffic movements at different speeds with a 40 cm distance from the antenna, simulating movement in an 80 cm wide access control passageway. As shown in Figure 13, five tags are placed on the chest, left arm, right arm, left pocket, and right pocket, respectively. Three movement speeds including 1 m/s, 1.5 m/s and 2 m/s are adopted, which mimics three situations: constant speed passing, fast passing and running passing, respectively. Passage behaviors are further divided into two categories: (1) “moving in” behavior: from A to B; (2) “moving out” behavior: from B to A. The volunteers execute each behavior 20 times by carrying the tags at the same locations.

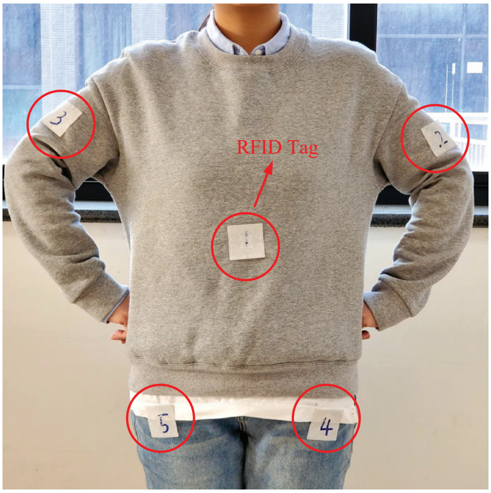


Figure 13. Tag positions.

First, we study the performance of the moving direction. Figures 14 and 15 show the detection accuracy of the signal-based model and the slot-based model under different tag positions and different moving speeds. For the signal-based sensing model, the motion direction (in or out) has a small impact on sensing accuracy, but the moving speed has a great impact on the detection accuracy. The detection accuracy generally decreases as the moving speed increases. This is consistent with our intuition that high speeds reduce the collected data, which makes the signal-based analysis hard, leading to relatively low accuracy. Additionally, even when the speed is the same, the accuracy of different tags is different. For example, the right arm's tag has less than 70% accuracy as the tag moves out. The reason is that the human body blocks the line-of-sight signals, and the reflected signals caused by multi-path will give rise to estimation errors of the distance. This indicates that the signal-based solution can function properly in a relatively ideal scenario but easily suffers from environmental changes.

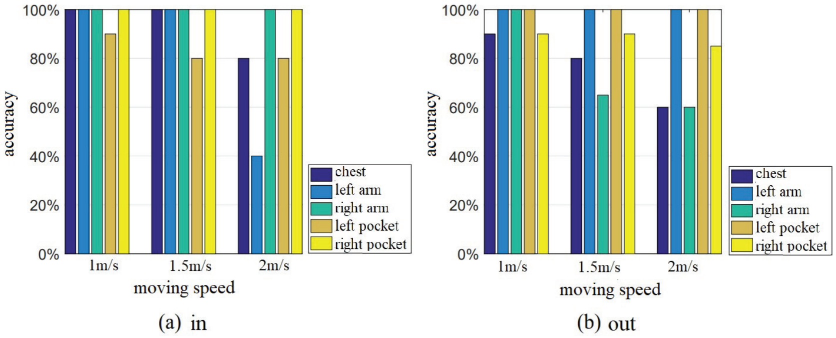


Figure 14. Detection accuracy of signal-based sensing model.

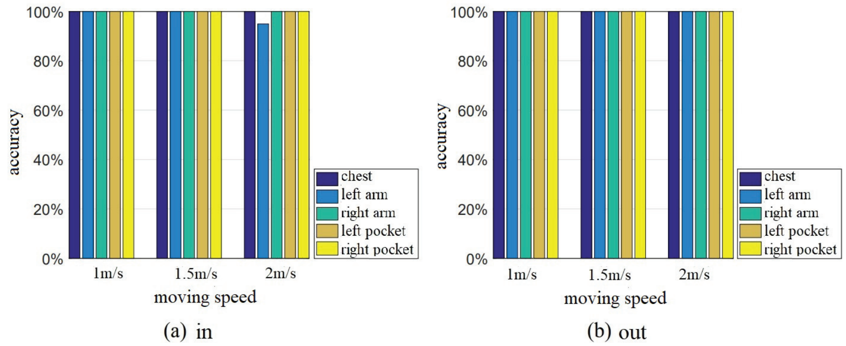


Figure 15. Detection accuracy of time-slot-based sensing model.

Compared with the signal-based solution, the time slot-based model has much better performance. As shown in Figure 15, the accuracy almost remains stable at a high level, regardless of the tag's position, moving direction, and moving speeds. This well validates the good robustness of the slot-based solution. The reason is that we use the reading records rather than signals to detect the direction, which has only two states in a time slot, making it robust to different environmental factors. Next, we study the impact of other factors on accuracy. The following experiments were carried out based on the time-slot-based sensing model.

4.2.2. Impact of Antenna Angle

In Figure 16a, we study the impact of antenna angle on sensing performance. We adjust the antenna angle γ from 0° to 40° with the step of 10° and repeat the experiments 50 times at each angle, with half of the constant speed and half of the running speed. As we can see, the accuracy is close to 100% when the angle is no less than 10°. The case of $\gamma = 0°$ sees a slight decline. The reason is that the inclined angle helps two antennas better read tags along their facing directions, which benefits direction detection. When the angle is 0, the difference between the two antennas comes from only that of antenna positions, which is too small to properly identify all cases. However, large inclined angles make it hard to deploy the antennas in a gate. We recommend 20° in this case.

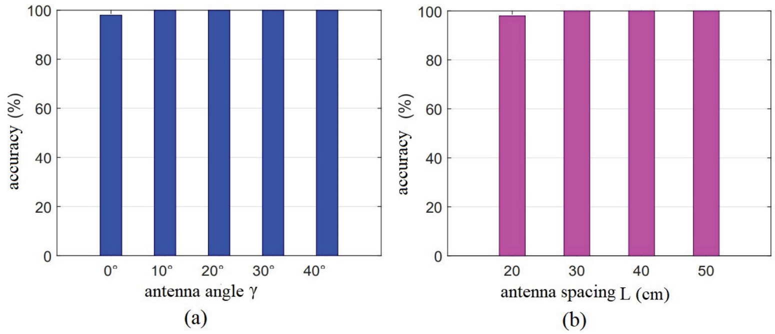


Figure 16. Detection accuracy with different antenna angle and distance.

4.2.3. Impact of Antenna Distance

In Figure 16b, we evaluate the impact of the antenna spacing distance on the detection accuracy. We change the antenna spacing distance L from 20 cm to 50 cm with the step 10 cm and conduct the experiments 50 times for obtaining the average results. As we can see, the accuracy is close to 100% when the distance is no less than 30 cm. The case of $L = 20$ cm sees a slight decline. The reason is that a large distance helps two antennas better distinguish moving in and moving out (different directions) from the time domain. We suggest that the distance be set to 30 cm or larger in practical use.

4.2.4. Impact of Different Users

In this study, we investigate the impact of different users on the accuracy of RF-Access. Eight volunteers (five males and three females) were invited to participate in the experiments. Their heights ranged from 155 cm to 185 cm and their weights varied from 45 kg to 80 kg. Each volunteer randomly placed the tag at one of the five positions and passed through the passageway. As shown in Figure 17a, the system can maintain high detection accuracy of active moving directions for different volunteers. Similarly, we can verify that the detection accuracy remains stable when multiple people pass in parallel, as shown in Figure 17b. The results demonstrate that RF-Access can obtain accurate and stable access direction detection results for different visitors.

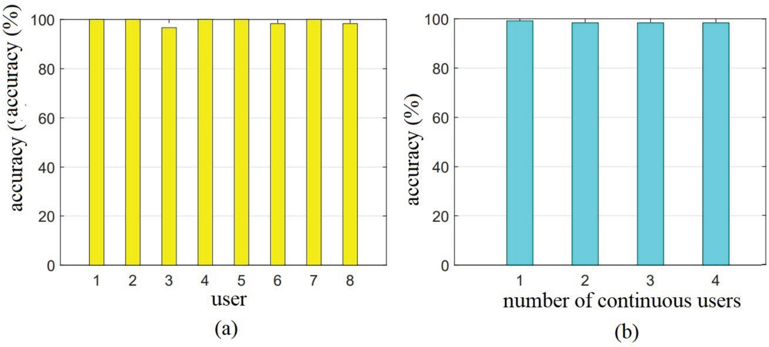


Figure 17. Detection accuracy for the visitors with different shapes and behaviors.

4.3. Intrusion Detection

4.3.1. Experimental Methods

Next, we study the accuracy of intrusion detection of our tag-array-based sensing model. We let volunteers follow each other and pass through the access control passageway. Meanwhile, the antennas keep collecting the signal changes of the tag array. We label the data and use these data as training samples with uniform distribution. As shown in Table 1, we invited the different volunteers to conduct the experiments 50 times under each scenario. For the single intrusion detection, we let up to three volunteers (without carrying any tags) pass the access control and calculate the average output of 50 experiments.

Table 1. Experimental setup of tailgating intrusion detection.

Number	Visitor Quantity	Legal Visitor Quantity	Illegal Visitor Quantity
1	1	1	0
2	2	2	0
3	2	1	1
4	3	3	0
5	3	2	1
6	3	1	2

4.3.2. Detection Accuracy

Table 2 shows the confusion matrix for the classification of 1–3 visitors in the experiment. Each row and each column in the table represent the real and estimated number of the moving visitors, respectively. Each element in the matrix represents the percentage correctly estimated. As shown in Table 2, the average recall rate of the classification is 96.10%, and its standard deviation is 0.016. The cases of 1–3 visitors are not wrongly judged as zero, and the recall rates of three categories are higher than 95% for people counting. The overall accuracy is 95.67%. Specifically, if the estimated number is greater than the real one, it is considered that illegal visitors exist in the access control system. The false alarm rate in the experiment is 1.33%. On the contrary, if the estimated number is less than the real value, there exists a possibility of missing the illegal intrusion, and the rate in the experiments is 0.03%. Both the false alarm rate and the omission rate are low. In a single intrusion detection, the accuracy rate is as high as 99.9%. Based on the above experiments of single intrusion detection and tailgating intrusion detection, we can obtain that the accuracy of RF-Access for illegal intrusion detection is 96.67%.

Table 2. Confusion matrix of people counting.

True Value	**Estimated Value**			
	0 Visitor	**1 Visitor**	**2 Visitors**	**3 Visitors**
0 visitor	1	0	0	0
1 visitor	0	0.98	0.02	0
2 visitors	0	0.02	0.95	0.03
3 visitors	0	0.007	0.04	0.953

5. Conclusions

In this paper, we propose a novel barrier-free access control system called RF-Access with UHF RFID technology. The main advantage of RF-Access is that it provides non-intrusive access control by removing flap barriers and processes of swiping the identity card, which greatly improves time efficiency and quality of service. RF-Access addresses two key issues of non-intrusive access control: motion direction detection and illegal intrusion detection by using a dual-antenna tag-array together with a time-slot based model. We implement a prototype of RF-Access with commercial RFID devices. Extensive experimental results show that our proposed system has good performance.

Author Contributions: Conceptualization, X.W. (Xuan Wang), Y.Y. and J.L.; methodology, X.W. (Xuan Wang) and J.L.; software, X.W. (Xia Wang) and Y.Y.; validation, X.W. (Xuan Wang) and Y.Y.; writing—original draft preparation, Y.Y., X.W. (Xuan Wang), and X.W. (Xia Wang); writing—review and editing, X.W. (Xia Wang) and J.L.; supervision, J.L. and Z.Z.; funding acquisition, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: The National Natural Science Foundation of China under Grant 62072231, the Open Project of State Key Laboratory for Novel Software Technology under Grant KFKT2021B15, and the Collaborative Innovation Center of Novel Software Technology and Industrialization.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Choi, T.M. Coordination and Risk Analysis of VMI Supply Chains With RFID Technology. *IEEE Trans. Ind. Inform.* **2011**, *7*, 497–504. [CrossRef]
2. Chen, X.; Liu, J.; Wang, X.; Liu, H.; Jiang, D.; Chen, L. Eingerprint: Robust Energy-related Fingerprinting for Passive RFID Tags. In Proceedings of the USENIX NSDI, Santa Clara, CA, USA, 25–27 February 2020; pp. 1101–1113.
3. Fyhn, K.; Jacobsen, R.M.; Popovski, P.; Larsen, T. Fast Capture-Recapture Approach for Mitigating the Problem of Missing RFID Tags. *IEEE Trans. Mob. Comput.* **2012**, *11*, 518–528. [CrossRef]

4. Liu, J.; Zhu, F.; Wang, Y.; Wang, X.; Pan, Q.; Chen, L. RF-scanner: Shelf scanning with robot-assisted RFID systems. In Proceedings of the IEEE INFOCOM, Atlanta, GA, USA, 1–4 May 2017; pp. 1–9.
5. Shangguan, L.; Zhou, Z.; Zheng, X.; Yang, L.; Liu, Y.; Han, J. ShopMiner: Mining Customer Shopping Behavior in Physical Clothing Stores with COTS RFID Devices. In Proceedings of the ACM SenSys, Seoul, Korea, 1–4 November 2015; pp. 113–126.
6. Liu, J.; Chen, S.; Chen, M.; Xiao, Q.; Chen, L. Pose Sensing with a Single RFID Tag. *IEEE/ACM Trans. Netw.* **2020**, *28*, 2023–2036. [CrossRef]
7. IEE: A Sense for Innovation. Available online: https://iee-sensing.com (accessed on 11 October 2022).
8. Xu, X. Application and Innovation of Eight Integrated Technologies of Intelligent Access Card System. *China Secur. Prot.* **2014**, *8*, 52–54.
9. Yang, L.; Chen, Y.; Li, X.Y.; Xiao, C.; Li, M.; Liu, Y. Tagoram: Real-time tracking of mobile RFID tags to high precision using COTS devices. In Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, Maui Hawaii USA, 7–11 September 2014; pp. 237–248.
10. Stefaniak, P.; Jachnik, B.; Koperska, W.; Skoczylas, A. Localization of LHD Machines in Underground Conditions Using IMU Sensors and DTW Algorithm. *Appl. Sci.* **2021**, *11*, 6751. [CrossRef]
11. Mai, A.; Wei, Z.; Gao, M. An access control and positioning security management system based on RFID. In Proceedings of the 7th International Conference on Intelligent Human-Machine Systems and Cybernetics, Hangzhou, China, 26–27 August 2015; Volume 2, pp. 537–540.
12. Wang, Y. Open Trouble-Free Guard Management System Based on RFID Technology. Master's Thesis, Ocean University of China, Qingdao, China, 2008.
13. Fan, J. Research and Design of Student Apartments Barrier-Free Access Management System Based on RFID Technology. Master's Thesis, Harbin Engineering University, Harbin, China, 2015.
14. He, S.P.; Li, A.G.; Zhang, X. Design of Removable Intelligenct Barrier-free Access Control System Based on Mobile Technique. *Meas. Control Technol.* **2017**, *36*, 72–75.
15. Impinj Inc. Available online: http://www.impinj.com (accessed on 11 October 2022).
16. atlasRFIDstore. Available online: https://www.atlasrfidstore.com/impinj-xspan-gateway-rfid-reader (accessed on 11 October 2022).
17. Griffin, J.D.; Durgin, G.D. Complete Link Budgets for Backscatter-Radio and RFID Systems. *IEEE Antennas Propag. Mag.* **2009**, *51*, 11–25. [CrossRef]
18. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32. [CrossRef]
19. Vayyar. Available online: https://vayyar.com/technology/ (accessed on 11 October 2022).
20. Laird Inc. Available online: https://www.lairdconnect.com/rf-antennas/rfid-antennas/s902-series-rfid-antenna (accessed on 11 October 2022).

applied sciences

MDPI

Article

Electromagnetic Assessment of UHF-RFID Devices in Healthcare Environment

Victoria Ramos [1,*], Oscar J. Suárez [2], Samuel Suárez [3], Víctor M. Febles [3], Erik Aguirre [4], Patryk Zradziński [5], Luis E. Rabassa [3], Mikel Celaya-Echarri [6], Pablo Marina [1], Jolanta Karpowicz [5], Francisco Falcone [4,6] and José A. Hernández [3]

[1] Instituto de Salud Carlos III, 28029 Madrid, Spain
[2] Dirección General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual, 28071 Madrid, Spain
[3] Engineering and Telematic Department, Hospital Universitario de Canarias, 38320 La Laguna, Spain
[4] Electrical, Electronics and Communications Department, Universidad Pública de Navarra, 31006 Pamplona, Spain
[5] Central Institute for Labour Protection–National Research Institute (CIOP-PIB), 00-701 Warszawa, Poland
[6] School of Engineering and Science, Tecnologico de Monterrey, Monterrey 64849, NL, Mexico
* Correspondence: vramos@isciii.es; Tel.: +34-918-222-128

Abstract: In this work, the evaluation of electromagnetic effect of Ultra High Frequency Radio Frequency Identification (UHF-RFID) passive tags used in the healthcare environment is presented. In order to evaluate exposure levels caused by EM field (865–868 MHz) of UHF-RFID readers, EM measurements in an anechoic chamber and in a real medical environment (Hospital Universitario de Canarias), as well as simulations by 3D Ray Launching algorithm, and of biophysical exposure effects in human models are presented. The results obtained show that the EM exposure is localized, in close vicinity of RFID reader and inversely proportional to its reading range. The EM exposure levels detected are sufficient to cause EM immunity effects in electronic devices (malfunctions in medical equipment or implants). Moreover, more than negligible direct effects in humans (exceeding relevant SAR values) were found only next to the reader, up to approximately 30% of the reading range. As a consequence, the EM risk could be firstly evaluated based on RFID parameters, but should include an in situ exposure assessment. It requires attention and additional studies, as increased applications of monitoring systems are observed in the healthcare sector—specifically when any system is located close to the workplace that is permanently occupied.

Keywords: UHF-RFID; occupational exposure; public health; SAR; 3D-RL; electromagnetic risk; hospitals; 2D contour maps

Citation: Ramos, V.; Suárez, O.J.; Suárez, S.; Febles, V.M.; Aguirre, E.; Zradziński, P.; Rabassa, L.E.; Celaya-Echarri, M.; Marina, P.; Karpowicz, J.; et al. Electromagnetic Assessment of UHF-RFID Devices in Healthcare Environment. *Appl. Sci.* **2022**, *12*, 10667. https://doi.org/10.3390/app122010667

Academic Editor: Jia Liu

Received: 25 August 2022
Accepted: 18 October 2022
Published: 21 October 2022

1. Introduction

The application of the Information and Communication Technologies (ICT) that guarantee smart and seamless assistance has been significantly increasing and, thus, the health sector has become dependable on these technologies. To quote a relevant example, a reference should be made to the tracking system that is based upon short-range radio frequency, Ultra High Frequency—Radio Frequency Identification (UHF-RFID). This system is used to aid the identification process of materials, instrumentation and people at healthcare centers.

At the outset, the monitored objects are assigned a digital identity, with the use of labels attached to the objects that contain written individual number, as replaced or supplemented by barcodes, which are optically read by scanners (using infrared laser beams). With regard to the use of optical technologies, long-term and substantial human efforts are required for an object to be subject to individual processing, as an object needs to be approached to the scanner each time and a bar code needs to be located precisely within the optical scanner line.

The RFID is a widely used wireless technology for Automatic Identification and Data Capture (AIDC); it has been commonly applied to identify and track tags attached to specific objects. The RFID readers obtain and write data on tags, which are most frequently "passive tags", i.e., small electronic circuits which are supplied (charged) by the production of electromagnetic energy of the electromagnetic field (EMF) transmitted by the reader of RFID system.

Smart solutions for medical purposes (e-Health) are globally implemented as Smart Health [1] solutions. In this context, RFID technology enables objects to retain to their identity, similar to a unique serial number. The wireless RFID data exchanged are processed to provide real-time data in the monitoring systems. Usually, fixed readers and handheld readers are employed and, to this extent, from the point of view of the environmental electromagnetic impact, the following are most often recognized to be fit for their intended purpose: Manually Operated (MO) readers or Autonomous (A) readers. A schematic of performance of performance of an UHF-RFID system used in healthcare centers [2] is depicted in Figure 1.

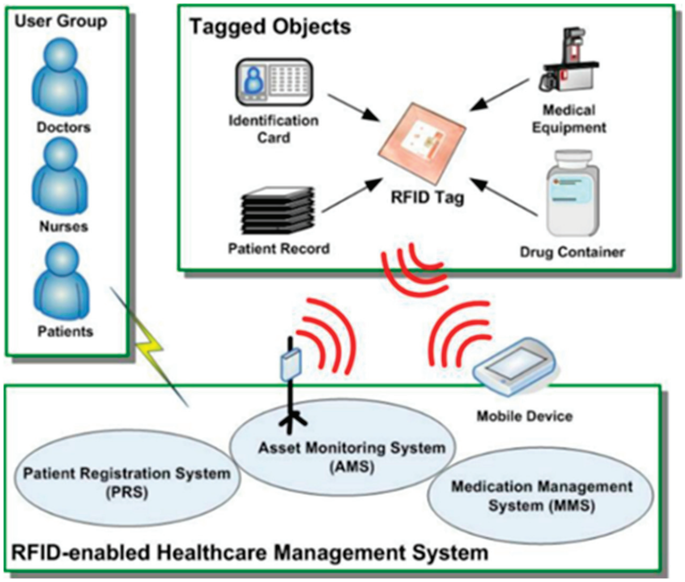

User Group
Doctors
Nurses
Patients
Tagged Objects
Identification Card
Medical Equipment
RFID Tag
Patient Record
Drug Container
Mobile Device
Asset Monitoring System (AMS)
Patient Registration System (PRS)
Medication Management System (MMS)
RFID-enabled Healthcare Management System

Figure 1. RFID performance scheme at a health center [2].

What we may observe today is that the environment and individuals are more and more exposed to new electromagnetic conditions, with no relevant provision made therefore in the legislation on human exposure or sufficient previous studies on their longstanding effect, considered low intensity exposure effects or operation of medical devices in indoor environments [3–9]. The electromagnetic assessment of the operation of the UHF-RFID system, that operates at the 865–868 MHz range, being in fact similar to the frequency of the EMF emitted by mobile communication GSM systems, and is essential for underpinning all aspects in response to a high demand for dynamic wireless applications in the healthcare environment.

For these technologies to be developed, manufactured and deployed further on, a need for signals, devices, antennas and complete systems to be measured and analyzed with respect to RF exposure nearby has emerged. The Electromagnetic Interference (EMI) may cause severe problems to electronic devices, and can imply dangerous consequences, if medical devices are affected. In relation with the effect of exposure on humans, the studies regarding the risk posed by mobile communication devices to health prove of relevance here [8,10,11]. In all cases, the electromagnetic environmental impact and the related risk can be mitigated when the relevant preventive measures are undertaken, as shown in [12,13].

The exposure levels recorded for the UHF-RFID system are subject to examination with the aim of verifying compliance with relevant laws and regulations; for example, the European general public recommendation 1999/519/EC, the European Directive 2013/35/EU on workers EMF exposure, EMC, RED or MED directives, using relevant European Standards or legislation transposing international legislation into legal system in particular countries, that apply to the electromagnetic environmental impact on safety of patients, attending visitors, workers or various electronic devices that have been used in the healthcare environment. In brief, in compliance with the laws and regulations concerning the minimum safety requirements as set forth in by international legislation, it has been assumed that humans should be protected against thermal effects caused in the body by exposure to the RF EMF. Considering the fact that sensitivity to these exposure effects differs in population, vulnerable populations should be protected against such exposure more restrictively (for example, pregnant women or users of medical implants).

The laws and regulations on the limitation of the EMF exposure levels are usually divided into those that refer to the so-called limits regarding workers' EMF exposure (which may be applied when the exposed humans are notified of and trained on the results of periodical assessment of exposure, electromagnetic hazards expected at the workplace, as well as any necessary preventive measures that was applied there; additionally, the volume and location of the space affected by EMF at the workplace should be accurately designated, protected against an access by unauthorized individuals, as well as all the actions undertaken by the employer are sufficiently documented in an appropriate manner). Exposure limits applicable to general public exposure are lower than the workers' exposure, as they are applicable to the population that may not be informed of electromagnetic hazards, and include vulnerable individuals; and, no preventive measures are required to be applied to reduce the expected electromagnetic hazards. However, the description of both kinds of exposure limits includes also the information on the exceptions to the rule—for the exposure lower than the specified limits; electromagnetic hazards are not excluded where the EMF affects vulnerable persons or electronic devices.

In general, the electronic devices may be almost completely immune to electromagnetic disturbance (even if its effect is as strong as an intentional military electromagnetic attack); but to achieve such immunity, the cost-generating design of the device is required (generating even very expensive production of highly immune devices). Various lower-cost electronic devices, that are at the same time much less immune to electromagnetic disturbances, are used in everyday life and work, depending upon their function and intended use. At the minimum immunity of low-cost electronic devices, they can actually operate in an appropriate manner when affected by EMF of the typical characteristic expected in the environment of their intended use; and, for the case of RF EMF impact on the devices used today, it is the level of exposure at the level of small fraction of general public exposure limits provided by the aforementioned European legislations. Taking into consideration the relevant role that the medical devices play today, including implanted devices such as cardiac stimulators, by applicable technical regulations (like, for example, technical regulations, namely EMC, RED, LVD or MED directives) it is required that they have better electromagnetic immunity than the basic immunity required for various low-cost electronic devices for everyday use. A device manufacturer delivers a relevant declaration on the level of electromagnetic immunity, along with the operating manual, e.g., in a section with the description of environmental conditions, safety, or EMC.

A relevant study of the analysis of the electric field (E-field) parameters is made, for example, as regards the exposure to spatial distribution of the results of the 3D Ray Launching (3D-RL) technique simulation, as displayed via 2D contour maps, as being processed with the use of a relevant MATLAB® algorithm [13,14]. Some other studies of the E-field parameters were based upon the scenario which entailed the far-field conditions, and applicable at least a several wavelength away from the emitting antenna [15,16]. There are also studies carried out whereby there were performed the measurements or numerical simulations of the Specific Energy Absorption Rate (SAR), and whereby the information on the biophysical effects of the EMF exposure in the human body was obtained, as well as the results of the research assessment with regard to the relevant limits related to the protection against thermal effects caused by EMF influence, that have been accurately determined under applicable laws and regulations and exposure assessment guidelines described in the analysis of the research papers, for example [17–22].

2. Materials and Methods

The purpose of the RF EMF measurements was to assure the compatibility between wireless systems installed at a healthcare center [23,24]. In order to analyze their use in the healthcare environment and the influence of the UHF-RFID system at the 865–868 MHz frequency range, several measurement procedures have been employed. In situ measurements are performed, among other things, to:

- determine RF exposure levels from the Equipment Under Test (EUT) and ambient sources,
- consider applicable regulations (exposure limits), as observed or extrapolated to maximum or actual maximum levels; or
- to monitor the RF exposure levels, even if they are well below the exposure limits that apply to ensure the protection against thermal effects of EMF influence.

In order to accomplish the objectives set for in situ measurements, it is required that frequency selective assessment be carried out whereby the contributions of relevant sources of interest to the total RF exposure will be determined, including other exposures from radio-communication systems such as mobile phones or internet access.

The projects were subject to the two assessment procedures, i.e., the first at the Hospital Universitario de Canarias (HUC), with the measurements having been performed where the RFID devices had been installed for assessment purpose. Additional measurements were performed in Madrid, where the assessment was made in an anechoic chamber, with the aim being to examine the worst-case scenario. An ad-hoc numerical simulation study was performed by means of: (1) Specific Absorption Rate (SAR) values from exposure near MO-RFID readers, (2) distribution of exposure from AG-RFID reader by means of an in-house 3D-RL algorithm, and (3) 2D contour maps representation [25,26].

2.1. UHF-RFID Devices Assessed

At the beginning of the process, there is an in situ analysis performed to identify the source of RF emission within the surrounding area. The in situ RF exposure assessment was performed at the measurement area, with the use of the selected exposure metric, measurement type and measurement techniques to satisfy the measurement objectives. Figure 2 depicts specific devices that were included into the study, i.e., manually operated (MO) and autonomous gate (AG) and autonomous shelf (AS) RFID readers (as specified in Table 1, including passive tags compatible with all the specified readers).

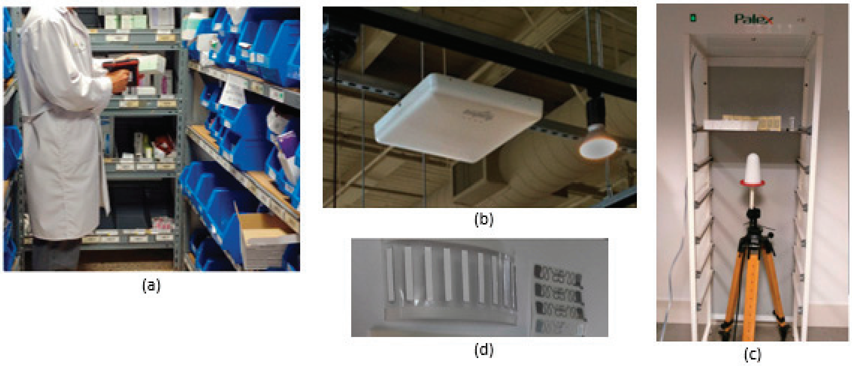


Figure 2. The RFID UHF readers used for the purpose of the study and commonly used at hospitals: (**a**) handheld reader AB700 (reader type: MO-RFID); (**b**) fixed xArray Gateway R680 (reader type: AG-RFID); (**c**) shelving DYANE Smartshelf (reader type: AS-RFID), (**d**) passive RFID tags compliant with (**a**–**c**) readers (type: EPCglobal UHF RFID Class 1 Gen 2).

Table 1. The Specifications of RFID UHF readers commonly used at hospitals and used during the study.

Description	**Key Parameters of the RFID UHF Readers Used for the Study**		
	Handheld Reader AB700	**Fixed xArray Gateway R680**	**Shelving DYANE Smartshelf**
Reader type	Manually Operated (MO-RFID reader)	Autonomous Gate (AG-RFID reader)	Autonomous Shelf (AS-RFID reader)
Frequency	860–960 MHz	860–960 MHz	860–960 MHz
Air Interface Protocol (compliant tags)	EPCglobal UHF RFID Class 1 Gen 2 [1] ISO/IEC 18000-63	EPCglobal UHF RFID Class 1 Gen 2 ISO/IEC 18000-63	EPCglobal UHF RFID Class 1 Gen2 ISO/IEC 18000-63
Max Receive Sensitivity	not available	−82 dBm [0.5 mV/m]	−84 dBm [0.4 mV/m]
Tag read sensitivity	from (−22 dBm) to(−10 dBm) [equivalent to the range: 0.5–2 V/m]		
Reading Range	0–7 m (according to tag and environment)	up to 1.5 m (according to tag and environment)	the entire interior of the cabinet
Writing Range	0–3 m (according to tag and environment)	not applicable	not applicable
Transmitted Power	up to 1 W ERP	up to 2 W ERP (EU1) [27] 4 W ERP (EU2) [27] 4 W ERP (FCC) [28]	up to 1 W ERP (EU1)
Antenna	1 antenna	1 phase array antenna (52 dual-polarized beams in 9 sectors)	4 expandable to 32 antennas with Speedway Antenna Hub optimized for imping reader antennas (RP TNC connector)

[1] duty cycle 48–82.3% for interrogator (reader) to tag communications [29].

The handheld readers (AB700 (ETSI)) are gun-shaped transceivers, normally used close to the human body. The RFID is used as shown in Figure 2a and can affect specific parts of the operator's body. It is recommended to make RFID readings with the arm extended to limit the exposure, but it increases the musculoskeletal load experienced by operator [7,8,30]. The relevant technical specifications are specified in Table 1.

The UHF-RFID fixed xArray (Gateway R680 (ETSI)) used for the study is located within at the Hospital Universitario de Canarias (HUC). The platform was installed for the assessment purpose, and the compliance with the requirements set was conducted. The xArray provides real-time identification and localization of the tagged items. It was positioned in the center of a room ceiling, with a room height of approximately 3.5 m, and eventually the housed estimated area was of 8 × 8 m. The Impinj's Item Sense management software triggers and automatically handles the management and monitoring infrastructure. The UHF-RFID device used for the study is presented in Figure 2b and the relevant technical specifications are presented in Table 1.

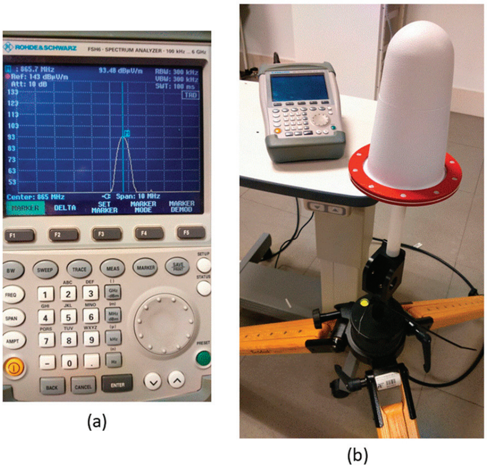
The device DYANE Smartshelf subject to assessment hereunder is an RFID smart shelving system, that is used for automation of tagged reagent inventory control in operating theatres and clinical laboratories in real time. It is presented in Figure 2c. The process is handled, with the use of the DYANE software, which provides access to parameter reports. The relevant technical specifications are shown in Table 1.

2.2. EMF Spatial Distribution and Level Measurements

The comprehensive exposure assessment, source identification, and configuration at a maximum transmission power or actual maximum power was accurately performed for the purpose of this paper. The characteristic features of the RF EMF exposure were studied with respect to its spatial distribution to be denoted in E-field strength (E, in V/m), based on results of measurements or calculations.

2.2.1. Hospital Universitario de Canarias (HUC)—Tenerife (Assessment of MO-RFID and AS-RFID Readers)

The measurements were performed, with the use of frequency selective equipment, i.e., a R&S FSH6 spectrum analyzer (measurement uncertainty <1.5 dB, typical 0.5 dB) and an antenna ETS-LINDGREN, Mod.3181 (500–9000 MHz), that are specified in Figure 3.



(a)

(b)

Figure 3. Measurement set up used for in situ measurements of EMF emitted by studied RFID readers: (**a**) Rhode & Schwartz FSH6 spectrum analyzer, (**b**) Antenna ETS-LINDGREN, Mod.3181 on tripod.

The measurements were made at an RFID core frequency (866 MHz), in a "demo" mode of MO-RFID reader operation, whereby undisturbed emission was guaranteed, without a need for human involvement in the procedure.

The measurements were carried out in a wide-open area, a tower located on the 4th floor of the hospital. Measurements were recorded at distances of from 0.25 and 4 m, and at angles between 0° and 180°, rotating in 45° angle steps.

The E-field was assessed near the reader with an antenna located vertically (compliant with a regular position when the MO-RFID reader is used at a "gun-like" position). The exposure scenarios (ESs) include:

- Exposure caused by activation of MO-RFID reader placed on a table, at a 1 m height, with reading tags located at a 1 m height from the floor
- Five angles (degrees): 0, 45, 90, 135, and 180
- Five distances (m): 0.25, 0.5, 1, 2, 4.

An AS-RFID reader was placed inside a room at an approximate height of 3.5 m, without windows and with a door near the wall. Measurements were carried out at 866 MHz and at 1.0 m, 1.3 m and 1.7 m heights from the floor, representing the zone of genitalia, breast and abdomen, and head respectively to the floor, as they are considered sensitive parts of a human body. The levels were also assessed inside the Smartshelf 0.075 m to the rear part, which was a minimum distance of proximity. The fact that there were no doors in the wardrobe can be used to examine the worst-case scenario. When it is located at the patient examination area, they would be exposed rather sporadically and of short duration.

2.2.2. Anechoic Chamber—Madrid Laboratory (Assessment of MO-RFID and AG-RFID Readers)

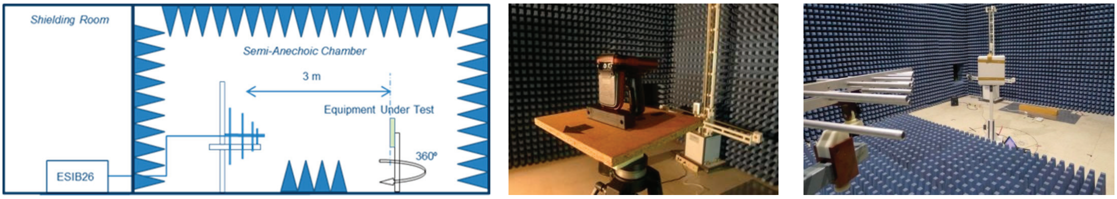
The measurements of the ERP that involved the worst-case scenario were made at The Dirección General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual (Madrid). Table 2 presents the list of the tools that were mainly used for this purpose.

Table 2. Laboratory devices used for anechoic chamber UHF-RFID assessment.

Equipment	Marque-Brand	Model
EMI Receptor	Rohde & Schwartz	ESIB26
RF Generator	Rohde & Schwartz	SMT02
Log-Period Antenna	EMCO	3146
Semi anechoic chamber	IRSA	3 m
Software	Rohde &Schwartz	EMC32-E
Mast	EMCO	1050
Table	EMCO	1060-1.2

Measurement uncertainty: ±3.81 dB of E-field strength; at duty cycle: 100%.

The measurements of EMF emission of RFID readers (working band: 865–868 MHz) were carried out in an anechoic chamber with an absorbent on the floor, with the device situated vertically on a support (in case of a MO-RFID reader, also in the presence of an individual to achieve continuous transmission). The E-field strength (E) emitted at distances of 0.5 m, 1.0 m and 3.0 m from the equipment were recorded. The measurement setup is presented in Figure 4. The study includes a concise and precise description of the procedures carried out during the experiment. The complete and detailed information is available in [13].



(**a**) (**b**) (**c**)

Figure 4. Laboratory measurements of the EMF emitted by RFID readers inside the anechoic chamber: (**a**) measurement scenario, (**b**) measurement of a MO-RFID reader, (**c**) measurements of AG-RFID reader.

2.3. Simulations of Exposure from the AG-RFID Reader by Means of an In-House 3D-RL Algorithm

An in-house simulation MATLAB® algorithm was used and E-field estimations were obtained. Far-field conditions were supposed during all the processed simulations, and the parameters like dielectric permittivity and conductivity were obtained for specific elements. The simulation results exhibit uncertainty in the 2 dB to 5 dB range, owing to the 3D scenario mapping process.

Specific materials were considered with variables in Table 3. Other simulation parameters are shown in Table 4, apart from free space losses, reflection, refraction or diffraction. The emission was produced by the devices at the same positions as in the real-life scenario. A concise and precise description of the experimental work is presented here. The complete and detailed information is available in [13].

Table 3. Material Properties for 3D Ray Launching Simulations [13].

Material	Conductivity (σ) [S/m]	Relative Permittivity (εr)
Aluminum	37.8·106	4.5
Steel	7.69·106	4.5
Nylon	0.24	1.2
Wood	0.21	2.88
PVC	0.12	4
Polypropylene	0.11	3
Glass	0.11	6.06
Concrete	0.02	25
Rubber	1×10^{-14}	2.61

Table 4. Variable Configuration for 3D Ray Launching [13].

Parameter	Value
Operation Frequency	865–868 MHz
Transmitted Power	0.00316–2 W
Horizontal angular resolution (ΔΦ)	1°
Vertical angular resolution (Δθ)	1°
Permitted maximum reflections	6
Cuboids size (Mesh resolution)	0.5 m × 0.5 m × 0.5 m
Diffraction phenomenon	Activated

Simulation uncertainty: 2 dB to 5 dB, owing to the 3D scenario mapping process.

The graphic representation of the information on the EM levels is considered a well-known tool for clear depiction of the information as presented in previous works drafted by [6,13,14].

This paper has been prepared with the use of the methodology for the production of 2D contour maps that offer graphic, immediate and accurate representation of the EMF distribution. The data collected were imported using graphic software (Surfer 8) to draw 2D contour maps showing the previously measured field strength values. The selected measurement points are displayed in Figure 5.

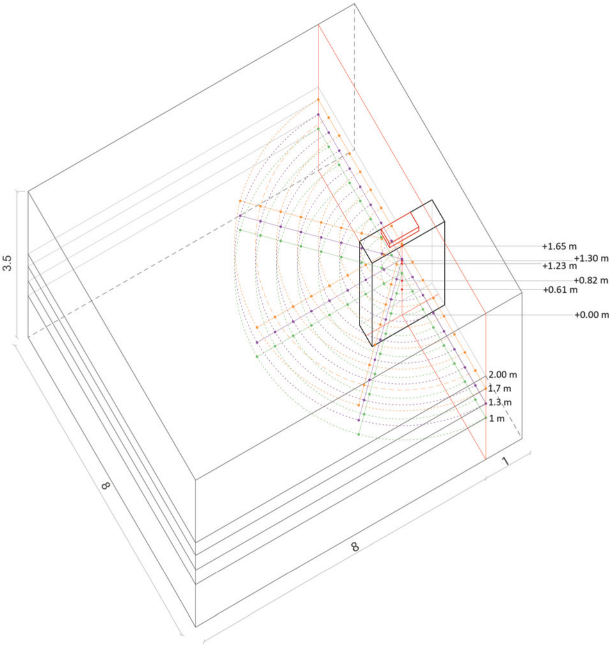


Figure 5. Grid and measurement points in a care room of the HUC for the AS-RFID reader assessment.

2.4. Specific Absorption Rate (SAR) Values from Exposure near MO-RFID Readers

When individuals approach the source of EMF where near-field exposure conditions are recognized (i.e., in the distance from the source shorter than the wavelength of emitted EMF or even several wavelengths), their exposure has to be assessed using the parameters characterizing the effects of EMF influence in tissues. In case of radiofrequency EMF exposure, the relevant parameter is the metrics of thermal effects—time derivative of the incremental electromagnetic energy (dW) absorbed by an incremental mass (dm), recognized as SAR values expressed in watts of absorbed EMF energy per kilogram of exposed tissue, (W/kg). The SAR is assessed as averaged over the entire exposed body and also as localized SAR averaged in particular smaller parts of the exposed body (over 10 g mass of any continuous tissue—SAR10g) [12]. SAR values are assessed by the numerical modeling of the EMF interaction between the model of EMF source and heterogeneous anatomical body model, usually with the use of Finite-Difference Time-Domain (FDTD) numerical code compliant with the requirements set forth in the relevant international standard [31]. In the international guidelines and applicable laws and regulations relevant limits regarding mentioned SAR, values have been provided aimed for assessment of EMF exposure of workers and general public. As provided for in the relevant international laws and regulations, the SAR must be assessed for all the cases of the localized exposure within reactive near-field [24]. Moreover, under the Directive 2014/53/EU (RED), it is required to take all intended and reasonably foreseeable operating conditions of radio equipment use into account for the exposure assessment [32].

The parameters of a typical MO-RFID reader used for our simulation are presented in Table 1. As regards the exposure scenarios applied for the purpose of the study, the antenna was located vertically (similarly to the position of an external antenna in a MO-RFID reader shown in Figure 2). The exposure scenarios include, as presented in Figure 6:

- Exposure of an operator of a MO-RFID reader grasping a gun in the hand,
- Exposure of people approaching an operator of an MO-RFID reader—scanned person or bystander.

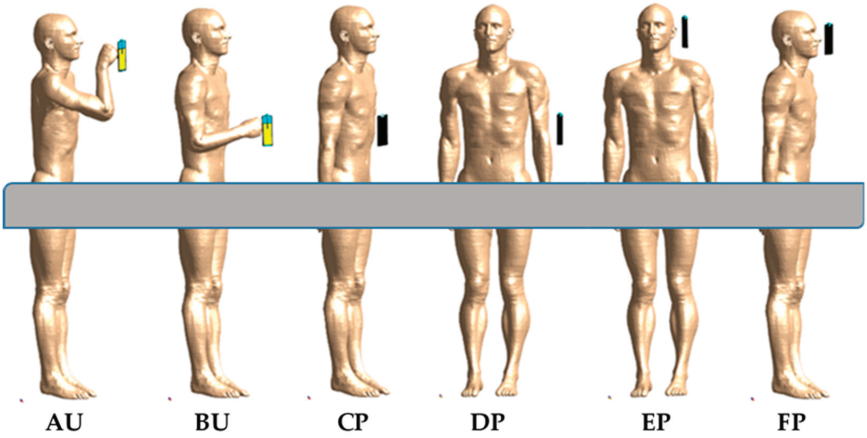


Figure 6. The exposure scenarios: (1) exposure of an operator grasping a MO-RFID reader (AU—in front of the face; BU—in front of the chest, (2) exposure of an individual approaching a RFID gun used as in AU or BU scenario (CP—in front of the chest; DP—at the side of the body, at the height of the chest; EP—at the side of the body, at the height of the head; FP—in front of the face). The anatomical numerical model of operator—Duke developed by the ITIS Foundation (over 300 tissues/organs: muscles, fat, bones, nervous tissues, heart, liver, skin, etc.).

Based on the principles of the electromagnetic hazard management system, the EMF exposure of a reader operator is assessed with respect to the exposure limits set for the worker exposure (when an operator is an informed and qualified worker and the relevant prevention measures with respect to electromagnetic hazards are applied and accurately evidenced), or with respect to the general public exposure limits (when a gun is used by a person assuming to be without a regular employment contract, i.e., with no understanding of electromagnetic hazards and where prevention measures are not applied).

Similarly, the exposure of a scanned person or a bystander is assessed in terms of the exposure limits set for the general public exposure or worker exposure (depending upon the aim of their presence nearby a activated reader and applied electromagnetic hazards management system).

Numerical simulations were carried out with the use of anatomical numerical male model and Sim4Life software (Zurich Med Tech, Switzerland) and Finite Difference Time-Domain solvers (FDTD). The FDTD method is a solution of Maxwell's curl equation in the time domain [31]. The uncertainty of the numerical simulations (i.a. related to the model of EMF source, dielectric properties of the model of human body and model resolution (staircase approximation)) was estimated as not exceeding ±1 dB (K = 1), within the range compliant with the state of the art in the field [33,34].

An accurate description of the work is presented here, however additional information is available in [12].

3. Results

This is here to focus on the electromagnetic impact of the UHF-RFID system upon the healthcare environment (studied through measuring and/or modeling the EMF parameters or modeling the effects of EMF exposure), to include:

(a) Measurements of E-field values at a platform at the HUC (evaluation of EMF emitted by MO-RFID and AS-RFID readers);

(b) Measurements of the E-field values at an anechoic chamber, that have been taken as for a worst case (evaluation of EMF emitted by MO-RFID and AG-RFID readers);

(c) Simulations of the SAR values, using the FDTD method (evaluation of effects of exposure to EMF emitted by MO-RFID reader);

(d) Simulations of the E-field values, using an in-house 3D-RL algorithm and 2D contour maps representation (evaluation of the EMF emitted by the AG-RFID reader).

3.1. Hospital Universitario de Canarias (HUC)—Tenerife (Measurement-Based Assessment)

An extensive catalogue of opportunities for the RFID technology to serve as an intended use also involves a variety of the EMF exposure options on the side of device operators, along with other persons that may be present at the site.

3.1.1. EMF Exposure near MO-RFID Reader

Radiation pattern, (to include maximum values from measurements for horizontal and vertical positions of measuring antenna and adjusted RFID antenna position) was sampled out around antenna starting in front of UHF RFID antenna with angle step of 45º, to cover major, lateral, and back radiation.

The E-field distribution was evaluated along three axes passing through the center of the antenna of the MO-RFID reader (gun): in the front and back of the reader plane—perpendicular to it and at the side of the reader—perpendicular to the reader’s edge at some distances of the reader center. The results were normalized to an output power equal to the case considered in the numerical simulations (1 W). Measurements obtained in Torre Norte 4 Floor may be observed in Table 5.

Table 5. The E-field measurements results obtained near the MO-RFID reader: frequency—866 MHz, location—HUC, Torre Norte 4 Floor.

Distance (m)	E-Field Peak Value [V/m]				
	Angle (º)				
	0	45	90	135	180
0.25	0.117	0.117	0.117	0.118	0.118
0.50	0.118	0.118	0.118	0.118	0.119
1.00	0.119	0.119	0.112	0.109	0.105
2.00	0.099	0.070	0.066	0.090	0.093
4.00	0.062	0.058	0.050	0.040	0.042

Level measurement uncertainty <1.5 dB, typical 0.5 dB.

Most of E-field intensity levels were in the range from 0.040 V/m to 0.090 V/m. Nevertheless, a peak value of 0.210 V/m was registered at the angle 0°, at the height of 1.0 m and at a distance of 1.5 m. Lower values of 0.137 V/m and 0.116 V/m were registered at the 180° angle, at 1.5 and 2.0 m, respectively. The peak value of 0.210 V/m corresponds to front position: MO-RFID reader and antenna are at the height of 1 m and between them, there are 1.5 m and the lowest at the 180° angle.

In addition, a peak of 0.190 V/m was registered at the height of 1.7 m, at the 0° angle and at a distance of 1 m, obtaining lower values, 0.155 V/m and 0.127 V/m, at the 180° angle, at 1.0 and 1.5 m, respectively. As for the previous measurement results, peak value was obtained in a front position and the lowest at the 180° angle. The following is a concise and precise description of the results of the experiment. The complete and detailed information is available in [13].

3.1.2. EMF Exposure near the AS-RFID Reader

The distance was measured from the rear panel of the cabinet, where the RF emitting antennas are located, to the center of the antenna. The measurements at 135° and 180° have been made at angles of 45° and 90° angles, for the rear wall of the cabinet. The heights were measured from the floor to the center of the antenna. Figure 5 presents the map where the measurement points are marked.

At 1.0 m, 1.3 m and 1.7 m heights, the average of the recorded E-field strength values was 0.056 V/m, 0.059 V/m and 0.061 V/m, respectively.

Along with the distance increase, there the E-Field decrease was recorded, that was more specific and more clearly observable as the measuring angle was getting narrower, the foregoing can be up to almost 10 dB/m at 4.0 m for zero angles. However, at 180° we can observe more constant values.

The test was also carried out for the same 866 MHz frequency value, inside the cabinet at different heights of from 0.61 and 1.65 m, above the cabinet floor. Measures were also carried out at 0.075 m from the rear panel, where the emitting equipment was located, and at 0° angle. The field levels remained at approximately 0.270 V/m for all heights applied for the purpose of the test. The results obtained are presented as the Radiation Diagram in Figure 7 and the results presented on a 2D contour maps are accurately depicted in Section 3.5. later on.

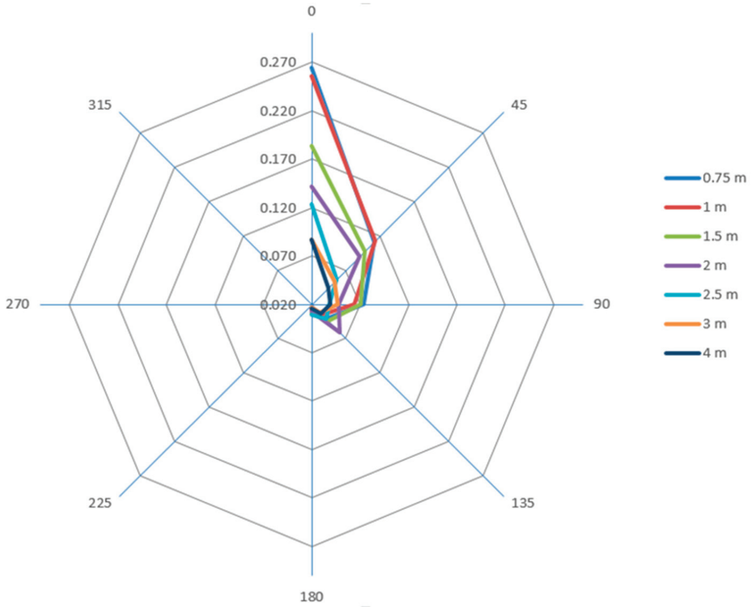


Figure 7. Spatial distribution of E-field measured near AS-RFID reader (V/m).

3.2. Anechoic Chamber—Madrid (Evaluation by Measurements)

3.2.1. EMF Exposure near MO-RFID Reader

The dimensions of an anechoic chamber, where measurements on the EMF emitted by the MO-RFID reader were made, were as follows: 9.76 m × 6.71 m × 6.10 m. The reader was set on a manual positioning device, and, thus, the former could be rotated to facilitate the measurement of the radiation pattern. The radiation pattern, (maximum values from measurements for horizontal and vertical positions of measuring antenna and adjusted RFID antenna position) was sampled out around antenna, starting in front of an UHF RFID antenna with a 45° angle step, to cover major, lateral and, back radiation.

The differences in E-field values measured (Em) and calculated (Ec) are shown in Table 6 and Figure 8. The calculated measurements are obtained based on the ERP (Effective Radiated Power) values, and an equivalent calculation of the E-field intensity is performed at the measurement distance. The test equipment, with a transmission button pressed, delivers emissions for an approximate time of 1 min and then emission stops.

Table 6. The results of measurements and calculations of E-field near MO-RFID reader (at 3 m away).

Azimuth	Ec	Ec ± U	Em	Em ± U
(o)	V/m	V/m	V/m	V/m
0	1.30	0.89–1.89	1.96	1.26–3.04
45	1.30	0.89–1.89	1.79	1.16–2.78
90	1.08	0.74–1.57	1.39	0.89–2.15
135	0.95	0.65–1.38	0.95	0.61–1.48
182	0.34	0.24–0.50	0.46	0.30–0.72
225	0.33	0.23–0.49	1.08	0.70–1.67
270	0.53	0.37–0.77	1.44	0.93–2.24
315	1.04	0.71–0.71	1.79	1.16–2.78

Ec—E-field calculated value; Em—E-field measured value; Ec ± U—the range of E-field calculated ± uncertainty; Em ± U—the range of E-field measured ± uncertainty.

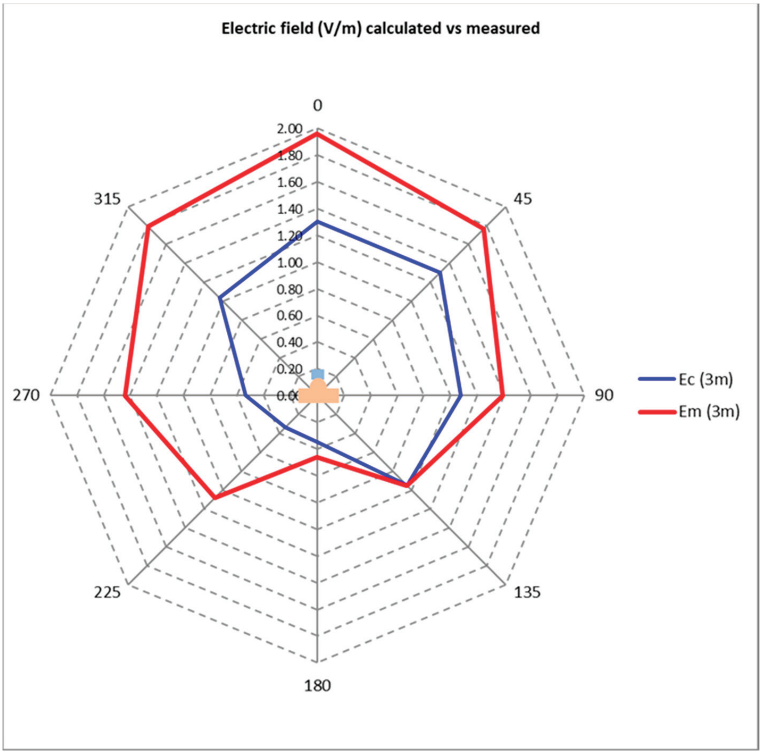


Figure 8. Spatial distribution of E-field measured and calculated near MO-RFID reader.

3.2.2. EMF Exposure near AG-RFID Reader

The maximum levels, 15.88 V/m and 10.68 V/m, were registered at the shortest as can be seen. These values decrease notably along with the distance. The lowest levels were registered at 3 m away from AG-RFID reader, with values of 1.49 V/m and 0.71 V/m recorded at 0° and 45° angles, respectively, and 0.25 V/m at of from 90°–270°. Table 7 presents the E-field strength values along the direction of the maximum radiation from the device under test in function of the distance. Figure 9 presents the calculated radiation pattern of the AG-RFID reader, depending upon the distance value [13].

Table 7. The E-field peak values measured at 0.5 m, 1.0 m and 3.0 m from the AG-RFID reader [13].

	Calculated E-Field, Ec, V/m		
Azimuth, (o)	**3 m Away from the Reader**	**1 m Away from the Reader**	**0.5 m Away from the Reader**
0	2.65	7.94	15.88
45	1.78	5.34	10.68
90	0.51	1.52	3.05
135	0.44	1.33	2.65
182	0.39	1.17	2.33
225	0.32	0.96	1.91
270	0.69	2.06	4.11
315	20.3	6.08	12.16

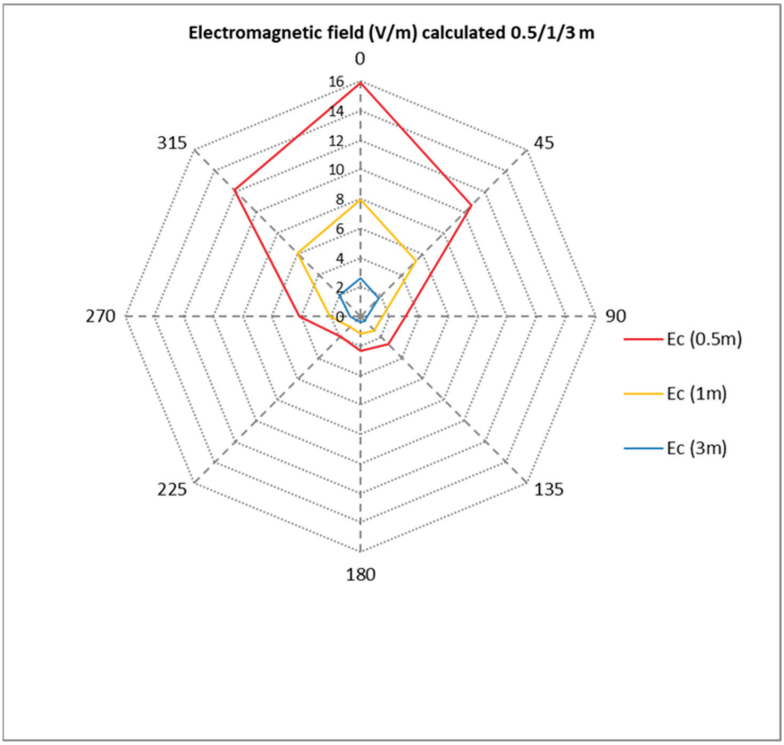


Figure 9. Spatial distribution of E-field calculated near AG-RFID reader [13].

A concise and precise description of the experimental work is presented here. Additional information is available in [13].

3.3. *Specific Absorption Rate (SAR) Values from Exposure near Handheld UHF-RFID Readers*

Considering the exposure to EMF of the user of the MO-RFID reader, the highest WB SAR value (0.036 W/kg, i.e., approximately to 50% of relevant limit regarding the exposure of general public, as set by the European recommendation 519/1999) was obtained at the AU and BU exposure scenarios, when a MO-RFID reader is grasped near the front of the body. The obtained SAR values were summarized in Table 8.

Considering the exposure of the other person present nearby the activated reader (scanned person or anyone present in the vicinity), the highest WB SAR value (0.034 W/kg, again approximately to 50% of the limit on public exposure) was obtained at the CP exposure scenario, when MO-RFID reader is in front of the chest.

Table 8. Whole body averaged and local SAR under exposure to an EMF at a frequency of 865 MHz emitted by the UHF-RFID gun reader; values normalized at level of the EMF emission from an RFID at 1 W (ERP), (6 min continuous exposure).

Exposure Scenario	WB NSAR	NSAR 10g				
		Head	Torso	Palm	Arm	Leg
AU–Head-20 cm	0.036	0.091	0.038	4.2	-	0.0026
BU–Chest-20 cm	0.036	0.054	0.34	3.8	-	0.0079
CP–Hip-16 cm	0.034	0.33	2.1	-	0.15	0.051
DP–Chest-5 cm	0.014	0.095	0.82	-	2.1	0.020
EP–Side-5 cm	0.022	1.3	0.46	-	0.15	0.0021
FP-Chest-5 cm	0.018	2.1	0.15	-	0.014	0.0044

The maximum values of local SAR 10g were obtained for the palm of MO-RFID reader operator (in the AU scenario), as well as the breast and head of the exposed person (in the CP and FP scenarios)—at the levels comparable with a relevant limit regarding the exposure of general public. Local SAR 10g values in other analyzed cases (in legs, torso and head) were found significantly lower due to significantly greater distance between the reader antenna and the particular parts of the body.

Figure 10 shows the E-field distribution within the UHF-RFID gun area, at a radiated power of 1 W: distribution along the plane normal to the antenna.

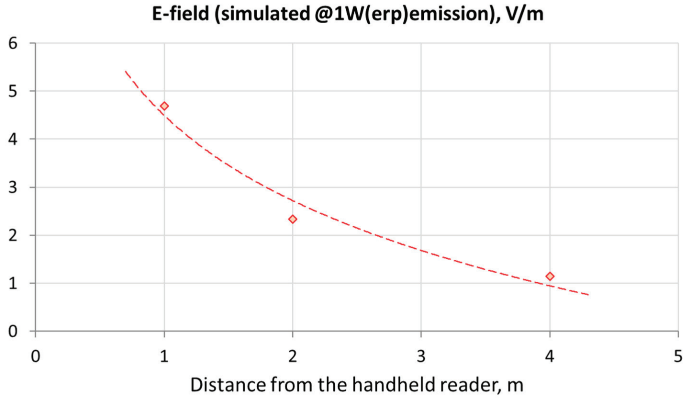


Figure 10. E-field distribution at a plane normal to the UHF-RFID gun antenna plane at a radiated power of 1 W. Spatial distribution of E-field measured near the AS-RFID reader.

The reading range of various UHF-RFID reader depends upon the radiated power and sensitivities of a passive tag used (typically 0.6–1 V/m of EMF exposure coming from the reader is required to read passive tags, however older tags may have lower sensitivities) [12]. The passive tags reading range of such sensitivities at a radiated power of 1 W was found in the range 4–10 m. The E-field values lower than 3 V/m (minimum required electromagnetic immunity of medical equipment used in professional healthcare environment according EN 60601-1-2) in this case were found at distances longer than approximately 30% of the reading range [35].

The worst-case may be depicted as a stay near a reader for 6 min with continuous emission at maximum power, although a more usual exposure scenario is with a shorter exposure time. Moreover, the remaining furniture, its fixation, the gun handle and the monitor were not considered in our model, but they may also contribute to the decrease of the EMF values. However, RFID guns may also have emitting antennas for other radio communication technologies operating at radiofrequency band, like Bluetooth, Wi-Fi, public cellular networks (used for the transmission of data, e.g., using LTE services), which can increase the SAR in a human body when activated along with the gun RFID antenna. The following is a concise and precise description of the results of the experiment. Additional information is available in [12].

3.4. Simulations of E-Field Distribution from AG-RFID Reader Using In-House 3D-RL Algorithm

E-field distribution within cut plane heights is presented in Figure 11. The maximum values are obtained inside the room in which the AG-RFID reader is located. It was positioned on the center of a room ceiling, with a height around 3.5 m, covering an estimated zone of 8 × 8 m. As height increases, so do the average E-field levels, as the measuring points are closer to the reader antenna.

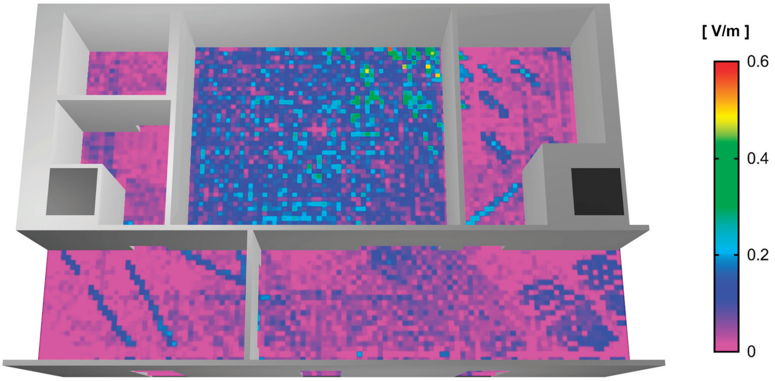


Figure 11. E-field distribution within the hospital ward simulation scenario [13].

To validate the E-field results obtained with the 3D RL approach, they have been compared with those from the ward scenario in the real case, considering different angle values (with orientations of 0°, 45°, 90° and 135°) and different cut-plane heights (h = 1 m and h = 1.7 m) inside the room. Some results are displayed in Figures 12 and 13, showing good agreement between the simulation and measured levels, within a linear radial distribution, 0° orientation, and cut plane height of 1 m. Deviations between the simulation and measurement results were in the range of 2–5% in E-field value estimation, and are given by differences between the topo-morphological description of the simulation scenario as compared to the real one, as well as deviations in material parameters.

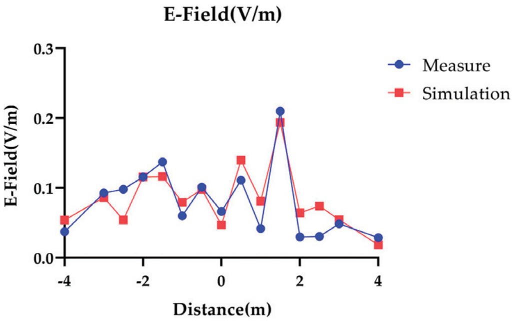


Figure 12. E-field estimation within a linear radial distribution, 0° orientation, cut plane height 1 m [13].

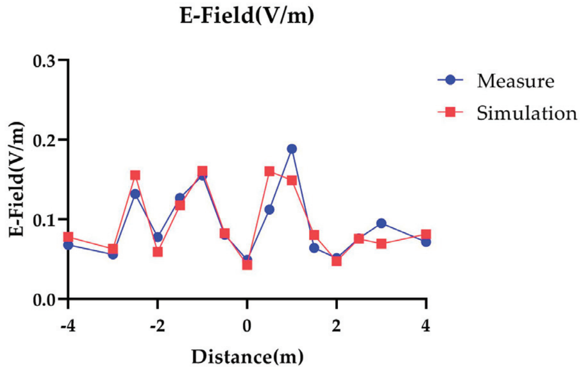
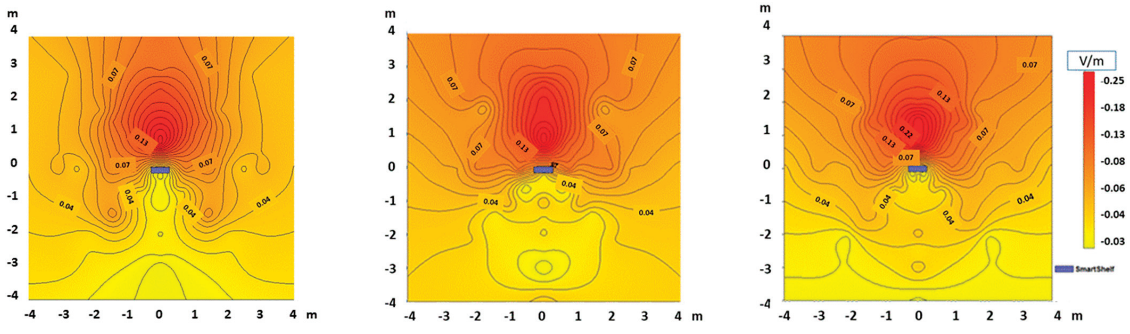


Figure 13. E-field estimation within a linear radial distribution, 0° orientation, cut plane height 1.7 m [13].

A concise and precise description of the experimental work is presented here. Wide and detailed information may be found in [13].

3.5. 2D Contour Maps Representation of E-Field Distribution near AS-RFID Reader

The graphic designs are to be perceived to be an accurate view of the EMF values at specific locations at the healthcare center. After the data collecting process is finished, the data were transferred to the graphic software (Surfer 8) to generate 2D contour maps, based on the previously measured EMF parameters. For each measurement, the antenna was oriented to detect the E-field maximum level and make relevant records. The EMF value curves were accurately presented. Graphs were prepared to depict the measurements at three different heights in the case of AS-RFID reader. As in the case of the AG-RFID reader, the curves of the E-field distribution were included there, as well. Given the fact that this distribution is symmetric, the results were extrapolated to the other unmeasured side. The 2D contour maps and the location of the radiation source are shown in Figure 14a–c. The mean values obtained are 0.056 V/m for 1.0 m high, 0.059 V/m for 1.3 m high, and 0.061 V/m for 1.7 m high. The points with the higher electromagnetic exposure recorded are accordingly marked in a more intensive red color, specifically in the front part, which is the direction where the radiating elements of the rear part are pointing.



(**a**) (**b**) (**c**)

Figure 14. 2D Contour map of the experimental values of the E-field (V/m) in the vicinity, up to 4.0 m from the center point, of AS-RFID reader: (**a**) at 1.0 m height above the floor; (**b**) 1.3 m height above the floor; (**c**) 1.7 m height above the floor.

4. Discussion

Given the more and more frequent use of the wireless networks within the proximity of medical devices, it will be crucial to determine the points with higher exposure levels. Following the results obtained by the authors, the EMF measured in far-field (sufficiently away from the readers, i.e., at distance of at least 0.5 m away from the readers antenna) are within the limits provided to evaluate the health hazards to exposed humans, that have been due to the thermal effects of the absorption of electromagnetic energy in tissues, as specified for in the applicable laws and regulations and research review reports. At the frequency of 866 MHz, like for the EMF emission from the tested UHF RFID readers, the specific limits aimed to assess the thermal exposure effects, lie within the range of 40–200 V/m, for example: the limit of 88.3 V/m has been delivered to assess the EMF exposure at the work environment, in compliance with the European Directive 2013/35/EU, [36] or the limits of 88.3 V/m and 193.8 V/m were set forth in the ICNIRP 2020 to assess whole body and local occupational exposure, respectively, or accordingly, many-fold lower limits set for the general public exposure at discussed frequency.

Nevertheless, what should be emphasized to this extent is the fact that the level of emitted EMF is inversely proportional to the distance from the emitting antenna, and to the reading range of the applied RFID system. Consequently, the closer to the antenna, the more the EMF level rises. At the near-field, within a distance shorter than the wave length (as for the consider RFID readers emitting EMF of an approximate wavelength of 0.3 m), the thermal effects of EMF exposure near the source are to be examined, with the use of SAR computer simulations. The results of the studies carried out for such near-field exposure case (when a manually operated RFID reader is used, or by mistake rather, anyone is present directly close the autonomous reader) show that the electric field strength directly close to the reader may raise significantly exceeding 5 V/m, when in the far-field the EMF exposure level is many-time lower, depending on the distance from the antenna and the reading range of used system. With regard to the average value of the measured E-field, the distances at which these values were obtained and the fact that the exposure would be sporadic near autonomous readers located away from people, the conclusion goes that an operator of the considered manually operated devices or the individuals approaching their proximity may suffer from the exposure at levels comparable to the exposure limits provided to protect against thermal effects of EMF influence on exposed tissues. The results obtained by the authors show that whilst taking the EMF exposure effects in the near-field surrounding UHF RFID readers into consideration, the relevant preventive measures should be undertaken with the aim being to ensure sufficient protection of individuals who may be present there, where the RFID reader emitting over 1 W of electromagnetic radiation is used and the individuals may access the areas that is closer than 30% of reading range of the applied RFID system.

However, all guidelines included the notes that the vulnerable individuals may require additional protection, including also the protection against inappropriate operation of electronic devices, at the level of exposure which is formally compliant with international exposure limits—with the foregoing to be of specific significance for medical implants that are more often used in healthcare centers than in public areas. Specifically more attention should be paid to the use of manually operated RFID the application of which is planned at the areas accessible to patients and visitors. The foregoing implies the E-field levels may be considered negligible where autonomous readers are used and located far from space accessible for workers, patients and visitors in healthcare centers. When individuals are within a direct proximity of readers emitting antennas, there emerges a need to undertake the relevant prevention measures, that will be of assistance to vulnerable individuals, users of medical implants and electronic devices. To this extent, the lowest limit of E-field to be examined as regards the electromagnetic interferences with electronic devices (EMC) is 3 V/m (CENELEC) EN 60601-1-2:2015 [35]. Therefore, the space where E-field level may exceed the EMC-related attention level is many-time larger than the space of exposure which requires evaluation with respect to SAR limits. However, following the SAR results, it is revealed that the EMF exposure near to the manually operated UHF RFID readers (guns) do not provide the SAR values that will exceed the general public limits, on the condition that the emission does not exceed 1 W, which in fact implies the use of the RFID system with a reading range of from 3 to 10 m (depending upon the sensitivities of used tag).

The E-field values obtained with the use of the 3D-RL deterministic approach showed good agreement between the simulation and measurement values, indicating the adequate option to perform estimation of volumetric E-field distribution and mapping with the use of the proposed methodology. This is why the foregoing approach is considered a useful tool, with the specified methodology to provide an immediate and accurate vision of the EM fields, for detect the highly exposed areas, within the proximity of the patients, visitors and the healthcare personnel. The 2D graphic representation, with 2D contour maps, may be of assistance when ensuring protection against EM interferences with medical devices, that may cause potential damage to patients, and when detecting highly exposed locations, whereby the emission values do not reach the suggested limits, and when planning and developing the prospected high-tech healthcare centers [6]. All the above specified activities and measures should be compatible with a sufficient signal level set for the wireless systems as installed at a healthcare center.

A potentially excessive amount of exposure to the EMF emitted by UHF-RFID devices can be dangerous to patients or other people; therefore, it requires further more comprehensive analysis and examination, with the good practice guidelines to be accurately developed for the design and use of RFID systems at the healthcare industry.

There have been some limitations for the exposure formally compliant with mentioned international guidelines, including the principles to be applicable to precautionary measures that in fact require some further consideration [37,38]. The limits provided by the guidelines are considered only with regard to the protection against the thermal effects of such exposure, yet not against any other potentially harmful effects as reported for the lower EMF exposures. However, as it has been determined under the applicable guidelines and laws and regulations, vulnerable individuals, such as the users of medical implants specifically, may require some further protection to be further considered, for example as required from employers' activities, following the provisions of the Directive 2013/35/EU [36].

The electromagnetic hazard assessment methods subject to discussion hereunder, as well as the issue of the assessment of the RFID system operation in healthcare environments, seems to be of importance due to social issues, legal issues as well as scientific research that are continuously applicable to such assessment, e.g., following the rhetoric of the SCHEER Scientific Committee on Health, Environmental and Emerging Risks, elaborating their opinion on the need of a revision of the annexes in Council Recommendation 1999/519/EC and Directive 2013/35/EU, in view of the latest scientific evidence available with regard to RF (100 kHz—300 GHz)—provided for public discussion in 2022.

5. Conclusions

Due to the more frequent use of the wireless communication networks within the proximity of medical devices at healthcare centers, it has become crucial to determine the points with higher levels of exposure.

A comprehensive exposure assessment, source identification, and configuration at maximum transmitted power or actual maximum power is performed. The characteristic of Radiofrequency EMF exposures have been studied, in terms of their spatial distribution denoted at the E-field strength, based upon the measurements or calculations results.

Following the results obtained by the authors, the electric field strength (at 866 MHz frequency) values, as measured or simulated with the use of the computer modelling in far-field areas of the examined UHF RFID readers intended for manual or autonomous operation at the healthcare centers (>0.5 m from antenna), are substantially lower than the exposure limits provided for in guidelines, laws and regulations that are applicable to the protection of health of the EMF exposed individuals against hazards associated with the thermal effects of the absorption of electromagnetic energy in tissues.

Still, all the guidelines included notes whereby it was stated that vulnerable individuals may require some additional protection at exposure levels below mentioned thermal effects-based limits, including the protection against inappropriate operation of electronic devices, with the foregoing of specific importance for the medical implants that appear to be more likely used in the healthcare centers than in public areas.

The evaluation of the thermal effects of EMF exposure near the readers (in case of exposure in near-field surrounding of EMF source—when manually operated UHF RFID reader is used, or when accidental exposure of an individual who is approaching an autonomous reader) requires the SAR computer simulation. The results obtained by the authors shown that whilst taking the effects of the EMF exposure in the near-field surrounding UHF RFID readers into account, the relevant preventive measures are to be undertaken, with the aim being to ensure sufficient prevention of individuals who may be present there. Applying relevant prevention measures needs to be considered specifically where the RFID reader that emits electromagnetic radiation of over 1 W has been used, or where the vicinity of applied RFID system is accessible for individuals, who may approach to the reader closer than 30% of its reading range.

To conclude, the use of manually operated RFID readers should specifically constitute the focal point of further research on the matter, as well as their prospected installation at the areas accessible by patients and visitors.

Author Contributions: Conceptualization, V.R., O.J.S. and J.A.H.; methodology, V.R., O.J.S., J.K., F.F. and J.A.H.; software, S.S., V.M.F., E.A., M.CE., L.E.R., P.M. and P.Z.; validation, V.R., O.J.S., J.A.H., J.K. and F.F.; formal analysis, O.J.S., E.A., P.Z., M.C.-E. and J.A.H.; investigation, V.R., J.A.H., F.F. and J.K.; resources, V.R., O.J.S. and J.A.H.; data curation, O.J.S. and P.M.; writing—original draft preparation, V.R., J.A.H., O.J.S., S.S., E.A., P.Z., L.E.R., M.C.-E. and P.M.; writing—review and editing, V.R., O.J.S. and J.A.H.; visualization, V.R.; supervision, V.R.; project administration, V.R.; funding acquisition, V.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Instituto de Salud Carlos III project "Electromagnetic "Characterization in Smart Environments of Healthcare, and their involvement in Personal, Occupational, and Environmental Health" (PI14CIII/00056) https://portalfis.isciii.es/es/Paginas/DetalleProyecto.aspx?idProyecto=PI14CIII%2f00056 (accessed on 24 July 2022), and project " (PI19CIII/00033) TMPY 508/19 " Metrics development for electromagnetic safety assessment in healthcare centers in the context of 5G" https://portalfis.isciii.es/es/Paginas/DetalleProyecto.aspx?idProyecto=PI19CIII%2f00033, (accessed on 24 July 2022) from Sub-Directorate-General for Research Assessment and Promotion. The results of a research task (II.PB.15) carried out within the National Programme "Improvement of safety and working conditions" partly supported in Poland in 2020–2022—within the scope of research and development—by the National Centre for Research and Development were also included.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data supporting reported results can be found at https://repisalud.isciii.es/handle/20.500.12105/8365 (accessed on 24 July 2022).

Acknowledgments: Authors special acknowledge for his guidance and all contributions of José Carlos Fernandez de Aldecoa at Hospital Universitario de Canarias, to David Rubio from the Secretary of State for Digital Progress, General Directorate of Telecommunications and Technologies of the information (Madrid, Spain), for his contribution in performing measurements in the semi-anechoic chamber, and to Irene Perán for her technical support with AUTO-CAD works.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Solanas, A.; Patsakis, C.; Conti, M.; Vlachos, I.; Ramos, V.; Falcone, F.; Postolache, O.; Perez-Martinez, P.; Pietro, R.; Perrea, D.; et al. Smart health: A context-aware health paradigm within smart cities. *IEEE Commun. Mag.* **2014**, *52*, 74–81. [CrossRef]
2. Ting, S.L.; Kwok, S.K.; Tsang, A.H.C.; Lee, W.B. Critical Elements and Lessons Learnt from the Implementation of an RFID-enabled Healthcare Management System in a Medical Organization. *J. Med. Syst.* **2011**, *35*, 657–669. [CrossRef] [PubMed]
3. Zeghnoun, A.; Dor, F. *Description du Budget Espace Temps et Estimation de Lexposition de la Population Francaise Dans Son Logement*; Institut de Veille Sanitaire: Lyon, France, 2010.
4. Lopez-Iturri, P.; de Miguel-Bilbao, S.; Aguirre, E.; Azpilicueta, L.; Falcone, F.; Ramos, V. Estimation of Radiofrequency PowerLeakage from Microwave Ovens for Dosimetric Assessment at Nonionizing Radiation Exposure Levels. *Biomed. Res. Int.* **2015**, *2015*, 603260. [CrossRef] [PubMed]
5. Gryz, K.; Karpowicz, J.; Leszko, W.; Zradziński, P. Evaluation of exposure to radiofrequency radiation in the indoor workplace accessible to the public by the use of frequency-selective exposimeters. *Int. J. Occup. Med. Environ. Health* **2014**, *27*, 1043–1054. [CrossRef]
6. de Miguel-Bilbao, S.; Martín, M.A.; Pozo, A.; Febles, V.; Hernández, J.A.; Fernández de Aldecoa, J.C.; Ramos, V. Analysis of exposure to electromagnetic fields in a healthcare environment: Simulation and experimental study. *Health Phys.* **2013**, *105*, S209–S222. [CrossRef]
7. de Miguel-Bilbao, S.; Aguirre, E.; Lopez-Iturri, P.; Azpilicueta, L.; Roldán, J.; Falcone, F.; Ramos, V. Evaluation of Electromagnetic Interference and Exposure Assessment from s-Health Solutions Based on Wi-Fi Devices. *Biomed. Res. Int.* **2015**, *2015*, 784362. [CrossRef]
8. de Miguel-Bilbao, S.; García, J.; Ramos, V.; Blas, J. Assessment of human body influence on exposure measurements of electric field in indoor enclosures. *Bioelectromagnetics* **2015**, *36*, 118–132. [CrossRef]
9. Neubauer, G.; Cecil, S.; Giczi, W.; Petric, B.; Preiner, P.; Frohlichand, J.; Röösli, M. The Association between Exposure Determined by Radiofrequency Personal Exposimeters and Human Exposure; A Simulation Study. *Bioelectromagnetics* **2010**, *31*, 535–545. [CrossRef]
10. de Miguel-Bilbao, S.; Ramos, V.; Blas, J. Assessment of Polarization Dependence of Body Shadow Effect on Dosimetry Measurements in the 2. *4 GHz Band. Bioelectromagnetics* **2017**, *38*, 315–321. [CrossRef] [PubMed]
11. Gryz, K.; Zradziński, P.; Karpowicz, J. The role of the location of personal exposimeters on the human body in their use for assessing exposure to the electromagnetic field in the radiofrequency range 98-2450 MHz and compliance analysis: Evaluation by virtual measurements. *Biomed. Res. Int.* **2015**, *2015*, 272460. [CrossRef] [PubMed]
12. Zradziński, P.; Karpowicz, J.; Gryz, K.; Ramos, V. An evaluation of electromagnetic exposure while using ultra-high frequency radiofrequency identification (UHF RFID) guns. *Sensors* **2020**, *20*, 202. [CrossRef] [PubMed]
13. Ramos, V.; Suarez, O.J.; Febles, V.M.; Aguirre, E.; de Miguel-Bilbao, S.; Marina, P.; Rabassa, L.E.; Suárez, S.D.; Celaya- Echarri, M.; Falcone, F.; et al. Electromagnetic Characterization of UHF-RFID fixed reader in Healthcare centers related to the Personal and Labour Health. *IEEE Access* **2022**, *10*, 28614–28630. [CrossRef]
14. Ramos, V.; Trillo, A.M.; Suarez, O.J.; Suarez, S.; Febles, V.M.; Rabassa, L.E.; Karpowicz, J.; Fernandez-Aldecoa, J.C.; Hernandez, J.A. Electromagnetic Characterization for UHF-RFID Fixed based reader in Smart healthcare environments. In Proceedings of the 2020 International Symposium on Electromagnetic Compatibility—EMC EUROPE, Rome, Italy, 23–25 July 2020; pp. 23–25. [CrossRef]
15. Azpilicueta, L.; Rawat, M.; Rawat, K.; Ghannouchi, F.; Falcone, F. Convergence Analysis in Deterministic 3D Ray Launching Radio Channel Estimation in Complex Environments. *Appl. Comput. Electromagn. Soc. J. (ACES)* **2014**, *29*, 256–271.
16. Azpilicueta, L.; López-Iturri, P.; Aguirre, E.; Vargas-Rosales, C.; León, A.; Falcone, F. Influence of meshing adaption in convergence performance of deterministic ray launching estimation in indoor scenarios. *J. Electromagn. Waves Appl.* **2017**, *31*, 544–559. [CrossRef]
17. Zradziński, P.; Karpowicz, J.; Gryz, K.; Morzyński, L.; Młyński, R.; Swidziński, A.; Godziszewski, K.; Ramos, V. Modelling the Influence of Electromagnetic Field on the User of a Wearable IoT Device Used in a WSN for Monitoring and Reducing Risks in the Work Environment. *Sensors* **2020**, *20*, 7131. [CrossRef]
18. Carranza, N.; Ramos, V.; Lizana, F.H.; García, J.; del Pozo, A.; Monteagudo, J.L. A Literature Review of Transmission Effectiveness and Electromagnetic Compatibility in Home Telemedicine Environments to Evaluate Safety and Security. *Telemed. J. E Health* **2010**, *16*, 530–541. [CrossRef] [PubMed]
19. Carranza, N.; Febles, V.; Hernández, J.A.; Bardasano, J.L.; Monteagudo, J.L.; Fernández de Aldecoa, J.C.; Ramos, V. Patient Safety and Electromagnetic Protection: A Review. *Health Phys.* **2011**, *100*, 530–541. [CrossRef]
20. International Commission on Non-Ionizing Radiation Protection (ICNIRP). Guidelines for limiting exposure to electro-magnetic fields (100 kHz to 300 GHz). *Health Phys.* **2020**, *118*, 483–524. [CrossRef]
21. International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE) 62209-1528-2020. *Measurement Procedure for the Assessment of Specific Absorption Rate of Human Exposure to Radio Frequency Fields from Hand-Held and Body-Worn Wireless Communication Devices—Human Models, Instrumentation and Procedures (Frequency Range of 4 MHz to 10 GHz)*; IEC: Geneva, Switzerland, 2020.

22. International Electrotechnical Commission (IEC) 62209-3:2019. *Measurement Procedure for the Assessment of Specific Absorption Rate of Human Exposure to Radio Frequency Fields from Hand-Held and Body-Mounted Wireless Communication Devices—Part 3: Vector Measurement-Based Systems (Frequency Range of 600 MHz to 6 GHz)*; IEC: Geneva, Switzerland, 2019.
23. Zradziński, P.; Karpowicz, J.; Gryz, K.; Owczarek, G.; Ramos, V. Modelling and Evaluation of the Absorption of the 866 MHz Electromagnetic Field in Humans Exposed near to Fixed I-RFID Readers Used in Medical RTLS or to Monitor PPE. *Sensors* **2021**, *21*, 4251. [CrossRef] [PubMed]
24. European Recommendation. Council of the European Union Recommendation on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz), 1999/519/EC. *Off J. Eur. Commun.* **1999**, *L 199*, 59–70.
25. Celaya-Echarri, M.; Azpilicueta, L.; Aguirre, E.; Lopez-Iturri, P.; de Miguel-Bilbao, S.; Ramos, V.; Falcone, F. Spatial characterization of personal RF-EMF exposure in public transportation buses. *IEEE Access* **2019**, *7*, 33038–33054. [CrossRef]
26. Celaya-Echarri, M.; Azpilicueta, L.; Rodríguez-Corbo, F.A.; Lopez-Iturri, P.; Ramos, V.; Alibakhshikenari, M.; Shubair, R.M.; Falcone, F. Towards Environmental RF-EMF Assessment of mmWave High-Node Density Complex Heterogeneous Environments. *Sensors* **2021**, *21*, 8419. [CrossRef] [PubMed]
27. European Telecommunications Standards Institute (ETSI) EN 302-208 V3.3.1:2020-08. *Radio Frequency Identification Equipment Operating in the Band 865 MHz to 868 MHz with Power Levels up to 2 W and in the Band 915 MHz to 921 MHz with Power Levels up to 4 W.*; Harmonised Standard for Access to Radio Spectrum; ETSI: Sophia-Antipolis, France, 2020.
28. Federal Communications Commission (FCC). *Title 47—Telecommunication, Part 15—Radiofrequency Devices, Section 15.247—Operation within the Bands 902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz*; FCC: Washington, DC, USA, 2010; pp. 825–828.
29. GS1 AISBL. *EPC^{TM} Radio-Frequency Identity Protocols Generation-2 UHF RFID Standard. Specification for RFID Air Interface Protocol for Communications at 860 MHz–960 MHz, Release2.1*; GS1 AISBL: Brussels, Belgium, 2018. Available online: https://www.gs1.org/sites/default/files/docs/epc/gs1-epc-gen2v2-uhf-airinterface_i21_r_2018-09-04.pdf (accessed on 17 August 2022).
30. Zradziński, P.; Tokarski, T.; Hansson Mild, K. The significance of posture-related evaluation of electromagnetic field's influence from hand-operated devices. In *Electromagnetic Ergonomics—From Electrification to a Wireless Society*; Karpowicz, J., Ed.; CRC Press: Boce Raton, FL, USA, 2022.
31. Taflowe, A.; Hagness, S.C. *Computational Electrodynamics: The Finite-Difference Time-Domain Method*, 3rd ed.; Artech House: Norwood, MA, USA, 2015.
32. The European Parliament and the Council of European Union. Directive 2014/53/EU of the European Parliament and of the Council of April 16, 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Text with EEA relevance). *Off J. Eur. Union* **2014**, *L 153*, 62–106.
33. International Electrotechnical Commission (IEC) 62232-2017. *Determination of RF Field Strength and SAR in the Vicinity of Radiocommunication Base Stations for the Purpose of Evaluating Human Exposure*; IEC: Geneva, Switzerland, 2017.
34. International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE) 62704-1:2017. *Determining the Peak Spatial-Average Specific Ab-Sorption Rate (SAR) in the Human Body from Wireless Communications Devices, 30 MHz to 6 GHz—Part 1: General Requirements for Using the Finite-Difference Time-Domain (FDTD) Method for SAR Calculations*; IEC: Geneva, Switzerland, 2017.
35. European Committee for Electrotechnical Standardization (CENELEC) EN 60601-1-2:2015. *Medical Electrical Equipment—Part 1–2: General Requirements for Basic Safety and Essential Performance—Collateral Standard: Electromagnetic Disturbances—Requirements and Tests*; CENELEC: Brussels, Belgium, 2015.
36. The European Parliament and the Council of European Union. Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC. *Off J. Eur. Union* **2013**, *L 179*, 1–21.
37. Carciofi, C.; Valbonesi, S.; Bisceglia, B. Precautionary principle application and 5G development. In Proceedings of the IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Bologna, Italy, 9–12 September 2018; pp. 1192–1196. [CrossRef]
38. European Commission (EC). COM (2000) 1. *Communication from the Commission on the Precautionary Principle*; EC: Brussels, Belgium, 2000.

applied sciences

MDPI

Article

Sing-Ant: RFID Indoor Positioning System Using Single Antenna with Multiple Beams Based on LANDMARC Algorithm

Ping Tan [1], Tinaye Hamufari Tsinakwadi [2], Zhe Xu [3] and He Xu [2,*]

[1] School of Business, Tongda College of Nanjing University of Posts and Telecommunications, Yangzhou 225127, China; tanping5.20@njupt.edu.cn

[2] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; f1020030101@njupt.edu.cn

[3] College of Arts and Science, New York University, New York, NY 10003, USA; zx1251@nyu.edu

* Correspondence: xuhe@njupt.edu.cn

Abstract: RFID localization methods have been widely used in indoor positioning systems (IPS). Most localization techniques involve the use of multiple antennas and the placement of antennas and readers in order to ensure accurate positioning results. However, most localization techniques are complex and require high overhead costs in terms of needing multiple antennas and RFID readers. In this paper, we proposed a method to use a single antenna to perform all the reads and rely rather on the antenna beams to acquire multiple positioning data. A single array of antennas is configured to have multiple angles of operation and rely on different power levels as compared to regular antennas. By manipulating the beam pattern, direction and power, multiple sub-antennas can be conceived and the method utilizes antenna beams and relies mainly on one antenna to realize two-dimensional localization.

Keywords: indoor positioning system; RFID; LANDMARC; two-dimensional localization

Citation: Tan, P.; Tsinakwadi, T.H.; Xu, Z.; Xu, H. Sing-Ant: RFID Indoor Positioning System Using Single Antenna with Multiple Beams Based on LANDMARC Algorithm. *Appl. Sci.* **2022**, *12*, 6751. https://doi.org/10.3390/app12136751

Academic Editor: Jia Liu

Received: 20 May 2022
Accepted: 29 June 2022
Published: 3 July 2022

1. Introduction

Most indoor positioning algorithms are based on the idea of a LANDMARC (Location Identification based on Dynamic Active RFID Calibration) [1] approach to perform localization. LANDMARC uses reference tags in order to increase reader accuracy. Because tags are relatively inexpensive and multiple tags can be placed in one area, the reference tag system with LANDMARC helps to eliminate environmental factors such as weather and particle propagation in free space, because all the tags are subject to the exact same environmental hazards, and hence it can carry the same bias when being implemented. This allows for a more adaptive system and also robust results compared to conventional methods of placing multiple antennas, which also has extremely high costs because RFID readers or antennas are expensive.

For most indoor positioning systems, ultra-high-frequency (UHF) RFID technology is preferred, because the higher frequency allows for a wider read/write spectrum and more metadata of the RFID tag being read, and advanced operations are better supported in the higher-frequency bands. The LANDMARC system has the following three advantages compared to conventional means of RFID localization. First, there is no need for a large number of expensive RFID readers. Instead, it uses additional and cheaper RFID tags. Second, the environmental dynamics can easily be accommodated. The approach helps to offset many environmental factors that contribute to the variations in detected range because the reference tags are subject to the same effects in the environment as the tags to be located. Thus, it can dynamically update the reference information for lookup based on the detected range from the reference tags in real time. Third, the location information is more accurate and reliable. The LANDMARC approach is more flexible and dynamic and can achieve much more accurate and closer to real-time location sensing. Obviously, the placement of readers and reference tags is very important to the overall accuracy of the system. In order to implement LANDMARC, the RFID Electronic Product Code (EPC), which is a unique identifier per RFID tag, and the RSSI value are needed.

The main contributions of this paper are listed in the following:

(1) A single xArray RFID reader is used to detect the location of the target tag by using reference tags and adaptive beam pattern changing. By analyzing the location accuracy of different beam patterns, the larger scale for indoor positioning systems can be achieved.

(2) Optimizations between the effective range, number of reference tags, beam pattern and refresh rate are weighed and their tradeoffs are compared. The results show that the proposed method has a wide positioning range and better positioning accuracy.

(3) The proposed system's superiority is highlighted, especially in its range–accuracy performance. It can be widely used in indoor positioning requirement scenarios, such as libraries, warehouses, and so on.

2. Related Work

Many researchers have brought forward optimizations to the LANDMARC approach in order to stabilize the results and obtain higher accuracy, robustness and depth of operation when implementing localization. These modifications include antenna and reader positioning, such as ANTspin: Efficient Absolute Localization Method of RFID Tags via Spinning Antenna, which introduces a rotary table in the experiment. The reader antenna is fixed on the rotary table to continuously collect dynamic data. When compared with static acquisition, there is more information for localization [2]. Excluding antenna-based optimization approaches, data processing and predictive modeling approaches have been used, such as 3DLRA, which proposes a new three-dimensional localization method based on deep learning: combining RFID absolute location with relative location, analyzing the variation characteristics of the received signal strength (RSSI) and phase, further mining data characteristics by deep learning [3]. Some researchers have applied newer technologies such as ZigBee. ZigBee technology is the main technical index in the transmission, using data information as a carrier. It is widely used in human daily communication transmission. It is of great research value to apply the LANDMARC algorithm to ZigBee technology [4]. Floarea et al. presented a positioning system which uses two widely applied algorithms including Cell of Origin and the LANDMARC approach [5]. Other improvements include the Human Movement-based Relative Localization system, namely HMRL, using passive RFID to achieve accurate relative localization, and even some deep learning-inspired ones, such as advanced LANDMARC with the adaptive k-nearest neighbor algorithm [6–11].

All these improvements highlight how LANDMARC is the cornerstone of most indoor positioning systems (IPS). Using smart bracelets as wearable hardware as a part of the medical IPS is a more appropriate solution because there is a broad choice of this type of device on the market [12]. The VIRE algorithm improves the LANDMARC algorithm by inserting virtual tags evenly between reference tags [13]. Usually, in RFID positioning systems, we need more than one antenna to allow the positioning algorithm to achieve more accuracy. Moreover, some researchers have proposed single antenna-based positioning methods, which are more appropriate to be used in indoor environments. In addition, we can use data mining methods to improve the accuracy of indoor localization algorithms [14] and more sensors can be used for indoor positioning [15]. Wang et al. presented the power-adaptation scheme, which enhanced the positioning accuracy in a single antenna RFID system [16]. In the practical test, as a result of the complex environmental factors and multipath effect, the RSSI value from the RFID system cannot directly reflect the distance between the tag and the antenna. Unlike other RFID-based localization systems, Saab et al. proposed a novel RFID-based methodology which employs a single nonsteered stationary antenna and three passive tags mounted on each object to estimate the location and orientation of objects. This work provides an alternative and relatively cheap approach for remotely estimating the pose of an object [17].

3. LANDMARC Methodology

The implementation of the LANDMARC algorithm mainly starts from creating a mathematical model to classify the antenna and tag relationships, thus creating an array of antenna number rows and RSSI value columns. With each RFID, a successful read tag event contains the corresponding EPC code and the RSSI value. Thus, the needed inputs and parameters for determining the location of the target tag are shown below:

n—number of RF readers;
m—tag to be used as reference tag;
u—the target tags that will be tracked;
S—$(S_1,\ S_2,\ \ldots,\ S_n)$ S_i denotes the RSSI of each target tag highlighted by each reader i;
$\theta^{-}(\theta_1,\ \theta_2,\ \ldots,\theta_n)$ θ_i denotes the signal strength.

With these values and parameters, we can then calculate the Euclidian distance vector per RFID tag and antenna, and the resultant vector would be the Euclidian distance for reference tags and target tags. Suppose that in an indoor room, there are evenly spaced reference tags and readers, and the tags to be tested are randomly distributed indoors. The matrix of signal strength values measured by the reader for each reference tag [4] is:

$$S = \begin{matrix} S_{11} & S_{12} & \cdots & S_{1n} \\ S_{21} & S_{22} & \cdots & S_{2n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ S_{m1} & \cdots & \cdots & S_{mn} \end{matrix} \tag{1}$$

where S_{mn} represents the signal strength of the n-th reference tag measured by the m-th reader [4]. The reader measures the signal strength matrix of the tag under test, where T_{mu} represents the signal strength of the u-th tag to be detected by the m-th reader [18].

$$T = \begin{matrix} T_{11} & T_{12} & \cdots & T_{1u} \\ T_{21} & T_{22} & \cdots & T_{2u} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ T_{m1} & \cdots & \cdots & T_{mu} \end{matrix} \tag{2}$$

The magnitude of the spacing between the label is to be tested, and also the LANDMARC is used as our reference point, which will be determined by the Euclidian distances of the vector. The Euclidian distance of the vector is calculated as E_{ij}. This is the distance between the i-th reference label and also the j-th label to be located [18].

$$E_{ij} = \sqrt{\sum_{k=1}^{n}\left(T_{ik} - S_{jk}\right)^2 (i = 1, 2\cdots u; j = 1, 2\cdots n)} \tag{3}$$

For each target to be measured, we need find the k nearest reference labels. According to the distance between the k reference labels and the label to be tested, the weight coefficient occupied by each reference label is as shown below:

$$w_i = \frac{\frac{1}{E_i^2}}{\sum_{i=1}^{k}\left(\frac{1}{E_i^2}\right)} \tag{4}$$

where w_i represents the weight coefficient of the k nearest reference labels of the label to be tested. In order to find the nearest reference tag to the tracking tag, we can use the coordinate of the reference tag with the smallest E value as the unknown tag's coordinate. It can be called the 1-nearest neighbor algorithm [18]. Unlike conventional LANDMARC approaches, when using antenna beams, the accuracy can vary because of differences when switching between antenna beams, and its positioning is an independent value; hence, finding the equilibrium point between the number of reference points and also the accuracy and range relationship is the key problem.

4. Proposed Sing-Ant Methodology

In our method, we use the Impinj xArray Reader, where the antenna used is able to produce 52 beams, albeit sequentially, which means that only one antenna can be accessed at a time. Though the xArray gateway reader already has wide-area monitoring, there are some setbacks which need improvement. In this paper, with our proposed method and implementation, the following questions can be solved.

(1) The first issue of xArray is a lack of environmental adaptability. Because there are no reference tags, the existing model cannot factor in the effects of the environment. Thus, when we use the LANDMARC approach, there is no weather bias since all the tags are subject to the exact same weather conditions.

(2) Due to the fluctuating nature of RFID tag reads, the current RFID positioning system is highly unstable; usually, the location of the target tags is changed with every antenna beam change. This is solved by having clusters and sectors of antennas, which are more accurate, and also reference tags are used for positioning, so there is less fluctuation.

(3) In addition, the operation range can be extended depending on the degree of accuracy required by changing the number of neighbors and reference tags used. The current xArray reader has a fixed location sensing algorithm that cannot factor in the dynamism of different working environments without the use of reference tags.

The proposed method has the following settings for the xArray reader: the antenna read pattern, unless manually configured, always reads in ascending order. The first four make up the core center of the reading range, with each beam occupying almost a quarter of the central sphere. The rest of the beams are divided into circular rings around these four core beams, and the ring of beams consists of 8 antenna beams. Each ring expands outwards beyond the circle, forming circular as well as linear sections inside the overall functioning area. The ring and central core will be labeled as a cluster, whilst the combinations of linear beams being displaced further from the core will be named sectors. The first four antennas make up the core. This combination of the core and its sectors and clusters, respectively, will be the one used to locate tags in free space. Various combinations of arrangement and weighing will lead to better results and higher accuracy, at the same time accommodating longer ranges without any additional overhead.

4.1. Central Core

The central core plays a unique role in determining the location tag and accuracy of the IPS system. Due to the sequential activation of antennas, it will be the first group of beams to determine the position of the target tag. Moreover, it is the only beam combination that effectively scans the center of the effective area when the antenna is activated; hence, there is need to ensure that it is fully functioning. It is made up of four beams, all of them being perfectly symmetrical along the x-axis and y-axis. Hence, it has to be considered when working with the central antenna and in order to accommodate multiple scenarios and read events. The average wake time for any antenna beam is around 1.25 s, and there is a direct relationship between the number of scans of a system and also the distance from the main antenna. The core antenna beams of the Impinj xArray reader are shown in Figure 1, which shows that 4 antenna beams are used in our methods.

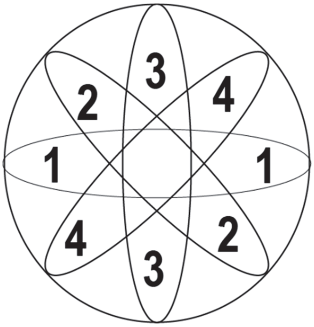


Figure 1. Core antenna beams of Impinj xArray reader.

4.2. Antenna Clusters

Antenna clusters are made up of the outer centric rings of antenna beams that surround the core and they are made up of 8 antenna beams, all scanning successively one after the other. The cluster's area of operation increases with each cluster, and as the circular area of coverage grows after each antenna is finished. Due to the large number of antennas, the sectors tend to have higher reliability and outrange the core. The mathematical operations required to work on the clusters are identical to the operations needed by the core. The structure of all the antenna cores is shown in Figure 2, where shows the examples of antenna clusters on the left side of the image, and a single isolated core is shown on the right side.

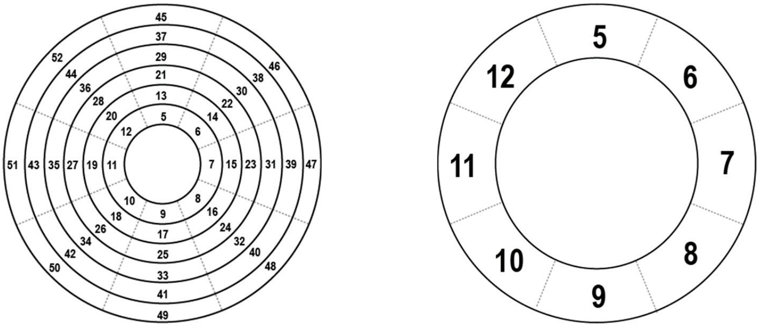


Figure 2. All antenna clusters (**left**) and a single antenna cluster (**right**).

Figure 2 shows that the antenna clusters are rings around the core. They are adept at determining the location of the target tag due to their lack of polarity, because, whilst they contain the same spread as the core cluster in that they calculate the difference in direction at 45° angles, they do not suffer from the same polarity drawbacks as the core does, and hence they can locate the target tag without having to be optimized.

4.3. Antenna Sectors

The antenna sectors protrude linearly outward from the core and are adept at measuring the distance from the core. They are composed of antenna beams that are protruding outwards from the core and are displaced in a line. They are made up of columns of antenna beams. Through the pattern in Figure 3, the entire sectors in our target area and a single isolated sector are shown. The mathematical calculation remains the same as for the central core and antenna cluster, with the only variations being in the number of antenna beams used by each single sector. The sectors of all antennas and a single antenna are shown in Figure 3.

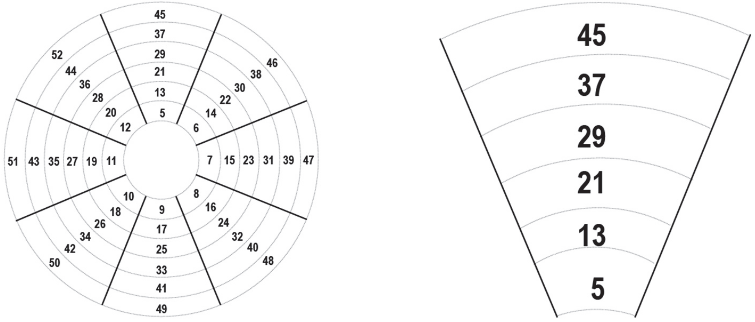


Figure 3. All antenna sectors (**left**) and a single antenna sector (**right**).

Figure 3 shows that the lines of the antennas are spreading straight upwards and hence this method allows for easier calculation of the *y*-axis spread as compared to clusters in which it is necessary to compare entire clusters in order to find the ideal point.

When handling clusters, the main challenge is the lack of sequential activation; it can be seen that they have a rather arbitrary antenna beam selection count, and these sequences appear at inconsistent intervals for the sequential calculation of a tag location. Hence, when working with antenna sectors, the position of the target tag relative to the sectors being measured must be calculated.

5. Design and Implementation of Sing-Ant

The main goal of the proposed system is to allow the accurate prediction of the location by using a combination of passive RFID reference tags via the LANDMARC approach and also use multiple antennas to better perceive the depth and different orientations of distance from the center. Therefore, this proposed system would allow for more accurate localization as it utilizes antenna positioning and also reference tags in order to narrow down the precise location of the target tag. The details of our proposed method are as follows.

From Equations (1) and (2), we can obtain multiple sub-matrices of the Euclidian distance between the target tag and the total number of reference tags, which are all mapped to the corresponding antenna that is being read. In order to make meaningful sense of the data, we split them into three calculations in order to best determine the mathematical model used to calculate the outcome. The three main calculation models are core, sector and cluster.

Since each of these calculations uses different configurations individually, which might be unable to accurately predict the location of the target tag, this can narrow down the location by focusing on their major advantages and lessening the disadvantages of the other systems. The core is ideal when tags are displaced near the center of the effective area of operation. Thus, when calculating the location of the target tag near the center, the first task is to create a reference list of all the tags that need to be scanned and create a custom RFID tag filter in order to limit reads, and hence devote more resources to the target tags and also allow higher read event success by limiting unwanted cards. This can be easily implemented by the use of a HashMap filter. The block diagram for filtering out unwanted tags is shown in Figure 4.

After tag filtering is finished, the next step is to choose the best values per antenna beam in order to select a single value to represent the RSSI. Because the RSSI is a fluctuating value that is highly inconsistent, in one antenna activation cycle, if the distance is close enough, we can obtain an average of 15 successful tag reads. The values, however, are sinusoidal in nature, and hence multiple mathematical modeling techniques can be used to filter the EPC values obtained, and the values are smoothed to be considered for calculation. Figure 5 shows the oscillating values of EPC. One of the easiest and most primitive methods to stabilize the results is to consider only those above or below the minimum and maximum average. This forces the final results to either be floor results or ceiling results. Throughout this test, the results are used. If only one EPC RSSI value is needed, then the maximum RSSI value per antenna beam cycle can be chosen.

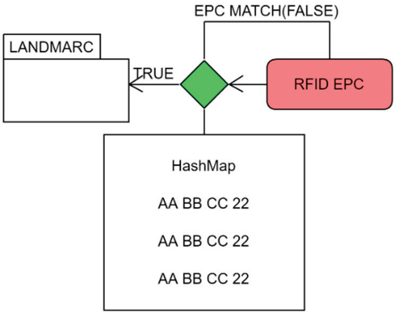


Figure 4. Card filter implementation.

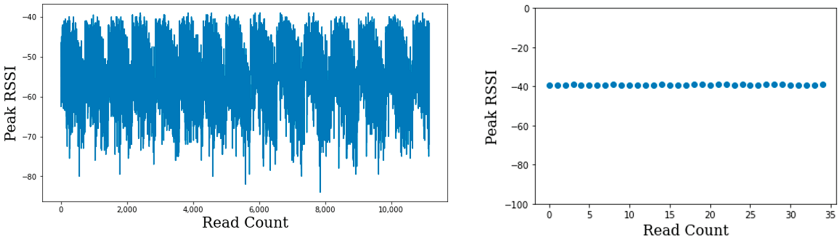


Figure 5. Received RSSI values (**left**) and filtered RSSI values (**right**).

In Figure 5, the two diagrams show how we can parse the received RSSI values in order to accommodate and allow for steadier and linear results; by choosing either the floor or the ceiling threshold, we can obtain fewer conflicting data. During the calculation, we deferred to the ceiling values as they showed the highest possible RSSI per RFID tag. In an ideal situation, lower RSSI values would arise from tags at a further distance. However, in the practical test, as a result of the complex environmental factors and multipath effect, the RSSI value from the device could not directly reflect the distance between the tag and the antenna [16]. Some RSSIs of reference tags and tags to be tested can be grouped into theoretical values and measured values according to different formulas [18]. The results can be logged to allow for further study, such as for deep learning models of estimation. The main idea behind position estimation via mapping techniques is to determine a regression scheme based on a set of reference tags' data, and then to estimate the position of a given node according to this regression function [19]. Whilst the results are pseudo-periodic, there is visible randomness. Due to the great interference brought by complex indoor channel environments to the wireless signal propagation, the RSSI value of tags appears to undergo random fluctuations [20].

When collecting the tag data and preparing to place them into our calculation matrices, it is necessary to account for unsuccessful tag read events. These are events whereby there is no RSSI value returned after an antenna beam has been activated and eventually deactivated. Null values can be handled in three ways depending on preference. They are listed as follows: omission, zero padding and infinity padding.

Omission simply requires the removal of all the data with missing values and instead using only fully read antenna matrices. Zero padding works by replacing the missed RSSI values with zero instead when they are not read. In infinite padding, if there is no read event, then a large number is used instead; the number has to be large enough to render the Euclidian distance value trivial.

In order to calculate multiple scenarios at one time, we wait for one cycle to complete and then record all the entries from one RFID reader cycle consisting of all the reference tags, target tags and their respective antenna beam RSSI value; the ideal resultant matrix would be split into two. The first matrix shows the antenna beam number and the RSSI of the reference tag.

$$S = \begin{bmatrix} S_{11} & S_{11} & \cdots & S_{1A} \\ S_{21} & S_{22} & \cdots & S_{2A} \\ \vdots & \vdots & \vdots & \vdots \\ S_{M1} & S_{M2} & \cdots & S_{MA} \end{bmatrix} \tag{5}$$

Defining the signal strength of the tag to be tested as a matrix S, S_{ij} (i = 1, 2 ... M, j = 1, 2 ... A) represents the RSSI value of tag i to be located and read by the antenna j [2]. The actual targets will also have their own matrix, mapped out in a similar nature to the original shown here. Therefore, in the event of having only one antenna tag as the target, it will be a vector matrix instead. This will be a regular occurrence, especially when trying to locate only one tag. Lastly, the matrix will appear as shown below:

$$\theta = \begin{bmatrix} \theta_{11} & \theta_{12} & \ldots & \theta_{1A} \\ \theta_{21} & \theta_{22} & \ldots & \theta_{2A} \\ \vdots & \vdots & \vdots & \vdots \\ \theta_{N1} & \theta_{N2} & \ldots & \theta_{NA} \end{bmatrix} \tag{6}$$

Defining the signal strength of the reference tag as a matrix θ_{ij} (i = 1, 2, N, j = 1, 2, ... A) represents the RSSI value of the reference tag i read by the antenna j [5]. We then followed up with the standard LANDMARC protocol for calculating the Euclidian distances and the value with the lowest figures represents the reference tag that is closest to our target tag. However, this is merely the beginning of our calculative process. Consequently, we need to optimize it for range and also direction, so we set antenna clusters and sectors in order to narrow down and fine tune the actual location and also attain better precision with less tags and a wider range. Thus, for the second phase of calculations, we assume that our input values are a row in a matrix T that contains all the Euclidian distances for the target matrix. For all reference points, we can have a corresponding matrix as shown. For example, if we have 5 reference points, then we can use 5 matrices representing this antenna beam, landmark and target tag matrix. By comparing the relationships and values between each antenna and the reference tags, we can assess the location of the tags by using similar amounts of reference tags.

$$T = \begin{bmatrix} T_{11} & T_{12} & \cdots & T_{1N} \\ T_{21} & T_{22} & \cdots & T_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ T_{M1} & T_{M2} & \cdots & T_{MN} \end{bmatrix} \tag{7}$$

With each value representing the Euclidian distance and the antenna beam towards it, we can assess which combination of read values better reflects the actual position of the tag, even at further ranges than normal. We can assign each antenna beam a pseudo-landmark, and the pattern configuration is shown in Figure 6.

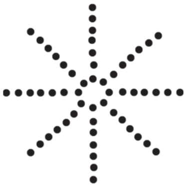


Figure 6. Antenna scatter plot.

Thus, for the wide-range approach, we propose a single neighbor approach, meaning that the reference tag with the lowest Euclidian distance per antenna cluster, core and sector will be assigned as the location.

6. System Deployment

With a functional mathematical model, the implementation was carried out in a standard lab room in open space. Our proposed design consists of one Impinj xArray Gateway RFID Reader located at the highest point (usually hanging from the ceiling) in our lab and the reference tags located on the floor. For the reference tags, we mapped them out in a square matrix arrangement of *n* * *n*, and each reference tag was assigned a location value for the first test of a wider range with less accuracy. For the experiments, since we used one neighbor, there was no need for weight adjustment and hence we could use the actual reference tag as the location. Since the Impinj xArray reader is a fixed infrastructure RFID reader, we used its SDK and low-level-reader protocol to change its mode and configure it to work in wide monitoring scenarios.

For the reference tags, we chose UHF passive RFID cards. The tags were passive tags, meaning that they did not have an independent power source and they relied entirely ion the reader for their power. The main reason for choosing UHF tags the read range, which is the largest compared to other tags, as shown in Table 1.

Table 1. Frequency and range comparison.

Tag Type	Frequency Range	Read Distance
Low frequency (LF)	120–140 kHz	10–20 cm
High frequency (HF)	3–30 MHz	10–20 cm
Ultra -high frequency (UHF)	869–928 MHz	3 m

Table 1 clearly shows that the higher the frequency, the longer the read range. We set RFID reference tags almost in a standard square manner and each passive tag represented a set coordinate point ranging from X $(X = 1, 2, \ldots, x)$ and Y $(y = 1, 2, \ldots, y)$. The final reference tag's location would be the coordinates from the two values. Thus, if our target tag was located at the bottom right corner (with respect to the antenna reader) of the room, then the location entry would be validated as $l = (x, y)$, with the two values being the maximum values of row and column length, respectively.

$$l = \begin{bmatrix} l_{11} & l_{12} & \cdots & l_{1y} \\ l_{21} & l_{22} & \cdots & l_{2y} \\ \vdots & \vdots & \vdots & \vdots \\ l_{x1} & l_{x2} & \cdots & l_{xy} \end{bmatrix} \tag{8}$$

Thus, depending on the accuracy and range, we could determine the overall location. Moreover, for finer locations and pinpointing exact coordinates, we can use more neighbors and then obtain weights for each reference tag; upon obtaining the weights, we can then simply place the location points using the weighted value. This would be practical for finer location values, but considering the abundancy and relative price of passive RFID tags, being cheap, we can afford to instead simply use multiple RFID tags. When the final setup is made, the arrangement will resemble Figure 7.

The UHF RFID tag has 4 memory banks, and they are the Electronic Product Code (EPC), user memory, reserved memory and tag identifier memory (TID). To identify the tags in the most efficient way possible, we configured our antenna as shown in Table 2.

Once the EPC and RSSI values were matched, we obtained the corresponding matrix of reference and target tags. Then, we started to calculate the Euclidean distances of the target tag with respect to the landmarks. The distances were calculated using the following formula below:

$$E_j = \sqrt{\sum_{i\ =1}^{n} (\theta_i - S_i)^2} \tag{9}$$

where $j \in (1,\ \ m)$ is the Euclidean distance in signal strength between a tracking tag and the reference tag r_j. Let E denote the location relationship between the reference tags and the tracking tag, i.e., the nearer the reference tag to the tracking tag, the smaller the E value. Upon acquiring the Euclidian distances, we could use the number of neighbors to calculate the location of the tags. If we use one neighbor, then the tag with the lowest values means that it has the highest correlation with the target tag, and it is designated as the location of the target tag. However, if we use multiple reference tags and use more than one neighbor to determine the location of our RFID target tag, then we use the formula below to acquire the exact location of the target tag.

$$(x, y) = \sum_{i=1}^{k} w_i (x_i,\ \ y_i) \tag{10}$$

The value of w_i refers to the factor of weight provided by the i-th nearest neighbor of the system; the weights are another independent design parameter but can be factored in when there is a need to obtain two-dimensional coordinates in a pseudo-linear nature as compared to simply using a single reference tag as our location point. The weight formula is calculated as shown below.

$$w_j = \frac{\frac{1}{E_i^2}}{\sum_{i=1}^{k} \frac{1}{E_i^2}} \tag{11}$$

This approach provided the least error in most of the experiments, which means that the reference tag with the smallest E value has the largest weight. This may be explained by the fact that the signal strength is inversely proportional to the square of the distance. Note that our approach can be easily extended to a three-dimensional coordinate [3]. As compared to other algorithms such as tri-lateration, which is a method that can find the coordinates of a sensor node, the sensor coordinates are the intersection point of three of the anchor nodes, and the intersection point is known as a localized node [11].

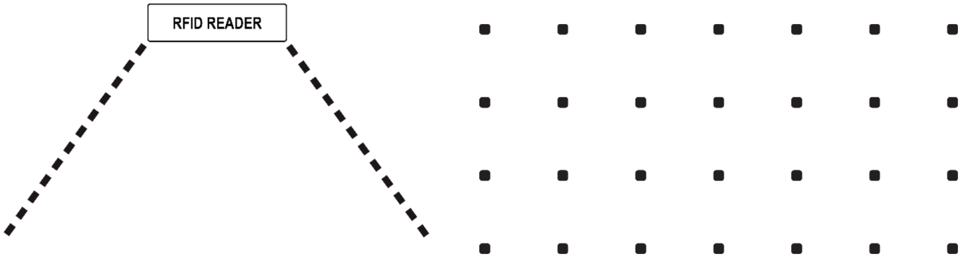


Figure 7. The mounted RFID reader (**left**) and the LANDMARC tags (**right**).

Table 2. Impinj xArray antenna configuration.

Configuration Setting	Value
setIncludeAntennaPortNumber	TRUE
setIncludePeakRSSI	TRUE
setIncludeCRC	TRUE
AntennaEnable	ALL

7. Results and Discussion

With the implementation of RFID mapping, the result is the physical layout. The first result when mapping out the coordinates was the relationship between the number of reference tags and the overall accuracy of the system. Having kept our lab operating area size constant, we discovered that, for the 1-Nearest Neighbor approach, the highest accuracy was obtained when we had the least amount of reference tags. Because of the higher polarization between antenna RSSI values, there is maximum displacement of landmark tags. Table 3 shows the results.

Table 3. The accuracy of tags in 1-Nearest Neighbor approach.

Number of Reference Tags	Positioning Accuracy
4	99.1
9	93.4
16	89.7
25	78.1

Table 3 shows that without adjusting for weights, high accuracy becomes much more difficult to obtain, and also sometimes, when the target tag is placed perfectly between the reference tags, then problems of multiple tags with very similar Euclidian values arise.

From Table 3, we can see that there is a tradeoff in 1-Nearest Neighbor, so considering multiple neighbors is an appealing approach, because there are some incorrect readings in the neighborhood of the correct one.

7.1. Antenna Beam Path Optimization

Having obtained all the data from our antennas and completed one full antenna cycle from beam 1 to 52, we can begin optimizations to smooth out the results that we obtain and allow for even higher levels of optimization. Instead of applying the weights on our RFID tags, we can instead use our antennas and their corresponding RSSI values to determine the rough location and improve the result from our reference tags. To do this, we sacrifice finer accuracy (usually around 10 cm) and instead compensate with range (more than 2 m from the reader). This distance creates a buffer for smaller margins of error and allows the use of fewer RFID cards to obtain the course location of the target tag via the 1-Nearest Neighbor approach; we can then optimize the results and map them out using the antenna clusters and sectors instead.

Starting with our clusters, in order to determine the sector of highest correlation with our reference tags, we create nested Euclidian vectors. The first is the vector matrix of each cluster *C* and each sector having the same Euclidian vector matrix.

$$C = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ \vdots \\ C_8 \end{bmatrix} \quad S = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ \vdots \\ S_6 \end{bmatrix} \tag{12}$$

Thus, in order to determine the location of the target tag, we first choose the highest correlation of the Euclidian value cluster. This will give the closest distance from the core. We perform a similar operation with the sectors and whichever pair of sector and cluster yield the highest values, which become the target RFID tag location point. Then, we cross-reference with our standard LANDMARC approach in order to validate the results, and if the selected antenna beam is in the neighborhood of our target tag, then we designate the localization event. As the graph below shows, the narrowing optimization is based on sectors and clusters.

The main aim of single antenna use for RFID localization is to improve the following features that preexisting models are unable to provide:

(1) Widen the range of effective scanned area;
(2) Maintain low RFID reader overhead;
(3) Use a single fixed antenna.

Our system stands out by using a single antenna and also relying on successive antenna beam shifting in order to predict the final results. Regarding its limitations, firstly, there are some blind spots from the antenna diagram as we can clearly see in the core that some areas are not covered by the antenna. Moreover, because only one beam can be active at one time, this means that we cannot obtain simultaneous real-time values as compared to conventional models that use multiple antennas in their setup. Thus, when predicting the model, a good amount of accuracy is traded off, especially working with the sector. Due to their irregular calculation scheme, they can only be fully utilized once a complete cycle (beam 1 through 52) of changing antenna beams has been completed. This means that other systems operate faster than ours because, on average, one complete antenna beam cycle will cost, on average, 0.4 s; hence, overall, we can obtain all results after more than 40 s. The core and sectors are used for LANDMARC location prediction whenever their beams are finished and data are collected. Then, the overall location is checked twice with the results. Therefore, the location refresh rate is refreshed much faster depending on the user configuration. Below, we present a list of the refresh times depending on how many sectors and clusters are being used altogether. Distance was increased or decreased to analyze the change in the relative positioning accuracy [3]. Whilst there was a slight drop in the tag count, overall, the number of successful tag reads was high enough to be equally as adequate as closely placed tags. As long as the target tags are in the effective range, then they will not affect the refresh rate. Table 4 shows the results of different clusters used.

Table 4. Refresh rate.

Components Used	Refresh Rate
Single core	3.2 s
1 core + 1 cluster	9.6 s
1 core + 2 clusters	16 s
1 core + 3 clusters	22.4 s
1 core + 4 clusters	28.8 s
1 core + 5 clusters	35.2 s
1 core + 6 clusters	41.6 s
1 core + 6 clusters + All sectors	>45 s

7.2. Model Comparison

The proposed method allows us to flexibly choose an adaptive refresh rate because we need minimal system tweaking and only adjust when the end system gives the location feedback. This should allow the setup to operate in real time and also allow it to operate on par with other systems.

There are many more comparative advantages of using this system compared to others and, as can be seen from the table below, the results are clear. With a proper cost–benefit analysis, our system surpasses several more systems and can be applied in industrial settings. The only trade-off would be accuracy for range and also its three-dimensional capabilities stripped away in return for maintaining the use of one antenna. However, these methods are not mutually exclusive and hence can be combined to work together—for example, allowing a different system to have multiple phases of operation. An example is the COCKTAIL algorithm. COCKTAIL is a more comprehensive localization algorithm. It also runs in two phases. The first phase is the same as the SA phase of SA-LANDMARC, which aims to determine a subarea where the target object exists [21]. These results can also be logged to allow for deep learning to distinguish and observe any hidden patterns, as when deep CNN is applied to RFID multi-tag localization with the joint fingerprint features of the RSSI and the phase difference of arrival (PDOA). The CNN for RFID localization has great advantages, such as the capability of processing a large amount of data, extracting and training fingerprint features, sharing the parameter structure and reducing the complexity of the neural network [22]. The model comparison results are shown in Table 5.

Table 5. Model comparison.

RFID Localization Method	3D Positioning	Fixed Antenna Position	Single Antenna Exclusively	High Accuracy of Positioning	Effective Radius
LANDMARC	✔			✔	2–3 m
ANTspin	✔		✔	✔	0.6 m
3DLRA	✔	✔		✔	0.53 m
Zigbee	✔	✔		✔	10 m
Deviation Correction	✔	✔		✔	1.5 m
WIMEC-LANDMARC	✔	✔		✔	2.5 m
Sing-Ant		✔	✔	✔	>5 m

7.3. ItemTest vs. Sing-Ant

The Impinj xArray reader already comes with an inbuilt location sensing algorithm that is accessible through ItemTest, their default application for connecting the reader. This, however, cannot be compared to the multiple advantages that Sing-Ant possesses. Firstly, there is environmental bias in the ItemTest location method due to a lack of reference tags, so when deploying, one has to factor in the environment to operate. Sing-Ant overcomes this by using reference tags, since they carry the same environmental bias as the target tags. Secondly, the stability of target location is greatly improved. Because ItemTest recalculates the position after every beam change, its position is always shifting, even if the target tag has not moved, and there are always shifting changes. Due to the nature of recalculating the position of each tag entry, it is scanned every time. Because of the margin of error when reporting analog values, we notice that every update event log ends up shifting the position of the tag, even when stationary, whereas, with Sing-Ant, unless the displacement is large enough to move the target tag near another landmark, the location values remain constant. Third, there are redundant entries when using ItemTest. Because it recalculates the position after every successful tag report event, a single beam can choose over five entries from the same tag, and the result is needless overcalculation, which reduces the robustness. Meanwhile, with Sing-Ant, only after a cluster, core or sector has been finished is the location calculated. Thus, when multiple entries are noticed, only one is used for calculation. This helps to stabilize the final results as unnecessary entries are not considered. Some of the key differences are shown in Table 6.

Table 6. System comparison of ItemTest and Sing-Ant.

Feature	Sing-Ant	ItemTest
Environmental bias	No	Yes
Location update	Per cluster/sector cycle	Per beam change
Accuracy rate	Constant	Varies per entry
Variable refresh rate	Yes	No

8. Conclusions

In this paper, we have presented a novel single-antenna RFID localization system based on the LANDMARC method, which reduces the number of neighbors to improve the traditional positioning mechanism. By having only one nearest neighbor, it defaults the actual tag location to a point near the reference tag and allows the system to keep its high accuracy. This is especially useful for workspaces where the exact location is not needed, such as warehouses. Optimization based on beam patterns was used, along with their refresh rate. This study makes use of a single antenna for RFID localization and establishes an adaptive equilibrium point between range and accuracy whilst using a reasonable error, which can be applied in indoor positioning systems. Our future research includes depth estimation and fully 3D positioning with a single antenna in RFID systems.

Author Contributions: Conceptualization, P.T. and T.H.T.; methodology, P.T.; data curation, P.T.; writing—original draft preparation, P.T. and T.H.T.; writing—review and editing, Z.X.; supervision and project administration, H.X.; funding acquisition, P.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by the Project of Philosophy and Social Science Research in Colleges and Universities in Jiangsu Province of China (No. 2020SJA2389), in part by the Scientific Research Fund of Tongda College of Nanjing University of Posts and Telecommunications (No. XK205XS20001), in part by the Scientific and Technological Support Project of Jiangsu Province (No. BE2019740) and the University-Industry Collaborative Education Program (No. 202102210003).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The tag event data will be posted on GitHub alongside the Sing-Ant code.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ni, L.M.; Liu, Y.; Lau, Y.C.; Patil, A.P. LANDMARC: Indoor location sensing using active RFID. In Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003. (PerCom 2003), Fort Worth, TX, USA, 26 March 2003; pp. 407–415.
2. Shen, L.; Zhang, Q.; Pang, J.; Xu, H.; Li, P.; Xue, D. ANTspin: Efficient Absolute Localization Method of RFID Tags via Spinning Antenna. *Sensors* **2019**, *19*, 2194. [CrossRef] [PubMed]
3. Cheng, S.; Wang, S.; Guan, W.; Xu, H.; Li, P. 3DLRA: An RFID 3D indoor localization method based on deep learning. *Sensors* **2020**, *20*, 2731. [CrossRef] [PubMed]
4. Zhang, Y.; Li, B. Improvement of LANDMARC Algorithm Based on ZigBee Technology. In Proceedings of the 2020 International Conference on Microwave and Millimeter Wave Technology (ICMMT), Shanghai, China, 20–23 September 2020; pp. 1–3.
5. Floarea, D.; Sgârciu, V. Indoor positioning using Cell of Origin and LANDMARC approach. In Proceedings of the 2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 25–27 June 2020; pp. 1–5.
6. Wang, G.; Qian, C.; Shangguan, L.; Ding, H.; Han, J.; Yang, N.; Xi, W.; Zhao, J. HMRL: Relative localization of RFID tags with static devices. In Proceedings of the 2017 14th Annual IEEE International Conference on Sensing, Communication and Networking (SECON), San Diego, CA, USA, 12–14 June 2017; pp. 1–9.
7. Chawla, K.; Robins, G.; Zhang, L. Object localization using RFID. In Proceedings of the IEEE 5th International Symposium on Wireless Pervasive Computing 2010, Modena, Italy, 5–7 May 2010; pp. 301–306.
8. Hahnel, D.; Burgard, W.; Fox, D.; Fishkin, K.; Philipose, M. Mapping and localization with RFID technology. In Proceedings of the IEEE International Conference on Robotics and Automation, New Orleans, LA, USA, 26 April–1 May 2004; Volume 1, pp. 1015–1020.
9. Wu, X.; Deng, F.; Chen, Z. Rfid 3D-landmarc localization algorithm based on quantum particle swarm optimization. *Electronics* **2018**, *7*, 19. [CrossRef]
10. Han, K.; Cho, S.H. Advanced LANDMARC with adaptive k-nearest algorithm for RFID location system. In Proceedings of the 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, Beijing, China, 24–26 September 2010; pp. 595–598.
11. Ahmed, A.T.; Rashid, A.N.; Shaker, K. Localization in Wireless Sensor Network. *Webology* **2022**, *19*, 692–704. [CrossRef]
12. Pospelova, I.V.; Cherepanova, I.V.; Bragin, D.S.; Sidorov, I.A.; Kostyuchenko, E.Y.; Serebryakova, V.N. The Estimation of the Potential for Using Smart-Trackers as a Part of a Medical Indoor-Positioning System. *Electronics* **2022**, *11*, 107. [CrossRef]
13. Yan, J. Improved Algorithm for RFID Indoor Positioning. *Adv. Comput. Signals Syst.* **2021**, *5*, 48–54.
14. Toro, U.S.; Yakub, N.A.; Dala, A.B.; Baba, M.A.; Jahun, K.I.; Bature, U.I.; Hassan, A.M. A Survey of Data Mining Techniques for Indoor Localization. *Int. J. Eng. Manuf.* **2021**, *6*, 19–35.
15. Bragin, D.; Kostyuchenko, E.; Faerman, V.; Kobzev, A.; Sidorov, I. Comparison of technologies of local patient positioning. *Int. J. Adv. Res. Technol.* **2021**, *12*, 362–386.
16. Wang, Z.; Xuan, A.; Liu, Z.; Alfadhl, Y. Research on RFID Positioning Algorithm with Single Antenna. In Proceedings of the 2019 8th Asia-Pacific Conference on Antennas and Propagation (APCAP), Incheon, Korea, 4–7 August 2019; pp. 34–38.
17. Saab, S.S.; Msheik, H. Novel RFID-Based Pose Estimation Using Single Stationary Antenna. *IEEE Trans. Ind. Electron.* **2016**, *63*, 1842–1852. [CrossRef]
18. Wang, D.; Su, Y.; Leng, Z.; Qi, Y. Optimization of Radio Frequency Identification Reference Tag Location Algorithm Based on Back Propagation Neural Network. In Proceedings of the 2021 6th Asia Conference on Power and Electrical Engineering (ACPEE), Chongqing, China, 8–11 April 2021; pp. 537–541.

19. Hou, Z.; Li, F.; Yao, Y. An improved indoor UHF RFID localization method based on deviation correction. In Proceedings of the 2017 4th International Conference on Information Science and Control Engineering (ICISCE), Changsha, China, 21–23 July 2017; pp. 1401–1404.
20. Liu, L.; Qiao, J.; Liu, R.; Wang, Z. Reseach on Optimization of RFID Indoor Positioning Algorithm Based on RSSI. In Proceedings of the 2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2), Taiyuan, China, 22–24 October 2021; pp. 3386–3390.
21. Zhang, D.; Lu, K.; Mao, R. A precise RFID indoor localization system with sensor network assistance. *China Commun.* **2015**, *12*, 13–22. [CrossRef]
22. Peng, C.; Jiang, H.; Qu, L. Deep convolutional neural network for passive RFID tag localization via joint RSSI and PDOA fingerprint features. *IEEE Access* **2021**, *9*, 15441–15451. [CrossRef]

applied sciences

MDPI

Article

Simulation of Radio Signal Propagation for UHF RFID Technology in an Indoor Environment Using Ray Tracing (Graphics) Method

Tomas Straka, Lukas Vojtech and Marek Neruda *

Department of Telecommunication Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 2, 16000 Prague, Czech Republic; strakto2@fel.cvut.cz (T.S.); lukas.vojtech@fel.cvut.cz (L.V.)
* Correspondence: marek.neruda@fel.cvut.cz

Abstract: RFID systems are often used in industry to reduce costs, increase process efficiency and minimize human intervention. The challenge is to design an RFID system before it is implemented in a specific environment in the shortest possible time and at minimum cost while maintaining the accuracy of the results. In this paper, a new approach to predicting indoor UHF RFID signal coverage is presented. It is based on a graphical ray tracing method. Simulations are performed based on spatial analysis of the illumination of a 3D indoor environment created from a 2D floor plan. The results show a heat map representing the predicted RSSI radio signal levels using a color range. The approach is validated by comparison with the results of the empirical Multi-Wall model. The time complexity of the approach is presented. The proposed approach is able to generate a heat map with the accuracy of the empirical Multi-Wall model. The interior room equipment required to refine the results ought to be investigated in the future.

Keywords: 3D visualization; indoor propagation prediction; ray tracing; RFID; signal representation; simulation; wave propagation

Citation: Straka, T.; Vojtech, L.; Neruda, M. Simulation of Radio Signal Propagation for UHF RFID Technology in an Indoor Environment Using Ray Tracing (Graphics) Method. *Appl. Sci.* **2022**, *12*, 11065. https://doi.org/10.3390/app122111065

Academic Editor: Jia Liu

Received: 10 September 2022
Accepted: 24 October 2022
Published: 1 November 2022

1. Introduction

Applications using passive RFID (Radio Frequency Identification) technology, especially in the UHF (Ultra-High-Frequency) spectrum, are encountered in many sectors of operation nowadays. It is especially the identification and localization of objects and people in indoor space [1–4], logistics and inventory [5–7] or the monitoring of pipeline defects [8] in order to improve performance and efficient productivity and to increase service quality. An RFID system typically consists of a reading device, i.e., an RFID reader with a set of antennas and RFID tags that store information about a product or service. A larger number of readers and tags together form a complex system for identifying, tracking and monitoring objects bearing RFID tags. In this paper, the focus is on passive RFID communication in the UHF band 860–960 MHz, where the energy to activate the RFID tag is obtained from the reader device. Thus, the reading area depends mainly on the power radiated by the reader, the sensitivity of the tags, the orientation of the antennas and the shape of the area of operation of the system [9].

For passive UHF RFID systems, a difficult problem is to design the optimal placement of these RFID systems so that the desired area is completely covered by the signal. The tags have to be activated by the reader, and at the same time, there is no unwanted interference between the reader and the tags, which could lead to service degradation and reduced quality or error conditions. Another problem is the operation of the RFID system in the UHF band, where influences related to the environmental properties are typical and can have a strong impact on the performance of the system [10]. Furthermore, when designing the system, the parameters of the reader, antenna and tags must be taken into account, as well as the practical implementation (cable lengths, availability of electricity, etc.) [11]. Last but not least, other telecommunications technologies that can be operated in a given location in the same frequency spectrum should be considered to avoid undesired interference when designing an RFID system [11].

For the design of the RFID system, in terms of the accuracy of the results, physical measurement or on-site experimentation, which allows for obtaining accurate values of the measured parameters, appears to be suitable. From the physical measurements, we can mention, for instance, the determination of the required power (strength of the electromagnetic field) of the antennas of RFID readers by placing the tag in the space and measuring their detectability by the reader. The values of the RSSI (Received Signal Strength Indicator) parameter of the tag response at a constant power of the RFID reader can be recorded in order to determine the reading range of RFID UHF readers or antennas [11]. However, this procedure seems to be inappropriate in terms of time and money consumption. As a suitable solution, the use of simulation tools allow the placement of RFID components in 2D or 3D space. The simulation allows the implementation of various scenarios, such as the prediction of tag coverage (detectability), the effect of signal attenuation on obstacles, reflections from surfaces and others [12]. Such simulations can then help, for instance, in tuning the performance of RFID readers and thus in estimating the signal range for tag activation. The results of these simulations can have comparable predictive value to physical measurements and can thus provide a basis for physical implementation.

Over the last decades, several methods have been proposed to simulate the propagation of electromagnetic waves ranging from extremely low-frequency (ELF) [13] to terahertz waves [14]. The authors of article [15] divide these methods into three categories: empirical methods, deterministic methods (full-wave simulation) and ray tracing. Empirical methods, such as One-Slope [16], Dual-Slope [16], COST-231 [16] or Okumura-Hata [17], are based on a large number of measurements but may be inaccurate in the case of atypical spaces. For the application of RFID deployment in an indoor area, these methods lack spatial information and energy changes due to multipath propagation, which is very important for defining the tag readability area [15]. Among the deterministic methods, Method of Moments (MoM) [18], Finite-Difference Time-Domain (FDTD) numerical method [19] and Finite Integration Technique (FIT) numerical method [20] are mentioned. These methods are accurate but are computationally complex and time-consuming [15]. As a compromise, the now widely used deterministic method ray tracing [15,21–30], more precisely, ray tracing (physics) (RT), is based on geometrical optics (GO). It is usable as an approximated method to estimate the intensity of an electromagnetic field [21]. In this method, electromagnetic waves are treated as rays. The principle is based on emitting a certain number of rays from a source and tracking them. These then interact with obstacles in the form of refraction, diffraction and reflection depending on the material of the object, and so attenuation occurs at the obstacles [21]. In an indoor environment, the material represents a large part of the influence on attenuation. In RT simulations, the material properties of all objects within the simulation are often taken into account based on the knowledge of the dielectric constant and permittivity in the range of operating frequencies [31]. For instance, the authors in [32] discuss the calibration of ray tracing models based on measurements of permittivity and conductivity in the indoor environment. The limitations of this method are mainly the number of rays emitted and the size of the surfaces on which the rays hit and on which the resulting intensity is subsequently calculated and correlated. In the first case, the calculation time increases with an increasing number of rays, and in the second case, inaccuracy in the calculation may occur due to the different number of incident rays [33].

RT is a frequency-independent and widely used method for 2D and 3D radio coverage prediction. Therefore, it is often implemented as a feature in software tools. Some of the frequently used tools include Altair WinProp [34], Wireless InSite [35] and Altair Feko [36]. The authors of [37] use a combination of Altair Feko and Altair WinProp to predict the coverage of an indoor RFID infrastructure. The authors of [21] study the coverage of UHF-RFID tags at 433 MHz in an indoor environment using Altair WinProp. The authors of [22] use Wireless InSite as a 3-D ray-tracer to evaluate the proposed tag placement algorithm for THz RFID. The papers are categorized in Table 1.

Table 1. Categories of papers.

Category	Papers	Comments
RFID applications	[1–8]	Practical use
RFID implementation	[9–12]	Difficulties of UHF RFID implementation
Empirical methods	[16,17]	Inaccuracy is increased with specific forms of the environment (e.g., corridors)
Deterministic methods	[18–20,31]	Computationally demanding depending on the number of walls and obstacles
Ray tracing (physics)	[15,21–30,32,33]	Calculation time increases with an increasing number of rays, inaccuracy in the calculation may occur due to the different number of incident rays
Commercially available SW	[21,22,34–37]	Some of the frequently used tools

An analog of the physical ray tracing method is encountered in the domain of computer graphics as a technique for generating images in computer graphics. It belongs to the group of so-called global illumination algorithms, further referred to as ray tracing (graphics) (RTg). This method can be considered as a possible approach to predict the coverage of the radio signal in the graphics domain. The equation that describes the propagation of light in a 3D scene (i.e., the rendering equation) was published by James T. Kajiya in 1986 in [38].

The aim of this paper is the verification of the use of the RTg algorithm for the simulation of radio signal propagation in a 3D indoor environment for UHF RFID technology. The investigation of this approach is the main contribution of the paper because the RTg algorithm solves the global illumination problem in the domain of computer graphics by default. In the simulation, the effect of reflections and refractions, where some parameters, such as the shape of the 3D environment and the influence of materials, are considered. The simulation results of this approach are compared with the results of simulations of the empirical Multi-Wall model used in the simulation tool I-Prop [11]. For the presented approach, we focus on verifying the functionality, repeatability, accuracy of the results and time consumption.

Considering the simulation results, it can be concluded that this approach is applicable to simulate the UHF signal coverage from an RFID reader in an indoor environment. The authors of [11] compare the results of the Multi-Wall model with the real measurement results. Based on the *p*-value in the ANOVA table being less than 0.01, the authors conclude a statistically significant relationship between the results. Comparing the two original and two simulated heat maps, the maximum difference is 6.7% in the range of RSSI values -20 to -30 dBm for antenna 1. In terms of the highest and lowest differences for RSSI ranges, it is 6.5% in the range -1 to -20 dBm and 0.9% in the range -80 to -100 dBm for antenna 1. The total time to create the simulated environment is less than 10 min and the simulation time to create the heat map is less than 1 min.

The rest of this paper is structured as follows: Section 2 describes the approach to the simulation with all the required settings. The results from the heat map comparison and the discussion of functionality, repeatability, accuracy of the results and time consumption of this approach are presented in Section 3. The conclusion of this paper is presented in Section 4.

2. Methods

For the design principle of this method, a combination of two tools is chosen. The SketchUp Pro 2021 software tool allows the creation of a 3D model of the indoor environment. The advanced multi-core ray tracing engine called V-Ray is a plugin of SketchUp Pro, which uses the ray tracing (graphical) method. This combination allows the entire simulation to be created in one framework. That is, creating a 3D scene based on the floor plan, setting up sub-components for the heat map simulation, such as materials or lights, and rendering the final heat map output on the layer of floor plans with the corresponding RSSI values. The complete process of creating a 3D scene up to heat map generation is shown in Figure 1 and is explained in detail in Sections 2.1–2.8.

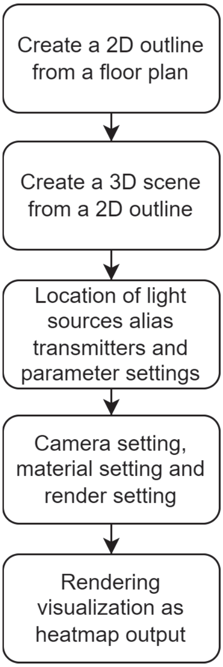

Create a 2D outline from a floor plan
Create a 3D scene from a 2D outline
Location of light sources alias transmitters and parameter settings
Camera setting, material setting and render setting
Rendering visualization as heatmap output

Figure 1. Procedure for creating heat maps.

2.1. RTg Method

Ray tracing (graphics) as a method for image generation by tracing the paths of light (rays) from the camera through pixels in the image plane is used in this approach; see Figure 2. The effects of rays encountering virtual objects are simulated.

The procedure of RTg is described in the following steps:

- Primary rays—traced from the camera into the scene determine what will be seen in the final image.
- Shadow rays—traced from each rendered point to each light in the scene determine whether the point will be illuminated or shadowed.
- Reflection rays—traced in the direction of the reflection vector, which depends on the type of reflection, i.e., fresnel or normal and the index of refraction of the material.
- Refraction rays—the direction of the rays depends only on the index of refraction of the material.
- glossy rays—many rays are traced in a cone, and the distribution of the cone depends on the amount of gloss of the material.

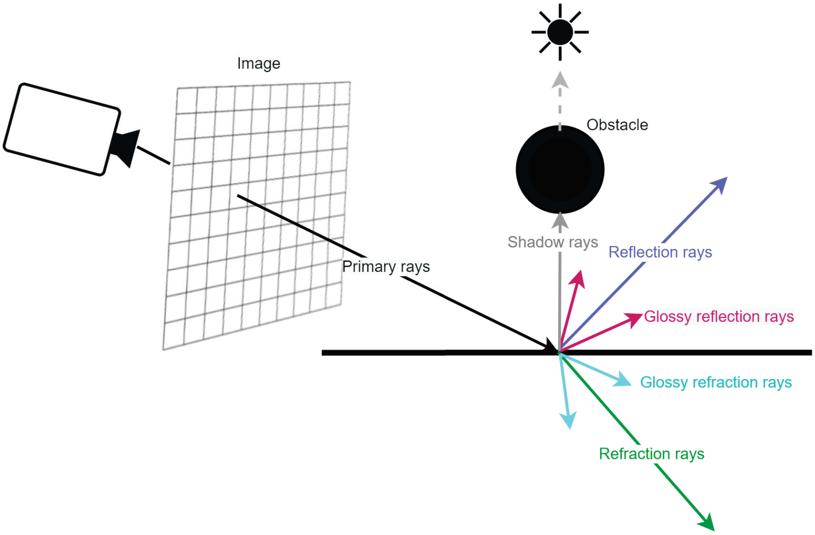


Figure 2. The basic mechanism of RTg.

2.2. *Selecting the Environment for Simulation*

For the purpose of comparing the simulation results with existing simulated values, the authors' indoor corridor environment in [11] is chosen. The following parameters needed to create the same environment are known:

- Floor plan of the area,
- Location of RFID readers (antennas),
- Heat map on 2D floor plan with corresponding RSSI values.

With these parameters, the outputs of the approach presented in this paper can be compared with the empirical Multi-Wall method used by the authors of [11]. The original floor plan is shown in Figure 3. The heat map over the floor plan with RSSI values is shown in Figure 4 for antenna 1 and Figure 5 for antenna 2.

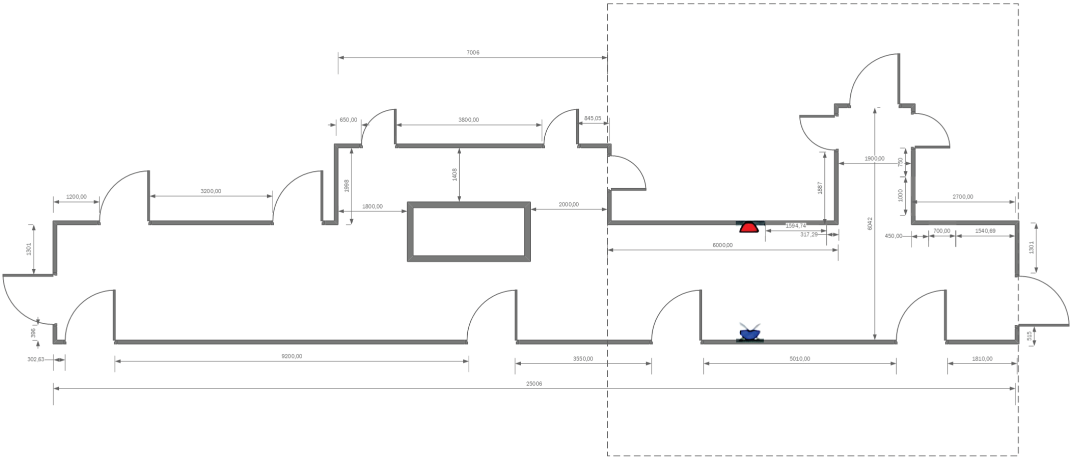


Figure 3. Original floor plan, taken from [11].

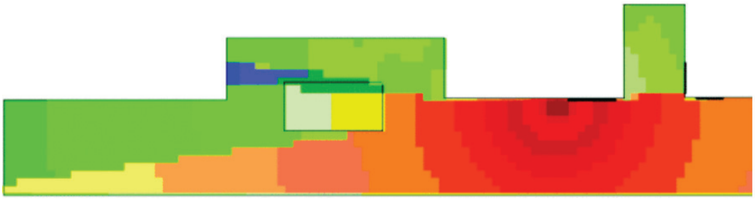


Figure 4. RFID signal propagation for antenna 1 in the corridor, taken from [11].

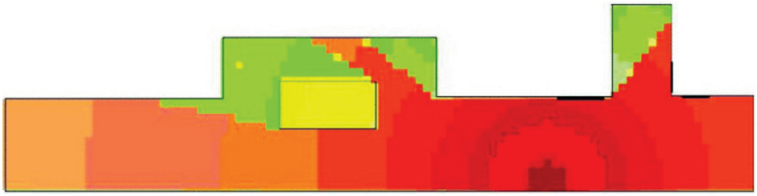


Figure 5. RFID signal propagation for antenna 2 in the corridor, taken from [11].

2.3. Selecting of Software Tools for Simulation

SketchUp Pro 2021 software tool is chosen for the creation of 3D indoor environments as a 3D architectural design tool with accurate metric mapping of physical space to virtual space. The V-Ray software add-on is used for the resulting heat map scene visualization, which is implementable as a plugin in the SketchUp tool. The V-Ray software is a multi-core ray tracing engine that is focused on fast and accurate visual results using the RTg method. The main feature of V-Ray is the VRayLightingAnalysis (VLA) renderer. It allows the analysis of the illumination intensity on 2D surfaces and in 3D space and creates a visual heat map in the environment. This map is generated with a smooth color transition representing a range of light intensity, from blue (low intensity) to red (high intensity). These color ranges can be compared to the range of RSSI color spectrum values; see Figure 6, used by the authors of [11].

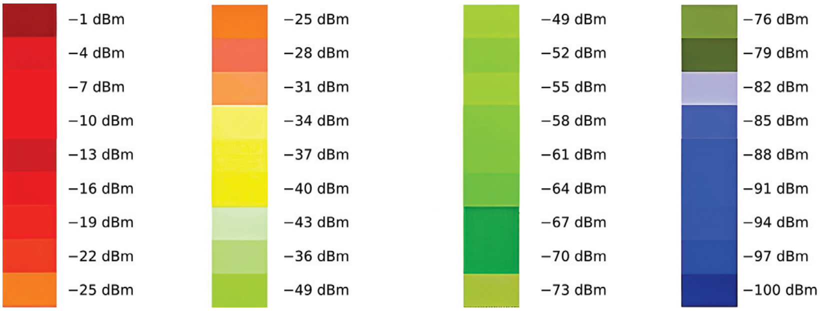


Figure 6. Color spectrum representing the RSSI values in the heat map used in the simulation, taken from [11].

2.4. Creating 3D Simulation Model

A floor plan is selected for modeling; see Figure 3. The 3D model is created in SketchUp in accordance with the floor plan; see Figure 7. The only unknown is the ceiling height, which has been set to 3 m, which we consider a sufficient compromise given the fact that only one floor is considered.

2.5. Sources of Signals

For the simulation, two light sources from the V-Ray Sphere Light are **placed** in the 3D scene in accordance with the original RFID antenna placement; the red dot is for antenna 1, and the blue dot is for antenna 2; see Figure 8. These light sources replace the original RFID antennas; see Figures 4 and 5. These light sources can be compared to the properties of an isotropic emitter. See Table 2 for the original antenna settings and Table 3 for the settings for the light sources.

The default SunLight function is disabled in the 3D scene and the Shadows, Affect (Diffuse, Specular, Reflections) functions are left unchanged in the "On" state.

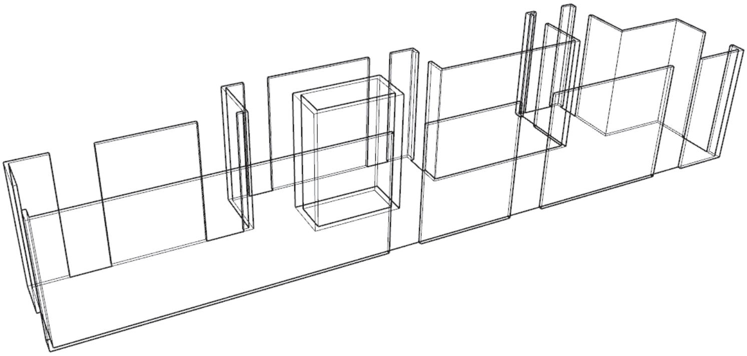


Figure 7. Three-dimensional model of the corridor from the floor plan in SketchUp.

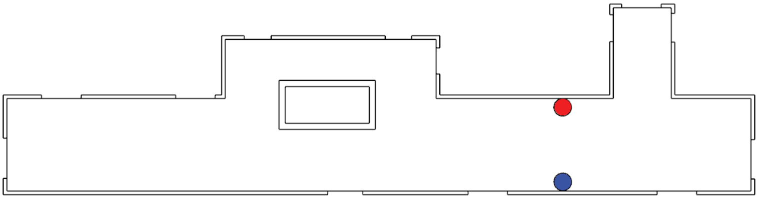


Figure 8. Position of light sources in the scene. Red dot for antenna 1, blue dot for antenna 2.

Table 2. Parameters of the RFID antennas.

Parameters	Value
Frequency (MHz)	868
Power emitted by the reader antenna 1 (dBm)	33
Power emitted by the reader antenna 2 (dBm)	33
Height of the antenna above the floor (m)	1.5

Table 3. Parameters set for V-Ray Sphere Lights.

Parameters	Value
Size (diameter of sphere) (cm)	5
Intensity (-)	33
units	scalar
Color	white (rgb(255,255,255))
No Decay	yes

2.6. Material Setting

Commonly used ray tracing simulation tools work with material properties for a specific frequency range, i.e., permittivity and conductivity coefficients. As this approach is based on the RTg method, light rays are used instead of interpreting electromagnetic waves and materials need to be modified accordingly to simulate the effect of electromagnetic properties on materials. The use of glass material (i.e., VRAY Glass material) seems to be appropriate. This material is applied to all objects in the scene with the following parameters:

- Diffuse color—rgb(255,255,255)
- Reflection color—rgb(255,255,255)
- Refraction color—rgb(204,204,204)
- Index of Refraction (IOR)—1.52
- Reflection Max Depth—5
- Refraction Max Depth—5

The diffuse color parameter set like this indicates that the material has white color as the default. The IOR parameter represents the glass material and indicates that light rays interact with the surface for ideal refraction and reflection. The reflection color parameter specifies the amount of reflection. The refractive color parameter allows the generation of the attenuation of optical rays due to the change in light transmittance of a given material. The authors of [11] give an attenuation due to walls of 14 dB, and this attenuation approximately corresponds to the above settings found by simulation. The maximum depth of reflection and refraction indicates how many times the ray can be reflected or refracted. This value is set by default for the VRAY Glass material, and increasing these values results in higher computational complexity. The maximum value of reflections and refractions is limited to 10 in this SW.

In terms of material limits, these limits can be specified as:

- Refraction color—rgb(0,0,0) (non-transparent)
- Refraction color—rgb(255,255,255) (fully transparent)
- Reflection color—rgb(0,0,0) (non-reflective)
- Reflection color—rgb(255,255,255) (fully reflective)

2.7. Camera and Render Setting

For the camera setting, the top view is chosen with an orthogonal view in accordance with the original heat map, Figures 4 and 5. It allows a comparison between the original and the generated heat map under the same conditions.

The rendering settings are configured to generate a heat map, and the processor is selected as the computational unit. It is common today to use a graphics processor to render computer graphics, but the VLA renderer does not currently support this option. The details of each setting can be seen in Figure 9.

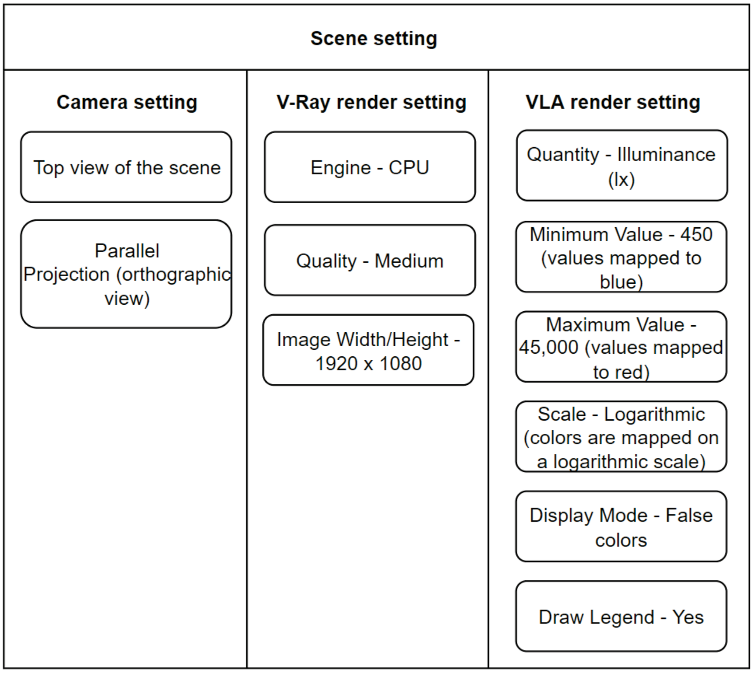
2.8. Comparing Heat Maps Using Pixel Presence in the Heat Map

The results of the RTg method, i.e., the simulated heat map shown in Figures 10a and 11a, are compared with the empirical Multi-Wall method, i.e., the original heat map shown in Figures 10a and 11b. The comparison is performed by the Python script [39]. The input of this script is the original and the generated heat map, but it is mandatory to unify the orientation and resolution of both heat maps. RTg and the VLA renderer used allows for the generation of heat maps with a smooth color spectrum of RSSI values, see Figures 10a and 11a, which is desirable in the case of more accurate coverage prediction in units of RSSI values. In the case of the comparative heat map; see Figures 10b and 11b, the resolution of RSSI values is not as fine. This is taken into account in the comparison of the simulated heat maps.

A smooth color spectrum of RSSI values shown in Figure 12 is loaded into the script based on the RSSI values from the I-Prop tool, Figure 6. A set of color ranges corresponding to the ranges of RSSI values is then created. The script then detects the color of each pixel and assigns it to a color range of RSSI values. The result is the percentage representation of each RSSI value or range of RSSI values from both heat maps, i.e., simulated and original. White, black and grayscale colors are not considered RSSI values and are excluded from the detection. From the original RSSI gradient values shown in Figure 6, it can be seen that the color ranges for -1 to -20 dBm are considered to be red. The shades of blue are considered equal in the -80 to -100 dBm range. The shades of green are found in the -40 to -60 dBm range, and thus, this fine differentiation disappears for this reason, the classification of the ranges is proceeded with:

- −1 to −10 dBm and −10 to −20 dBm is unified as −1 to −20 dBm
- −40 to −50 dBm and −50 to −60 dBm is unified as −40 to −60 dBm
- −80 to −90 dBm and −90 to −100 dBm is unified as −80 to −100 dBm

The evaluation of the matching tool in Python follows values of 10 dBm, i.e., −1 to −10 dBm etc.



Scene setting

Camera setting

- Top view of the scene
- Parallel Projection (orthographic view)

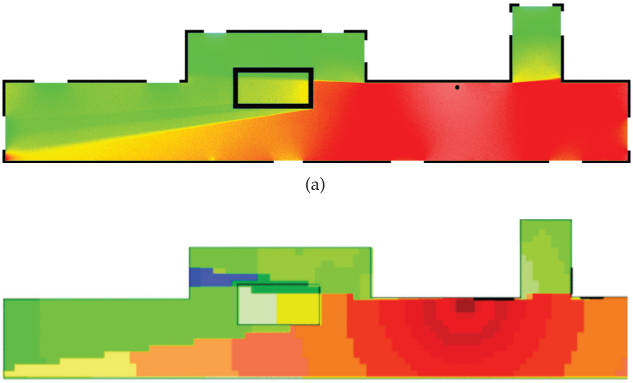
V-Ray render setting

- Engine - CPU
- Quality - Medium
- Image Width/Height - 1920 x 1080

VLA render setting

- Quantity - Illuminance (lx)
- Minimum Value - 450 (values mapped to blue)
- Maximum Value - 45,000 (values mapped to red)
- Scale - Logarithmic (colors are mapped on a logarithmic scale)
- Display Mode - False colors
- Draw Legend - Yes

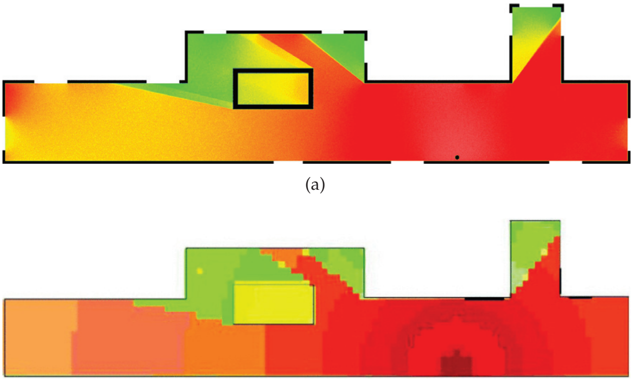
Figure 9. Scene settings for correct heat map rendering.



(a)

(b)

Figure 10. RTg heat map of antenna 1 (**a**) and Multi-Wall heat map (**b**) (taken from [11]).



(a)

(b)

Figure 11. RTg heat map of antenna 2 (**a**) and Multi-Wall heat map (**b**) (taken from [11]).

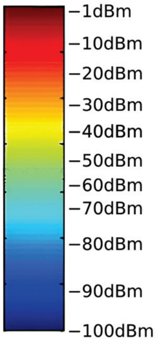


Figure 12. Smooth color gradient of RSSI values created from the template according to Figure 6.

3. Results and Discussion

3.1. Functionality and Repeatability

The evaluation criterion in terms of functionality is the ability of this approach to generate a heat map representing the electromagnetic (EM) signal intensity, which is based on the knowledge of the 3D form of the simulation environment, Figures 10a and 11a. This approach is validated against the heat map generated by the I-Prop tool, which uses the Multi-Wall method, Figures 10b and 11b. The functionality fulfills the evaluation criteria.

The repeatability is verified by generating two different heat maps, i.e., for antennas 1 and 2, while keeping the same parameter settings. The simulated heat map results are similar (equivalent) to the simulations generated by the Multi-Wall method for both scenarios.

3.2. Accuracy of the Results

The results of heat map comparison using RSSI color ranges are shown in Table 4 for antenna 1 and Table 5 for antenna 2. For antenna 1, it can be seen that there is about a 6.5% difference in the ranges −1 to −20 dBm and −20 to −30 dBm. Looking at the original and simulated heat maps, Figures 10a and 11a, the simulated heat map lacks the orange color at the circular distance from the antenna. It is replaced by the red color of the higher-intensity RSSI values. This is due to the fact that for the RTg method, the level of the transmitted signal does not decrease with distance from the source at the chosen setting with such a steepness as in the case of the Multi-Wall method. The remaining differences are less than 1.6%.

In the case of antenna 2, the highest difference is 2.7% in the range −1 to −20 dBm. This minor difference is most likely due to the smooth transition between the red and orange RSSI values in the simulated heat map, while in the original heat map, the color transitions are strictly limited. The remaining differences are less than 1.4%.

The remaining percentages, up to 100% of the heat map, are black, white and grayscale colors, which are excluded from the comparison as they do not represent the level of transmitted power.

Table 4. Percentage of pixels in the heat map by RSSI ranges for antenna 1.

RSSI range (dBm)	−1; −20	−20; −30	−30; −40	−40; −60	−60; −70	−70; −80	−80; −100
Original (%)	17.6	14.2	4.3	27.1	Null	Null	0.9
Simulation (%)	24.1	7.5	4.0	28.8	Null	Null	Null
Difference (%)	6.5	6.7	0.3	1.7	Null	Null	0.9

Table 5. Percentage of pixels in the heat map by RSSI ranges for antenna 2.

RSSI range (dBm)	−1; −20	−20; −30	−30; −40	−40; −60	−60; −70	−70; −80	−80; −100
Original (%)	30.5	19.2	4.0	8.9	Null	Null	Null
Simulation (%)	27.8	20.6	4.7	7.5	Null	Null	Null
Difference (%)	2.7	1.4	0.8	1.4	Null	Null	Null

3.3. Time Consumption

The time complexity of the tasks in this approach, in descending order, is as follows:

- Creating a 3D model,
- Software Tools Setup,
- Heat map rendering time.

The time taken to create a 3D model from a floor plan is strongly dependent on the complexity of the floor plan. There is only one room in this simulation and the time required to create the model is 3 min. It takes 3 min to set up the software. The rendering time of the heat map is strongly dependent on the complexity of the scene, the number of EM emitters, i.e., light sources, and the desired resolution of the heat map. The results for different heat map resolution configurations and different numbers of sources in the scene can be seen in Table 6. The difference in simulation time between antennas 1 and 2 are lower units of seconds, and this difference can be considered negligible. The simulation times given in Table 6 are for antenna 1. In the case of two active emitters, both antennas are active in the heat map. The simulation times for one and two active emitters differ by lower units of seconds and increase with increasing resolution of the heat map. In this simulation, the computation is performed in only one closed corridor. In the case of multiple simulation rooms, a larger difference in time between one and two active emitters can be expected as the computational complexity of propagating reflections and refractions increases.

Table 6. Test of time consumption for different resolutions of the heat map and a different number of emitters.

Resolution	**1 Source [s]**	**2 Sources [s]**
2560 × 1440 (2K)	29	35
1920 × 1080 (Full HD)	17	20
1280 × 720 (HD)	8	10

4. Conclusions

In this paper, the approach for simulation of radio signal propagation for passive UHF RFID technology in an indoor environment using the RTg method is proposed. Using a combination of the 3D modeling tool SketchUp and the V-Ray plugin for computer rendering of images, the use of the RTg method to render a heat map over a 2D floor plan in a 3D scene is demonstrated. The heat map thus presents the signal intensity in the environment as RSSI values. This approach has the potential to reduce the time and cost requirements for planning an RFID system infrastructure. It also provides a comprehensive view of the signal range in a real environment, which can improve the approach to the coexistence of multiple telecommunication technologies in a given environment.

A comparison of the RTg method with the Multi-Wall method and its verification based on the comparison of visual results of heat maps over a 2D plan in a 3D environment is presented. Two heat maps are generated in one environment for two different antenna locations, i.e., antennas 1 and 2. The largest difference of 6.7% is achieved for the RSSI value range of −20 to −30 dBm. The difference of 6.5% is achieved for the range of −1 to −20 dBm. These differences come at the strongest signal. Hence they have practically no effect on the functionality of the RFID system. We believe that this difference is negligible from a practical point of view. Practically, the most interesting results are the RSSI levels at which the signal is lost or almost lost. The maximum difference for the lowest RSSI range, i.e., −80 to −100 dBm, is 0.9% for antenna 1.

In terms of time, the entire simulation up to the resulting heat map can be created in 10 min. However, this strongly depends on the complexity of the scene and the number of signal sources. It is affected by the increase in time required to create a 3D model and the time required to calculate reflections and refractions from a larger number of objects.

Although this approach shows results comparable to other methods for radio signal prediction, further experimental investigation is needed. One possible goal is to make corrections to the set parameters in this approach based on real measurements or a larger number of validated simulation results. Furthermore, there is a need to minimize the time to create a 3D scene, which increases significantly with the complexity of the floor plan. Furthermore, the position and rotation of the RFID tag relative to the RFID antenna need to be considered, which is not currently accounted for in this approach. A future extension of this study should focus on the interpretation of signal strength in notional 3D space, e.g., by layering surfaces so that the three-dimensionality is not lost. This extension would also contribute significantly to the analysis of tag detectability for different locations in the indoor environment.

Author Contributions: Writing—original draft, T.S.; Writing—review & editing, L.V. and M.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by CTU in Prague grant no. SGS21/161/OHK3/3T/13.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

EM	Electromagnetic
ELF	Extremely Low-Frequency
FDTD	Directory of open-access journals
FIT	Finite-Difference Time-Domain
IOR	Index of Refraction
MoM	Method of Moments
RFID	Radio Frequency Identification
RSSI	Received Signal Strength Indication
RT	Ray Tracing
RTg	Ray Tracing graphics
UHF	Ultra-high-frequency
VLA	VRayLightingAnalysis render element

References

1. Diallo, A.; Lu, Z.; Zhao, X. Wireless Indoor Localization Using Passive RFID Tags. *Procedia Comput. Sci.* **2019**, *155*, 210–217. [CrossRef]
2. Tlili, F.; Hamdi, N.; Belghith, A. Accurate 3D localization scheme based on active RFID tags for indoor environment. In Proceedings of the 2012 IEEE International Conference on RFID-Technologies and Applications (RFID-TA), Nice, France, 5–7 November 2012; pp. 378–382. [CrossRef]
3. Hatem, E.; Abou-Chakra, S.; Colin, E.; Laheurte, J.M.; El-Hassan, B. Performance, Accuracy and Generalization Capability of RFID Tags' Constellation for Indoor Localization. *Sensors* **2020**, *20*, 4100. [CrossRef] [PubMed]
4. Fu, Y.; Wang, C.; Liu, R.; Liang, G.; Zhang, H.; Ur Rehman, S. Moving Object Localization Based on UHF RFID Phase and Laser Clustering. *Sensors* **2018**, *18*, 825. [CrossRef] [PubMed]
5. Banerjee, S.R.; Jesme, R.; Sainati, R.A. Performance Analysis of Short Range UHF Propagation as Applicable to Passive RFID. In Proceedings of the 2007 IEEE International Conference on RFID, Grapevine, TX, USA, 26–28 March 2007; pp. 30–36. [CrossRef]
6. Álvarez López, Y.; Franssen, J.; Álvarez Narciandi, G.; Pagnozzi, J.; González-Pinto Arrillaga, I.; Las-Heras Andrés, F. RFID Technology for Management and Tracking: E-Health Applications. *Sensors* **2018**, *18*, 2663. [CrossRef] [PubMed]
7. García Oya, J.R.; Martín Clemente, R.; Hidalgo Fort, E.; González Carvajal, R.; Muñoz Chavero, F. Passive RFID-Based Inventory of Traffic Signs on Roads and Urban Environments. *Sensors* **2018**, *18*, 2385. [CrossRef] [PubMed]
8. Deif, S.; Daneshmand, M. Multiresonant Chipless RFID Array System for Coating Defect Detection and Corrosion Prediction. *IEEE Trans. Ind. Electron.* **2020**, *67*, 8868–8877. [CrossRef]
9. Marrocco, G.; Di Giampaolo, E.; Aliberti, R. Estimation of UHF RFID Reading Regions in Real Environments. *IEEE Antennas Propag. Mag.* **2009**, *51*, 44–57. [CrossRef]
10. Fuschini, F.; Capriotti, L. A statistical approach to the evaluation of the coverage area of UHF RFID systems. In Proceedings of the 2011 IEEE International Conference on RFID-Technologies and Applications, Sitges, Spain, 15–16 September 2011; pp. 502–506. [CrossRef]
11. Svub, J.; Stasa, P.; Benes, F.; Vojtech, L.; Neruda, M.; Brozek, T. Autonomous System for UHF RFID Signal Measurement in Industrial Environment. In Proceedings of the 2018 11th IFIP Wireless and Mobile Networking Conference (WMNC), Prague, Czech Republic, 3–5 September 2018; pp. 1–6. [CrossRef]
12. La Scalia, G.; Aiello, G.; Micale, R.; Enea, M. Coverage analysis of RFID indoor localization system for refrigerated warehouses based on 2D-ray tracing. *Int. J. RF Technol.* **2012**, *3*, 85–99. [CrossRef]
13. Rahmatillah, R. ELF wave propagation simulation using FDTD method and satellite constellation concept for early warning system. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 19–22 February 2017; pp. 725–729. [CrossRef]
14. Zhang, Y.; Xu, G.; Zheng, Z. Terahertz waves propagation in an inhomogeneous plasma layer using the improved scattering-matrix method. *Waves Random Complex Media* **2021**, *31*, 2466–2480. [CrossRef]
15. Chen, R.; Yang, S.; Liu, Z.; Penty, R.V.; Crisp, M. A 3D Ray-tracing Model for UHF RFID. In Proceedings of the 2020 IEEE International Conference on RFID (RFID), Orlando, FL, USA, 28 September–16 October 2020; pp. 1–8. [CrossRef]
16. Andrade, C.B.; Hoefel, R.P.F. IEEE 802.11 WLANs: A comparison on indoor coverage models. In Proceedings of the CCECE 2010, Calgary, AB, Canada, 2–5 May 2010; pp. 1–6. [CrossRef]
17. Medeisis, A.; Kajackas, A. On the use of the universal Okumura-Hata propagation prediction model in rural areas. In Proceedings of the VTC2000-Spring. 2000 IEEE 51st Vehicular Technology Conference Proceedings (Cat. No.00CH37026), Tokyo, Japan, 15–18 May 2000; Volume 3, pp. 1815–1818. [CrossRef]
18. Kavanagh, I.; Pham-Xuan, V.; Condon, M.; Brennan, C. A method of moments based indoor propagation model. In Proceedings of the 2015 9th European Conference on Antennas and Propagation (EuCAP), Lisbon, Portugal, 12–17 April 2015; pp. 1–5.
19. Laner, A.; Bahr, A.; Wolff, I. FDTD simulations of indoor propagation. In Proceedings of the IEEE Vehicular Technology Conference (VTC), Stockholm, Sweden, 8–10 June 1994; Volume 2, pp. 883–886. [CrossRef]
20. Zakharov, P.; Dudov, R.; Mikhailov, E.; Korolev, A.; Sukhorukov, A. Finite Integration Technique capabilities for indoor propagation prediction. In Proceedings of the 2009 Loughborough Antennas & Propagation Conference, Loughborough, UK, 16–17 November 2009; pp. 369–372. [CrossRef]
21. Hatem, E.; Abou-Chakra, S.; Colin, E.; El-Hassan, B.; Laheurte, J.M. 3D Modeling for Propagation of UHF-RFID Tags' Signals in an Indoor Environment. In Proceedings of the 2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Manama, Bahrain, 19–21 November 2019; pp. 1–6. [CrossRef]
22. El-Absi, M.; Al-Haj Abbas, A.; Kaiser, T. Chipless RFID Tags Placement Optimization as Infrastructure for Maximal Localization Coverage. *IEEE J. Radio Freq. Identif.* **2022**, *6*, 368–380. [CrossRef]
23. Bosselmann, P.; Rembold, B. Investigations on UHF RFID wave propagation using a ray tracing simulator. *Frequenz* **2006**, *60*, 38–46. [CrossRef]
24. Hechenberger, S.; Neunteufel, D.; Arthaber, H. Ray Tracing and Measurement based Evaluation of a UHF RFID Ranging System. In Proceedings of the 2022 IEEE International Conference on RFID (RFID), Las Vegas, NV, USA, 17–19 May 2022; pp. 75–80. [CrossRef]
25. Škiljo, M.; Šolić, P.; Blažević, Z.; Perković, T. Analysis of Passive RFID Applicability in a Retail Store: What Can We Expect? *Sensors* **2020**, *20*, 2038. [CrossRef] [PubMed]

26. Firdaus, F.; Ahmad, N.A.; Sahibuddin, S. Accurate Indoor-Positioning Model Based on People Effect and Ray-Tracing Propagation. *Sensors* **2019**, *19*, 5546. [CrossRef] [PubMed]
27. Eid, A.H.; Soliman, H.Y.; Abuelenin, S.M. Efficient ray-tracing procedure for radio wave propagation modeling using homogeneous geometric algebra. *Electromagnetics* **2020**, *40*, 388–408. [CrossRef]
28. Salski, B.; Czekala, P.; Cuper, J.; Kopyt, P.; Jeon, H.; Yang, W. Electromagnetic Modeling of Radiowave Propagation and Scattering From Targets in the Atmosphere With a Ray-Tracing Technique. *IEEE Trans. Antennas Propag.* **2021**, *69*, 1588–1595. [CrossRef]
29. Yildirim, G.; Gunduzalp, E.; Tatar, Y. 3D shooting and bouncing ray approach using an artificial intelligence-based acceleration technique for radio propagation prediction in indoor environments. *Phys. Commun.* **2021**, *47*, 101400. [CrossRef]
30. Lee, J.Y.; Kang, M.Y.; Kim, S.C. Path Loss Exponent Prediction for Outdoor Millimeter Wave Channels through Deep Learning. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–5. [CrossRef]
31. Azpilicueta, L.; Rawat, M.; Rawat, K.; Ghannouchi, F.M.; Falcone, F. A Ray Launching-Neural Network Approach for Radio Wave Propagation Analysis in Complex Indoor Environments. *IEEE Trans. Antennas Propag.* **2014**, *62*, 2777–2786. [CrossRef]
32. Navarro, A.; Guevara, D.; Giménez, J.; Cardona, N. Measurement-based ray-tracing models calibration of the permittivity and conductivity in indoor environments. *Ing. Compet.* **2018**, *20*, 41–51. [CrossRef]
33. Taygur, M.M.; Sukharevsky, I.O.; Eibert, T.F. Computation of Antenna Transfer Functions with a Bidirectional Ray-Tracing Algorithm Utilizing Antenna Reciprocity. In Proceedings of the 2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC), Gran Canaria, Spain, 28 May–1 June 2018; pp. 1–4. [CrossRef]
34. Altair Engineering Inc. Radio Coverage Planning with Altair Winprop. Available online: https://web.altair.com/winprop-telecom (accessed on 4 September 2022).
35. Remcom Inc. Wireless Insite® Propagation Software Features. Available online: https://www.remcom.com/wireless-insite-em-propagation-features (accessed on 4 September 2022).
36. Altair Engineering Inc. Simulation for Connectivity, Compatibility, and Radar: Altair Feko. Available online: https://www.altair.com/feko (accessed on 4 September 2022).
37. Karuppuswami, S.; Reddy, C. RFID in Packaging Surveillance: Impact of Simulation Tools in Design, Coverage Planning and Placement of "Smart" Readers Along the Supply Chain. In Proceedings of the 2020 Antenna Measurement Techniques Association Symposium (AMTA), Newport, RI, USA, 2–5 November 2020; pp. 1–6.
38. Kajiya, J.T. The rendering equation. In Proceedings of the 13th Annual Conference on Computer Graphics and Interactive Techniques, New York, NY, USA, 31 August 1986; pp. 143–150.
39. Straka, T. Strakto2/RFID-Heatmap-Comparision. Available online: https://zenodo.org/record/7072080#.Y2CXK-RBxPY (accessed on 4 September 2022).

applied sciences

MDPI

Article

RFID Authentication System Based on User Biometric Information †

Yuanmu Huang [1], Bin Fu [1,*], Ningwei Peng [1], Yanwen Ba [1], Xuan Liu [1,2] and Shigeng Zhang [3]

[1] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[2] State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China
[3] School of Computer Science, Central South University, Changsha 410008, China
* Correspondence: fubin@hnu.edu.cn

† This paper is an extended version of our paper published in 16th International Conference, WASA 2021, Nanjing, China, 25–27 June 2021.

Abstract: Traditional authentication technologies usually perform identity authentication based on user information verification (e.g., entering the password) or biometric information (e.g., fingerprints). However, there are security risks when applying only these authentication methods. For example, if the password is compromised, it is unlikely to determine whether the user entering the password is legitimate. In this paper, we subdivide biometric information into physiological and behavioral information, and we propose a novel user authentication system, RF-Ubia, which utilizes the low-cost radio frequency identification (RFID) technology to capture unique biological or behavioral information rooted in the user and can be used in two schemes for user authentication. Consisting of an array of nine passive tags and a commercial RFID reader, RF-Ubia provides double assurance for security of identity authentication by combining user information and biometric characteristics. It first verifies the user's password, and then identifies the biometric characteristics of the legitimate user. Due to the coupling effect among tags, any change in tag signal caused by the user's touch will affect other tag signals at the same time. Since each user has different fingertip impedance, their touch will cause unique tag signal changes. Therefore, by combining biometric information, the tag array will uniquely identify users. The evaluation results show that RF-Ubia achieves excellent authentication performance with an average recognition rate of 93.8%.

Keywords: RFID; authentication; biometric information

Citation: Huang, Y.; Fu, B.; Peng, N.; Ba, Y.; Liu, X.; Zhang, S. RFID Authentication System Based on User Biometric Information. *Appl. Sci.* **2022**, *12*, 12865. https://doi.org/10.3390/app122412865

Academic Editor: Mario Lucido

Received: 27 October 2022
Accepted: 8 December 2022
Published: 14 December 2022

1. Introduction

With the rapid development of modern technology, new automatic identification technologies emerge in endlessly, among which radio frequency identification (RFID) technology has become the core technology of the Internet of Things with its excellent advantages.

With the commercialization of RFID, its application is becoming more and more widespread, including item tracking, motion detection [1,2], goods security and so on [3–7]. As the increasing demand on protection for security industry and personal privacy, user authentication technology has become particularly important. The purpose of user authentication is to verify whether a user is indeed a legitimate user registered in the system, which is a vital task in many applications, such as area or event access control and electronic payment.

In the existing work, user authentication methods are mainly divided into two categories: device authentication and user authentication. Authentication devices such as personal identity cards, authentication users such as fingerprints, etc.; both authentication technologies are each facing many potential risks and hidden dangers due to imperfect security mechanisms. Device authentication may have the risk of being lost, stolen, or copied. When users set their passwords too short or simple, their accounts can easily be stolen, leading to insecure accounts on other systems as well. If complex passwords consisting of numbers and letters are used alternately, it can increase the security strength of the password, but it will increase the complexity of the system usage and is very unfriendly to users. When the system uses ID cards to identify and verify user identity, the cards may be at risk of being copied or lost. As in the Hu-Fu (Wang et al. [8,9]) authentication scheme, if the authentication tag is stolen by an attacker, the attacker can pass the authentication without any hindrance; with RF-Mehndi (Zhao et al. [10]), although the personal card is also able to resist the attacker's counterfeit when it is lost or stolen, the user card needs to be recreated and the information collected will still cause trouble to the user. User authentication-based schemes to verify users' biological information, such as Vauth (Feng et al. [11]), Cardiac Scan (Lin et al. [12]), BioTag (Hu et al. [13].), and TrueHeart (Zhao et al. [14]) continuous authentication schemes, mostly require the use of dedicated sensors, which have major limitations in terms of cost and applicability. While the mainstream user authentication methods now use biometric features such as the user's fingerprint, face (Xu et al. [15]), and iris to authenticate the user's identity, biometric features such as fingerprints provide a more excellent authentication performance compared to traditional authentication techniques. However, it is by nature a static image or data matching and still has the possibility of being copied. To overcome these problems, cutting-edge research has proposed a concept of continuous authentication, i.e., using some device to continuously extract dynamic human biometric features for authentication, such as breathing (Wang et al. [16]), heart rate (Zhao et al. [14]), and sound resonance (Feng et al. [11]). However, continuous authentication requires a very high acquisition rate and computational power of the device, leading to excessive cost and difficulty, and it can still only be implemented in an experimental setting.

In summary, although many user authentication methods have been proposed [5,8–10], they have some contradictions and drawbacks in terms of application target, deployment scope, cost, system complexity, and security resistance. It is a new challenge to find a simple and secure authentication method. To address the shortcomings of current user authentication methods, we subdivide biometric information into physiological and behavioral characteristics, and we design and implement RF-Ubia, which is a simple and secure user authentication method for different people, supports both password and passwordless authentication methods, and can achieve high recognition accuracy and at a much lower cost than existing work.

RF-Ubia consists of nine passive tags forming a cryptographic array, with each tag acting as a cryptographic button, as shown in Figure 1. Users only need to touch the tag surface once to enter a password number. When the user touches multiple tags continuously, the digital sequence obtained is used as the user authentication password. In the process of touching, we also skillfully incorporate the biometric information into tag signals. When different users touch the RFID tags, distinctive phase changes will occur as a result of users' different body impedance. The closer these tags are in the array, the stronger the coupling effect among them will become [8–10]. When a tag is touched, not only its signal will change, but also the signals of the other eight tags will change due to the coupling effect. These signal changes are highly correlated with the user's body impedance. Normally, the impedance of the human body is about 300–1000 Ω. Different users have different body impedance, which leads to different changes in the phase signal of the tags. Combined with user's biometric information, different users who entered the same password can be distinguished. The main contributions of our work are summarized as follows:

- We propose a low-cost simple user authentication method called RF-Ubia, which allows users to effectively resist password theft even with simple passwords.
- We propose an extension of the RF-Ubia system that fuses user impedance and behavioral features, allowing users to authenticate users even if they forget their passwords, and ensures security that is largely immune to environmental interference, achieving an average recognition accuracy of 0.94. We improve the traditional anomaly detection and feature extraction algorithms to obtain more fine-grained feature information to improve accuracy. We used Random Forest in Wake to classify, and RF-Ubia was

able to achieve an average recognition accuracy of 0.96 while existing work based on template matching or convolutional neural networks (CNN) was below 0.92 under the same conditions.

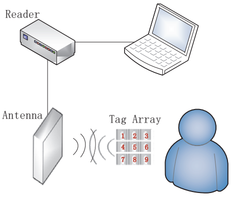


Figure 1. Illustration of RF-Ubia. The user touches the surface of the tag array to enter the password, and the reader captures the signal integrating the user's biometric characteristics.

2. Related Work

User authentication methods can be divided into three main categories: information, possessions, physiological and behavioral characteristics.

Information, such as passwords or security codes. The information-based approach is designed to use traditional cryptographic algorithms to perform authentication and use encryption technology to protect tags from illegal access [17–21]. Most of these methods require modifications to commercial communication protocols or tag hardware, making it difficult to apply them to lightweight passive tags.

Possessions, such as various certificates or ID cards. The physical information-based approaches identify and verify the tags by taking advantage of the differences in the tag circuit characteristics, which will be reflected in the backscattering signal. Ding et al. propose a reader authentication solution based on physical layer signals, namely Arbitrator [22,23], which can effectively prevent unauthorized access to tags. Ma et al. [24] propose a new physical layer recognition system based on internal similarity, GenePrint. Yang et al. [25] use additional phase offset as a new fingerprint called Tagprint for identifying a pair of readers and tags. Chen et al. explore a new fingerprint called Eingerprint [26] to authenticate passive tags in the commodity RFID system, which uses the electrical energy stored in the tag circuit as a fingerprint. Wang et al. explore a verification method called Hu-Fu [8]. The authors observe inductive coupling between two adjacent tags [27,28]. When two tags are placed very close and the coupling effect occurs, Hu-Fu can achieve the purpose of verification.

Physiological or behavioral characteristics. In recent years, the mainstream user authentication methods are based on different biological characteristics (e.g., fingerprint, face and retina) for identification. Compared with traditional authentication technology, the biometric authentication technology (especially fingerprint authentication) has achieved more excellent performance owing to its universality, uniqueness, permanence and anti-counterfeiting characteristics. RF-Mehndi [10] uses the physical characteristics of the tag and the biometric characteristics of the holder to verify the user's validity. When the user touches the tag, the physical layer information of the tag and the user's body impedance are combined to achieve verification.

Although RF-Mehndi combines the physical characteristics of the tags with the user's biometric information, it still cannot handle the case where the use's ID card is lost, which brings trouble to the user. Therefore, we design a system that can verify the user by combining its password with its biometric information, without the need for an ID card.

3. Design Background and Overview

In this section, we will introduce passive tags and how they are coupled, as well as the implementation process of our system.

3.1. Passive Tag

Our system uses passive tags, which do not have their own energy source, and obtain working electric energy by reflecting the carrier signals emitted by the reader [29]. An RF tag consists of an antenna and a chip. The main functions of the antenna are: (1) to receive the radio frequency signal emitted by the reader; (2) to transmit it to the chip for processing; (3) to send the chip data to the reader. The antenna is a conductor structure specially designed for coupling radiated electromagnetic energy. In general, the smaller the size of the antenna, the lower its radiation impedance and the working efficiency. Considering the above factors, the tag layout should be as small and simple as possible while still meeting the efficiency requirements. The model of the tag we use is Alien-9629, which measures 22.5 mm × 22.5 mm, and operates at 840–960 MHz.

3.2. Tag Coupling

Tag coupling is actually the energy transfer and information exchange between two devices. There are two ways of tag coupling: Backscatter coupling and Inductive coupling.

3.2.1. Backscatter Coupling

After the user touches the target tag, the electromagnetic wave emitted by the antenna activates it and brings back the tag information. This process is based on the spatial propagation law of electromagnetic waves. The recognition range is greater than 1 m.

Passive tags require sustained energy from electromagnetic waves emitted by the reader to keep working. We know that a changing magnetic field creates an electric field, and a changing electric field creates a magnetic field. When magnetic flux changes, an induced current will be generated in the closed coil. The current in the signal transmitter radiates radio electromagnetic waves through the antenna, forming a changing electromagnetic field. The changing electromagnetic field is induced by the antenna coil at the receiving end, and the voltage is generated inside the coil. The tag can be thought of as a closed coil that generates an induced current inside when it senses the signal emitted by the reader. It should be noted that the induced current generated in the tag will also radiate electromagnetic waves back to the reader antenna after modulation, and generate signals that can be recognized by the reader antenna, also known as backscattered signals.

3.2.2. Inductive Coupling

The inductive coupling is realized through the magnetic field of the tag according to the law of electromagnetic induction. Each tag, when activated, generates a magnetic field around its coil. When two tags are placed close to each other, their magnetic fields pass through each other's coils, resulting in a change in magnetic flux. The induced electromotive force will be generated inside the tag, thus affecting its power and signal. Figure 2 shows the state of a single tag state and the coupling state of two tags. When users touch the surface of one of the tags in the array, the tag circuit is then equivalent to adding an additional resistance, which causes the total resistance in the circuit to change and the tag power to change. Each user has a different body impedance, which makes it possible for the user to have unique biological information and to be distinguished from other users.

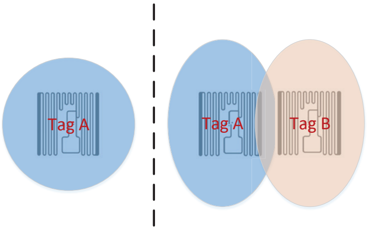


Figure 2. (**Left**) Single tag. (**Right**) Two tags are coupling.

3.3. System Architecture

In this part, we briefly describe the four steps for implementing the RF-Ubia system.

Hardware Settings. In order to realize the password function of RF-Ubia, we need to arrange nine RFID tags into a 3 × 3 layout first. The tag array is then fixed to prevent signal changes caused by the relative movement of the tags from affecting the user authentication results.

Tag Identification. The reader sends a signal to activate the nine tags in the array, then carries out a preliminary identification according to the EPC [30] of the tag. After the reader obtains the signal of the legitimate tag, it waits for the user to touch the corresponding tag and collects the signal data.

Data Processing. The purpose of this step is to process the tag data acquired by the reader to eliminate the inverted π phenomenon and periodic signal surround (i.e., phase unwrapping) of the tag phase. Then, we extract the characteristic information we need and identify the password sequence entered by the user.

User Authentication. The system first determine whether the identified password sequence is a valid password. If the password sequence entered by the user is indeed registered in the system, the second stage of verification will be performed. In the second stage, the system verifies whether the user is legitimate to prevent an illegal attacker from stealing the password sequence of the legitimate users.

4. System Design

In this section, we will describe the working flow of RF-Ubia in four parts, including signal collection, data preprocessing, feature extraction and authentication. Figure 3 depicts these four key steps.

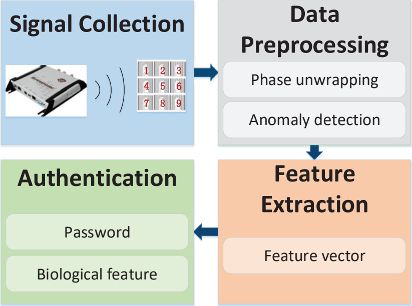


Figure 3. Work flow of the RF-Ubia system.

4.1. Signal Collection

The signal collection part of RF-Ubia is divided into registration stage and verification stage. In the registration stage, each user sets his or her password and touches the tag corresponding to the password in order. As users touch the tags multiple times, their identity information associated with their own password and body impedance is collected. Different impedance and passwords of different users make each person's identity information unique. In the verification stage, the user only needs to enter his or her password set in the registration stage, and the system back-end can obtain the relevant signal data of the tag and complete the authentication.

4.2. Data Preprocessing

The phase is a periodical function with the periodic signal surround and the inverted π phenomenon, which are the essential characteristics of the tag signal. As shown in Figure 4, the figure above shows the wrapped phase, and the figure below shows the inverted π phenomenon of the phase. In order to obtain usable phase characteristics, we need to preprocess the data after getting the tag signal to obtain the tag information with the phase unwrapped and the inverted π phenomenon eliminated.

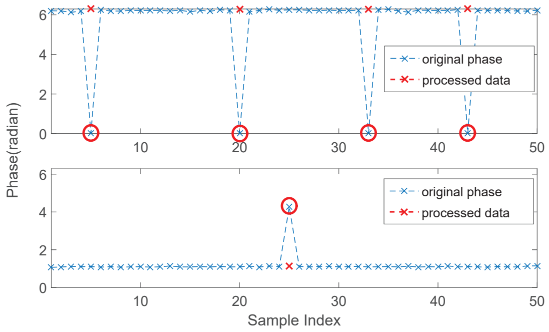


Figure 4. The '×' symbols circled in red represent data with period wrap or phase inverted π, i.e. abnormal data, while the red '×' symbols represent normal data after pre-processing. The figure above shows the wrapped phase. The figure below shows the inverted π phenomenon

In general, the first n data of the tag are the signal data when the tag is more stable, i.e., the tag signal without user touch interference. We select the phase average θ_m of the first n data of the tag as the tag phase reference value. Thus, the difference between the first n phase values of the tag and the reference value, respectively, $\Delta\theta_i = |\theta_i - \theta_m|$, can be obtained.

We handle anomalies by setting thresholds. Since the phase of the tag fluctuates on its own and changes when touched by the user, if the threshold [3] is set too large or too small, it can lead to some data being processed incorrectly and ultimately affect the overall experimental data. We set the threshold value as

$$\begin{cases} thres_1 = \pi - thres, \\ thres_2 = \pi + thres, \end{cases} \quad and \quad \theta_i = \begin{cases} \theta_i, & \Delta\theta_i \leq thres_1 \\ (\theta_i + \pi)mod2\pi, & thres_1 < \Delta\theta_i < thres_2 \\ \theta_i - 2\pi, & \theta_i - \theta_m \geq thres_2 \\ \theta_i + 2\pi, & \theta_i - \theta_m \leq -thres_2 \end{cases} \tag{1}$$

where the value of thres will be selected as the optimal value by iterative adjustment during the experiment. By comparing the difference $\Delta\theta_i$ with the set threshold, if $\Delta\theta_i \leq thres_1$, then the phase is normal data; if $thres_1 < \Delta\theta_i < thres_2$, then it is judged to be an inverted π phenomenon; if $\Delta\theta_i \geq thres_2$, then it is judged to be the occurrence of a phase wrapping phenomenon, as shown in Equation (1).

After processing the first n stable phases of the tag, the subsequent data of the tag are processed using a sliding window. We improve and optimize the processing algorithm because the user touch operation may cause a large abrupt change in the tag phase; for example, touching the tag causes the tag phase to change beyond $thres_1$, which is a phase change caused by the touch operation and not an inverse π phenomenon or a phase wrapping phenomenon. In this case, as the user's touch has a continuous effect on the phase and the inverted π is an episodic phenomenon, we will use the data after this phase to make a judgment. As shown in Equation (2), the average value of this phase θ_k and the m phases after it is taken, and if the difference between the phase value and the average value is small compared to the threshold value $thres_3$, then the phase is not anomalous and does not need to be processed.

$$\left| \theta_k - \frac{\sum_{i=1}^{m} \theta_{k+i-1}}{m} \right| < thres_3. \tag{2}$$

When the user touches the tags in the array, we find that some of them cannot feedback the tag signal. In Figure 5, two adjacent pieces of data are connected by dashed lines. A large amount of signal data is missing between the two pieces of data surrounded by blue circles. This is because the tag power becomes relatively small due to the influence of body impedance and coupling when the user touches, so it cannot reach the threshold value for activating the tag. Therefore, the tag has no phase signal during this touch stage and the reader cannot read the tag data. We take advantage of this phenomenon as a feature when verifying the user's identity. In order to preserve this feature, interpolation and data smoothing processing are not performed.

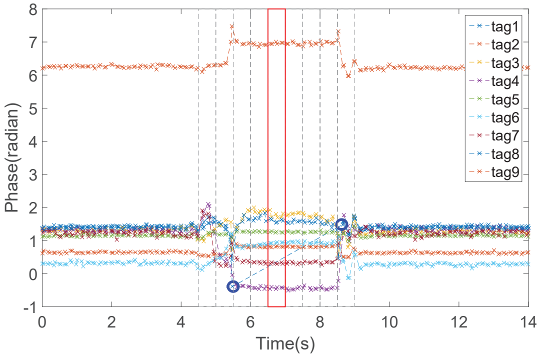


Figure 5. The dashed rectangle represents the window of abnormal phase signal, and the red rectangle represents the feature window. The line between the two blue circles indicates that these windows are more stable feature information. After phase unwrapping, some phase values will exceed the range of 0 to 2π.

4.3. Feature Extraction

After data preprocessing, we obtain a continuously available tag phase signal, and further extract the phase features related to user identity information. We find that the signal changes are relatively complex and chaotic at the moment when the user touches the tag, and the phase characteristics are also unstable. However, during touch, the phase signal of the tag tends to be stable. So, we propose an anomaly detection algorithm to extract the stable part in the middle of the tag phase signal. We first empirically set up a fixed-size window to detect the abnormal part. The average amplitude in the k-th window [2] of tag i can be expressed as

$$A_i(k) = \frac{\sum_{j=1}^{l} \left| \theta_j - \theta_m \right|}{l} \quad and \quad \theta_m = \frac{\sum_{j=1}^{l} \left| \theta_j \right|}{l}, \tag{3}$$

where l represents the data volume of the phase in the window, θ_j represents the phase value, and θ_m represents the average phase value of the tag obtained from the stable tag signal in the first window and is used as a metric to evaluate the anomaly. In Equation (4), the amplitude function $G(k)$ is obtained [2] by summing the amplitudes of all tags in the same window.

$$G(k) = \sum_{i=1}^{9} A_i(k). \tag{4}$$

After sliding window anomaly detection and comparison with the set threshold value, an anomaly sequence can be obtained. The first exception window detected is taken as the left exception window, which is caused by the user just touching the tag. The last one in a continuous set of exception windows starting from the left exception window is taken as the right exception window, which is caused by the user's finger leaving the tag surface. We take the middle window between the left exception window and the right exception window as our feature window. The purpose is to avoid using the more unstable signal caused by the user just touching the tag, and to obtain the relatively stable signal brought by the user's continuous touch. Figure 5 shows the feature window of the tag phase signal. The mean value of the nine tag phases in this window is

$$V = [A'_1, A'_2, A'_3, A'_4, A'_5, A'_6, A'_7, A'_8, A'_9]. \tag{5}$$

Then, the phase difference between any two of the nine tags is calculated to form an eigenvalue:

$$\Delta A_{ij} = \left| A'_i - A'_j \right|. \tag{6}$$

Since ΔA_{ij} and ΔA_{ji} are equal, and ΔA_{ii} is equal to 0, we can obtain 36 effective eigenvalues from a feature window to form the eigenvector

$$F = [\Delta A_{12}, \cdots, \Delta A_{19}, \Delta A_{23}, \cdots, \Delta A_{29}, \Delta A_{34}, \cdots, \Delta A_{89}]. \tag{7}$$

4.4. Authentication

For authentication, we use the classification function in Weka to train the user information collected during the registration stage into the validation model. After collecting user data and extracting feature information, the classification model can determine whether the user is legitimate.

4.5. Experiment and Evaluation

In this section, we first implement RF-Ubia, and then verify its performance through extensive experiments.

The RF-Ubia consists of a commercial reader, a directional antenna and several passive tags. The RFID reader we use is ImpinJ R420 commercial reader, the antenna model is Laird S9028PCR, and the tag model is Alien-9629. The software of RF-Ubia ran on a computer with an Intel(R) Core(TM) i5-3230M processor (2.60 GHz) and 12 GB RAM.

Experimental setups. We carry out the experiment in a conference room. As shown in Figure 6, the tag array formed by 9 Alien-9629 tags is fixed on the top of the box, and the antenna connected to the reader is placed at the bottom of the box to read the tag data. Finally, the data are processed by the computer.

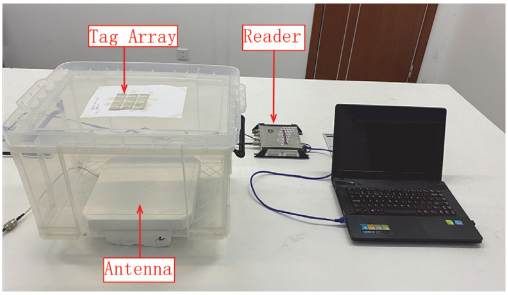


Figure 6. Experimental environment for testing RF-Ubia system.

Parameter Setting. In the data preprocessing stage, we take the first 10 phases of the tag as the signal data when it is stable, and set the size of the sliding window to 6, that is, there are six phases in the window. The sliding window size used in the anomaly detection algorithm is set to 0.5, indicating that the window contains 0.5 s of tag data. The settings for the remaining parameters in the preprocessing and exception detection algorithms are shown in Table 1.

Table 1. Algorithm parameter setting.

Parameter Name	Parameter Values
$thres_1$	$\pi - 1$
$thres_2$	$\pi + 1$
$thres_3$	1.5
$thres_4$	2
m	4

Metric. We use three major indicators to describe the performance of RF-Ubia, namely True Positive Rate (TPR), False Positive Rate (FPR) and Accuracy. TPR [4], as shown in Equation (8), is used to measure the accuracy of a single password identification performance. FPR, as shown in Equation (9), is used to measure the ratio of illegal users that pass the validation of RF-Ubia to all illegal users. Accuracy refers to the combination of the validation results, including the first stage and second stage of RF-Ubia.

$$TPR = \frac{ture\ positives}{ture\ positives + false\ negatives} \tag{8}$$

$$FPR = \frac{false\ positives}{false\ positives + ture\ negatives} \tag{9}$$

First, we evaluate the performance of the system for password identification (i.e., identifying the tags touched by the user). We collected 360 sets of data for evaluation. The TPR of each password (i.e., tag) from 1 to 9 is shown in Figure 7. The average accuracy of the system in identifying passwords exceeds 96.9%, indicating that RF-Ubia can effectively distinguish the tags touched by the user and enable the function of entering passwords.

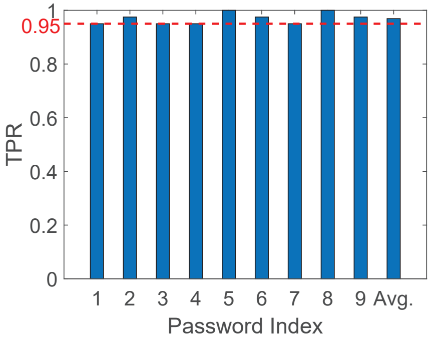


Figure 7. The TPR of RF-Ubia's password identification.

We verify the validity of RF-Ubia when multiple users use the same password. As shown in Figure 8, the FPR of the RF-Ubia does not exceed 0.04 when the password length is 2, indicating that RF-Ubia can effectively distinguish different users. In addition, we also evaluate the accuracy of RF-Ubia in identifying users with the same password when the password is longer. When the password length is 3, the identification accuracy of users with the same password is 98.75%. When the password length is 4, the accuracy reaches 100%. The longer the password is, the more user features can be utilized and therefore the higher the accuracy of user identification is. Considering password identification and user differentiation, the average accuracy of RF-Ubia system exceeds 92.8%.

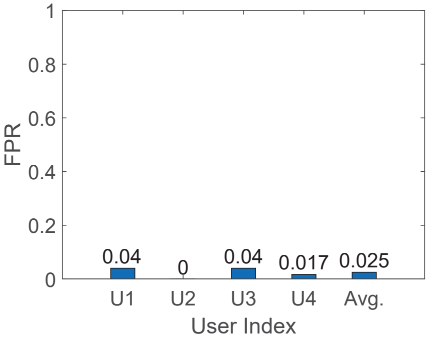


Figure 8. The FPR of RF-Ubia's user validation when multiple users use the same password with a length of 2.

Discussion. In this section, we propose a solution that uses a fusion of user information and biometric information for user authentication, which achieves a high user identification accuracy rate even when using only a simple password. However, it has some drawbacks—we still need to use passwords, which is not friendly to people who usually forget their passwords, such as elderly people with poor memory and those who do not use the authentication system regularly. We also need to try out different experimental environments to improve the robustness of the system. In our experiments, it can be observed that RFID signals are susceptible to dynamic environmental changes (e.g., someone moving), and since the typical bandwidth of normal human finger movements is between 3 and 5 Hz, the use of low-pass filters (e.g., Butterworth filters) is possible to mitigate such effects. For other normal movements of people, they lie between 0 and 18 Hz. Therefore, we can use advanced signal processing techniques (e.g., empirical pattern decomposition) to filter out noise with overlapping frequencies.

5. Extension of Authentication System

In order to make up for the above shortcomings, we refine the biometric technology and propose an authentication method based on the user's physiological and behavioral characteristics. Specifically, we authenticate users by allowing them to touch a specified sequence of tags without entering a specified password.

Behavioral characteristics and time series of touch. When the user touches a fixed tag sequence, he or she may touch it with unique habits or rhythm. As shown in Figure 9, the tag signal obtained by the user's touch contains time information, so an anomaly detection algorithm can be used to detect the signal changes to get the fragments of the user's touch and record the user's touch situation at each moment. Then, the user's touch rhythms, namely, the user's behavioral characteristics, can be extracted using the time series of touch.

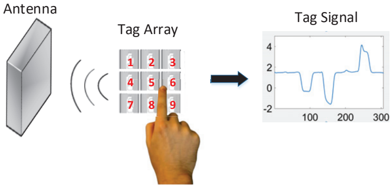


Figure 9. Description of the touch time schematic. The tag signal obtained from the user's touch contains time information, recording the user's touch at each moment.

User Characteristic Information. We use the physiological and behavioral characteristics of users to authenticate their identities. When the user touches the tag surface in the specified order, the system collects information related to the user's body impedance and behavior. After extracting the phase values of the tag touched by the user, the phase difference between two tags is calculated to form the feature value. Each touch of the user generates a feature vector with a length of 36, and the phase features of all the touches form the physiological feature information of the user. In addition, the system can obtain two time values for each touch of the user, that is, the beginning and the end of each touch, as shown in Figure 10. Finally, the user's behavioral characteristic information includes four parts: the duration of each touch, the interval between each touch, the frequency of touch and the duration error of each touch corresponding to the tag.

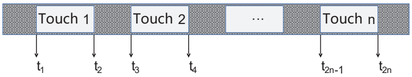


Figure 10. Authentication scheme based on users' physiological and behavioral characteristics. The start and end time of each user touch on the tag can be obtained.

5.1. System Design

In this section, we will introduce the implementation process of the improved system, including five steps of data collection, data preprocessing, anomaly detection, feature extraction and authentication.

Data collection. When registering, the user needs to touch each tag in a tag sequence specified by the system in order. For example, "1379" means that the user needs to touch the four tags 1, 3, 7, and 9 in sequence. The system can collect multiple sets of data when the user touches the tag with its own habits or rhythms. In the authentication phase, the user still only needs to touch the tags according to the tag sequence. Since the tag signal can change drastically with the touch, the user should make each touch last for a short period of time so that the system can obtain relatively stable tag phase values. After collecting the user data, the system needs to perform preprocessing and anomaly detection, and further extract the characteristic information of different users, and finally perform user authentication.

Data preprocessing. The system needs to preprocess the raw data from the user to obtain continuous and stable tag signal. This part is consistent with the data preprocessing method used before the improvement scheme. Specifically, for each tag, the difference between its phase value and the average of the phases values of other tags around it should be calculated to distinguish whether the data are abnormal. Then, compare the value with the set threshold value to determine whether periodic signal surround or inverted π phenomenon occurs, and perform the corresponding data processing according to the determination result.

Anomaly detection. In this scheme, the label signal is detected by the sliding window. After obtaining the exception window using the previous anomaly detection algorithm, we can get the left exception window and the right exception window with fuzzy time characteristics. In the anomaly detection algorithm, if the size and moving step of the sliding window are both large, the time span of the left and right exception window is also large, so the exact time when the user touches the tag cannot be obtain. Therefore, it is necessary to further process the exception window to obtain more accurate time features.

For the left exception window $left$, the sum of its amplitude $G(left)$ is larger than the threshold $thres_4$, while $G(left-1)$ is smaller than the threshold, indicating that the precise time of user touch must be between the left boundary $(left-1)$ of window and the right boundary $left$ of the window. Take the beginning time of the window $(left-1)$ to the end time of the window $left$ as the detection area of the exact time, and set the size and moving step of the sliding window to a smaller time granularity t, and then the average amplitude of the tag phase [2] in the window can be recalculated as

$$A_i'(k) = \frac{\sum\limits_{j=1}^{l} \left|\theta_j - \theta_m\right|}{l} \quad and \quad \theta_m' = \frac{\sum\limits_{j=1}^{5} \theta_j}{5}, \tag{10}$$

where l represents the number of tag phases in the window of size t. The new amplitude function can be obtained [2] from the average amplitude of each tag in the window.

$$G'(k) = \sum_{i=1}^{9} A_i'(k). \tag{11}$$

In anomaly detection, the time of the first window from left to right that detects an anomaly is taken as the precise time of the beginning of user's touch. Similarly, for the right exception window *right*, when the sum of its amplitude $G(right)$ is greater than the threshold $thres_4$, and $G(right+1)$ is less than the threshold, it means that the precise time of user touch must be between the left boundary *right* and the right boundary $(right+1)$ of the window. Take the beginning time of the window *right* to the end time of the window $(right+1)$ as the detection area of the exact time, then the time of the first window from right to left that detects an anomaly is taken as the precise time of the end of the user's touch.

Feature Extraction. So far, we have obtained the tag phase value, the beginning time and the end time of each touch. Using Equations (5)–(7), we can calculate the user's physiological characteristic information $F_{user} = [F_{tag1}, F_{tag2}, \ldots, F_{tagn}]$. The time series of user's multiple touches is

$$[t_1, t_2, t_3, t_4, \ldots, t_{2n-1}, t_{2n}]. \tag{12}$$

Subtracting the start time from the end time of the Kth touch gives the duration of the touch as

$$T_{persist}(k) = t_{2k} - t_{2k-1}. \tag{13}$$

Subtracting the start time of the $(K+1)th$ touch from the end time of the Kth touch gives the time interval between two touches as

$$T_{interval}(k) = t_{2k+1} - t_{2k}. \tag{14}$$

We can obtain n touches, n touch duration and $n-1$ duration between two touches. Then, according to the total time of user touch and the number of touches, the user touch frequency can be calculated as

$$frequency = \frac{n}{t_{2n+1} - t_1}. \tag{15}$$

The user's behavioral characteristic information is composed of the duration, time interval and the frequency of the touch. Therefore, the behavioral characteristic information can be defined as

$$F_{behavior} = [T_{persist}, T_{interval}, frequency]. \tag{16}$$

Finally, the user's physiological and behavioral characteristic information are combined to form the user's identification feature $[F_{user}, F_{behavior}]$.

Authentication. Our system identifies users based on their physiological and behavioral characteristics. Users do not need to remember their passwords, just touch the specified tags in order with their habits and rhythms, and the system can obtain their identity characteristics. In the registration phase, the system needs to collect multiple groups of data (at least 20 groups) as the training data for the classification model. In the authentication phase, users touch the same tag sequence, and the system extracts feature information from the user's touch and uses the classification model to authenticate users. We use the Random Forest classifier in Weka to identify and classify user identities. For each user, there are 20 groups of data for training and 20 groups of data for testing.

During the registration phase, users will need to collect multiple sets of data (a minimum of 20 sets) as training data for the classification model. In the authentication stage, users touch the same label order, the system collects user data and extracts feature information, and finally uses the classification model to authenticate users. User identity is identified and classified by using a Random Forest classifier in Weka. Twenty sets of data per user are used to train the classifier model and 20 sets of data are used as test samples.

5.2. Experiment and Evaluation

In the previous section, we describe the user's behavioral characteristics in detail and introduce how to extract it. We also improve the anomaly detection algorithm and obtain the precise time sequence of user's touches. In this section, we conduct specific experiments to verify the performance of the proposed system.

Experimental setups. The hardware part of the system consists of an RFID commercial reader, a directional antenna and nine passive tags. The RFID reader is an ImpinJ R420 commercial reader, the antenna model is Laird S9028PCR and the tag model is Alien 9629. We implemented the user interface and verification module on a Thinkpad laptop which collects data from the RFID reader through a low-level reader protocal-LLRP. The final data are processed and analyzed by a computer and MATLAB software.

Metric. We evaluate the impact of different lengths of the tag sequence that need to be touched on the performance of the scheme, and the lengths are set to 2, 3 and 4, respectively. In addition, with the sliding window's size is set to 0.3, we evaluate the impact of moving step size of the window on the performance. Different lengths will lead to changes in the amount of physiological and behavioral information of users. The longer the tag sequence, the more information about the user's physiological and behavioral characteristics. As shown in Figure 11, when the length is 2, the recognition rate of the system for users is 90.97%. When the length is 3, this figure increases to 97.92%. When the length is 4, this figure increases to 100%. The results show that the longer the sequence is, the more characteristic information is available, resulting in higher accuracy of user authentication.

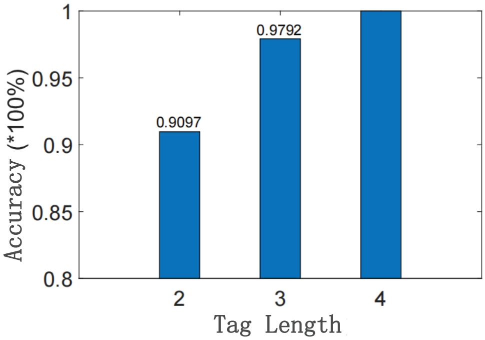


Figure 11. The effect of the length of the specified tag sequence on performance.

Impact of moving step size of the sliding window. In the anomaly detection phase, a different moving step size of the sliding window will lead to a different time accuracy of user's touch obtained by the algorithm, and different time series correspond to different behavioral characteristics of the user. Figure 12 shows the impact of different moving step size of the sliding windows on the performance of user authentication when only behavioral characteristics are used. The results show that the smaller the step size, the higher the accuracy of user authentication. A larger step size leads to poorer performance of authentication.

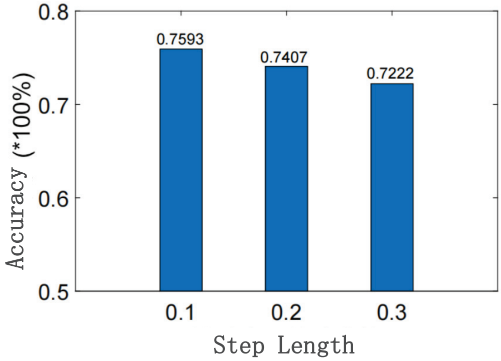


Figure 12. The effect of moving step size of the sliding window on performance.

Impact of the classification model. We evaluated six different classification models. To ensure fairness, we used the network structure and used the default parameter settings used in [31]. As can be seen in Figure 13, Random Forest gives the highest relative accuracy (0.959) for our RF-Ubia, and its latency is small. The rest of the classification models were relatively poor.

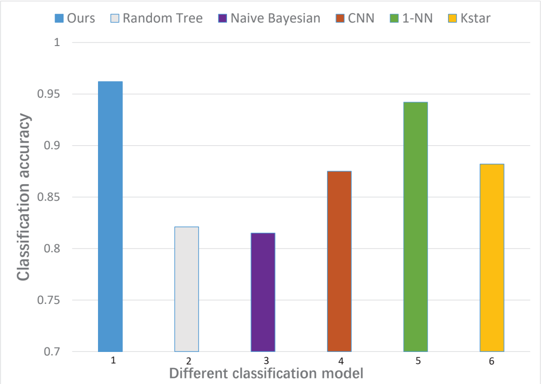


Figure 13. Performance of the system using different classification models.

Time Overhead Evaluation. When the user touches tags for authentication, the time overhead of the system to process the tag signal data can be divided into three parts, including data preprocessing, anomaly detection and feature extraction. When the length of the tag sequence that users need to touch is 4, it takes 0.376 s on average and 0.52 s at most to process a single data sample, and 0.52 s at most, which can satisfy people's daily authentication needs. The time cost of our method could be lower if a computer with better hardware equipment is available or the data processing algorithm can be further improved.

Comparison with State-of-the-art Authentication System. To be fair, we compared the Hu-Fu authentication scheme with other authentication systems in the same experimental environment. As shown in Table 2, in the Hu-Fu [8] authentication scheme, if the authentication tag is stolen by an attacker, the attacker can pass authentication without hindrance; in the RF-Mehndi [10] scheme, although the personal card is also resistant to counterfeiting by an attacker if it is lost or stolen, the need to recreate the user card and the collection of information can still cause problems for the user. Continuous authentication schemes such as VAuth [11] and Cardiac Scan [12], on the other hand, most require the use of specialized sensors, which have significant limitations in terms of cost overhead and applicability.

Table 2. Comparison with the performance of different authentication systems.

	Ours	**HuFu [8]**	**Mehndit [10]**	**VAuth [11]**	**Cardiac [12]**
Cost	Low	Normal	Low	Higher	Higher
Anti-interference	Normal	Normal	poor	Normal	poor
User Friendly	good	Normal	poor	Normal	good
Accuracy over Time	Normal	Normal	poor	good	Normal
Security Performance	good	Normal	Limited	Normal	Normal
Applicability	good	Limited	Normal	Limited	Limited
Mean Accuracy	93.8%	92.6%	90.6%	89.2%	91.2%

5.3. Discussion

We have extended the previous authentication method to incorporate the user's physiological and behavioral characteristics, allowing the user to simply touch a specified sequence of tags in sequence without using a password, where the user's touch habits and rhythm constitute their behavioral characteristics. We have improved the anomaly detection and feature extraction algorithms to more accurately find the start and end points of the action to extract accurate user touch times and improve the accuracy of the system. More experiments are needed for the selection of the classification model, and it is desirable to design an adaptive classifier model to improve the robustness of the system. Experimental results show that the proposed scheme incorporates the physiological and behavioral characteristics of the user and can identify different users with a high degree of accuracy.

6. Conclusions

We propose RF-Ubia, a low-cost user authentication system that utilizes commodity low-cost RFID devices to authenticate based on the user's biometric characteristics. In this work, we take into account different population groups where users can authenticate with or without passwords. We also improve the traditional sliding window anomaly detection algorithm to obtain a more accurate user touch time and compute information about the user's behavioral characteristics. We use the Random Forest classifier in Weka to identify and classify user identities, and extensive experiments show that the proposed system requires only a little training to reliably perform user authentication and detect attackers under random and mimic attacks. Comprehensive experiments have confirmed the high security and practicality of RF-Ubia, with an average accuracy rate of 94% for both authentication methods. RF-Ubia also leaves room for further research, including exploring more potential user behavior and extending more experiments to enhance authentication performance.

Author Contributions: Conceptualization, B.F. and N.P.; methodology, Y.H. and N.P.; Formal analysis, Y.H. and N.P.; writing—original draft preparation, Y.H. and N.P.; writing—review and editing, Y.B.; supervision and project administration, X.L. and S.Z.; funding acquisition, X.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 61772559, 61602167, 62172154), the Hunan Provincial Natural Science Foundation of China under grant No. 2020JJ3016. Xuan Liu's work is partially supported by the National Defense Science and Technology Innovation Special Zone Project of China.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data have been present in main text.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, X.; Yin, J.; Liu, Y.; Zhang, S.; Guo, S.; Wang, K. Vital Signs Monitoring with RFID: Opportunities and Challenges. *IEEE Netw.* **2019**, *33*, 126–132. [CrossRef]
2. Zhang, S.; Liu, X.; Liu, Y.; Ding, B.; Guo, S.; Wang, J. Accurate Respiration Monitoring for Mobile Users With Commercial RFID Devices. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 513–525. [CrossRef]
3. Chen, Z.; Yang, P.; Xiong, J.; Feng, Y.; Li, X. TagRay: Contactless Sensing and Tracking of Mobile Objects using COTS RFID Devices. In Proceedings of the 39th IEEE Conference on Computer Communications, INFOCOM 2020, Beijing, China, 27–30 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 307–316.
4. Han, J.; Ding, H.; Qian, C.; Xi, W.; Wang, Z.; Jiang, Z.; Shangguan, L.; Zhao, J. CBID: A Customer Behavior Identification System Using Passive Tags. *IEEE/ACM Trans. Netw.* **2016**, *24*, 2885–2898. [CrossRef]
5. Pradhan, S.; Chai, E.; Sundaresan, K.; Qiu, L.; Khojastepour, M.A.; Rangarajan, S. RIO: A Pervasive RFID-based Touch Gesture Interface. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, MobiCom 2017, Snowbird, UT, USA, 16–20 October 2017; ACM: New York, NY, USA, 2017; pp. 261–274.
6. Wang, C.; Xie, L.; Wang, W.; Chen, Y.; Bu, Y.; Lu, S. RF-ECG: Heart Rate Variability Assessment Based on COTS RFID Tag Array. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 85:1–85:26. [CrossRef]
7. Wang, C.; Xie, L.; Zhang, K.; Wang, W.; Bu, Y.; Lu, S. Spin-Antenna: 3D Motion Tracking for Tag Array Labeled Objects via Spinning Antenna. In Proceedings of the 2019 IEEE Conference on Computer Communications, INFOCOM 2019, Paris, France, 29 April–2 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 865–873.
8. Wang, G.; Cai, H.; Qian, C.; Han, J.; Li, X.; Ding, H.; Zhao, J. Towards Replay-resilient RFID Authentication. In Proceedings of the the 24th Annual International Conference on Mobile Computing and Networking, MobiCom 2018, New Delhi, India, 29 October–2 November 2018; ACM: New York, NY, USA, 2018; pp. 385–399.
9. Wang, G.; Cai, H.; Qian, C.; Han, J.; Shi, S.; Li, X.; Ding, H.; Xi, W.; Zhao, J. Hu-Fu: Replay-Resilient RFID Authentication. *IEEE/ACM Trans. Mob. Comput.* **2020**, *28*, 547–560. [CrossRef]
10. Zhao, C.; Li, Z.; Liu, T.; Ding, H.; Han, J.; Xi, W.; Gui, R. RF-Mehndi: A Fingertip Profiled RF Identifier. In Proceedings of the 2019 IEEE Conference on Computer Communications, INFOCOM 2019, Paris, France, 29 April–2 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1513–1521.
11. Feng, H.; Fawaz, K.; Shin, K.G. Continuous Authentication for Voice Assistants. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, MobiCom 2017, Snowbird, UT, USA, 16–20 October 2017; ACM: New York, NY, USA, 2017; pp. 343–355.
12. Lin, F.; Song, C.; Zhuang, Y.; Xu, W.; Li, C.; Ren, K. Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, MobiHoc'17, Snowbird, UT, USA, 16–20 October 2017; ACM: New York, NY, USA, 2017; pp. 315–328.
13. Hu, B.; Zhao, T.; Wang, Y.; Cheng, J.; Howard, R.; Chen, Y.; Wan, H. BioTag: Robust RFID-based continuous user verification using physiological features from respiration. In Proceedings of the 23th International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, MobiHoc'22, Seoul, Republic of Korea, 17–20 October 2022; ACM: New York, NY, USA, 2022; pp. 191–200.
14. Zhao, T.; Wang, Y.; Liu, J.; Chen, Y.; Cheng, J.; Yu, J. TrueHeart: Continuous Authentication on Wrist-worn Wearables Using PPG-based Biometrics. In Proceedings of the 2020 IEEE Conference on Computer Communications, INFOCOM 2020, Beijing, China, 27–30 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 30–39.
15. Xu, W.; Liu, J.; Zhang, S.; Zheng, Y.; Lin, F.; Han, J.; Xiao, F.; Ren, K. RFace: Anti-Spoofing Facial Authentication Using COTS RFID. In Proceedings of the 2021 IEEE Conference on Computer Communications, INFOCOM 2021, Vancouver, BC, Canada, 10–13 May 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–10.
16. Wang, Y.; Zheng, Y. TagBreathe: Monitor Breathing with Commodity RFID Systems. *IEEE Trans. Mob. Comput.* **2020**, *19*, 969–981. [CrossRef]
17. Li, T.; Luo, W.; Mo, Z.; Chen, S. Privacy-preserving RFID authentication based on cryptographical encoding. In Proceedings of the IEEE INFOCOM 2012, Orlando, FL, USA, 25–30 March 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 2174–2182.
18. Lu, L.; Han, J.; Xiao, R.; Liu, Y. ACTION: Breaking the Privacy Barrier for RFID Systems. In Proceedings of the INFOCOM 2009, 28th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, Rio de Janeiro, Brazil, 19–25 April 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 1953–1961.
19. Sun, M.; Sakai, K.; Ku, W.; Lai, T.; Vasilakos, A.V. Private and Secure Tag Access for Large-Scale RFID Systems. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 657–671. [CrossRef]
20. Weis, S.A.; Sarma, S.E.; Rivest, R.L.; Engels, D.W. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Computing*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2802, pp. 201–212.
21. Yao, Q.; Qi, Y.; Han, J.; Zhao, J.; Li, X.; Liu, Y. Randomizing RFID Private Authentication. In Proceedings of the Seventh Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2009, Galveston, TX, USA, 9–13 March 2009; IEEE Computer Society: Washington, DC, USA, 2009; pp. 1–10.

22. Ding, H.; Han, J.; Zhang, Y.; Xiao, F.; Xi, W.; Wang, G.; Jiang, Z. Preventing Unauthorized Access on Passive Tags. In Proceedings of the 2018 IEEE Conference on Computer Communications, INFOCOM 2018, Honolulu, HI, USA, 16–19 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1115–1123.
23. Ding, H.; Han, J.; Zhao, C.; Wang, G.; Xi, W.; Jiang, Z.; Zhao, J. Arbitrator2.0: Preventing Unauthorized Access on Passive Tags. *IEEE Trans. Mob. Comput.* **2022**, *21*, 835–848. [CrossRef]
24. Han, J.; Qian, C.; Yang, P.; Ma, D.; Jiang, Z.; Xi, W.; Zhao, J. GenePrint: Generic and Accurate Physical-Layer Identification for UHF RFID Tags. *IEEE/ACM Trans. Netw.* **2016**, *24*, 846–858. [CrossRef]
25. Yang, L.; Peng, P.; Dang, F.; Wang, C.; Li, X.; Liu, Y. Anti-counterfeiting via federated RFID tags' fingerprints and geometric relationships. In Proceedings of the 2015 IEEE Conference on Computer Communications, INFOCOM 2015, Hong Kong, China, 26 April–1 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1966–1974.
26. Chen, X.; Liu, J.; Wang, X.; Liu, H.; Jiang, D.; Chen, L. Eingerprint: Robust Energy-related Fingerprinting for Passive RFID Tags. In Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2020, Santa Clara, CA, USA, 25–27 February 2020; USENIX Association: Berkeley, CA, USA, 2020; pp. 1101–1113.
27. Han, J.; Qian, C.; Wang, X.; Ma, D.; Zhao, J.; Xi, W.; Jiang, Z.; Wang, Z. Twins: Device-Free Object Tracking Using Passive Tags. *IEEE/ACM Trans. Netw.* **2016**, *24*, 1605–1617. [CrossRef]
28. Yang, L.; Chen, Y.; Li, X.; Xiao, C.; Li, M.; Liu, Y. Tagoram: Real-time tracking of mobile RFID tags to high precision using COTS devices. In Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, MobiCom'14, Maui, HI, USA, 7–11 September 2014; ACM: New York, NY, USA, 2014; pp. 237–248.
29. Xi, Z.; Liu, X.; Luo, J.; Zhang, S.; Guo, S. Fast and Reliable Dynamic Tag Estimation in Large-Scale RFID Systems. *IEEE Internet Things J.* **2021**, *8*, 1651–1661. [CrossRef]
30. Liu, X.; Zhang, S.; Xiao, B.; Bu, K. Flexible and Time-Efficient Tag Scanning with Handheld Readers. *IEEE Trans. Mob. Comput.* **2016**, *15*, 840–852. [CrossRef]
31. Zou, Y.; Xiao, J.; Han, J.; Wu, K.; Li, Y.; Ni, L.M. GRfid: A device-free RFID-based gesture recognition system. *IEEE Trans. Mob. Comput.* **2017**, *16*, 381–393. [CrossRef]

applied sciences

MDPI

Article

Digitalization of Fresh Chestnut Fruit Supply Chain through RFID: Evidence, Benefits and Managerial Implications

Marialuisa Menanno [1,*], Matteo Mario Savino [1] and Riccardo Accorsi [2]

[1] Department of Engineering, University of Sannio, Piazza Roma 21, 82100 Benevento, Italy
[2] Department of Industrial Engineering, Alma Mater Studiorum, University of Bologna, Viale Risorgimento 2, 40136 Bologna, Italy
* Correspondence: marialuisa.menanno@unisannio.it

Abstract: This study provides evidence of supply chain (SC) management based on the digitalization of a fresh fruit-supply chain (i.e., chestnuts) using a radio-frequency identification technology (RFID). This research adopted the value-chain operation reference (VCOR) to assess the implications, issues, and benefits of the SC digitalization, and to explore how RFID can be configured regarding the VCOR blocks. Within this framework, the SC stages, processes, and operations were assessed using a tailored performance measurement system (PMS) including a set of metrics tracked, quantified, and evaluated alongside a monitoring field campaign. The results indicated that: (i) the benefits deriving from the RFID are constrained by specific organizational procedures adopted in operations management; (ii) the PMS Indicators of the centralized warehouse, balancing the inventory between the processing line and the distribution channels, presented the most significant improvements across the whole SC.

Keywords: supply chain traceability; radio frequency identification (RFID); value chain; fresh fruit; chestnuts

Citation: Menanno, M.; Savino, M.M.; Accorsi, R. Digitalization of Fresh Chestnut Fruit Supply Chain through RFID: Evidence, Benefits and Managerial Implications. *Appl. Sci.* **2023**, *13*, 5086. https://doi.org/10.3390/app13085086

Academic Editor: Jia Liu

Received: 8 March 2023
Revised: 11 April 2023
Accepted: 14 April 2023
Published: 19 April 2023

1. Introduction

Supply chain management (SCM) is used to plan operations and design SC systems able to meet customer demand within the due date and at the lowest cost. Such a target can be achieved with an efficient SC management that attempts to avoid errors and measure' uncertainties, as well as through the timely and precise monitoring of the inventory at the warehouses [1].

In this context, the value chain pattern [2] allows for the optimization of the SC stages by focusing on the benefits for customers and on certain added-value processes that they are willing to pay for. Nevertheless, value is subjectively perceived and dependent on context [3]. First, products or services may have not the same values worldwide, and furthermore, such values are not constant over time. Secondly, value occurs when needs are met through the provision of products, resources, or services. This is reasonably true for some agri-food products (e.g., fresh fruits, dairy) featured by low added value from suppliers' perspectives.

This study evaluated the problem of SC management in the fresh chestnuts industry with a twofold objective. The first was to explore the drivers of choice for the adoption of RFID technologies in food SC management and how these can be applied toward an enhanced control of chestnut storage/distribution operations. The second objective was to appraise the practical impact of this technology on SC management within the food supply chains. With regard to the undertaken methodology, the framework adopted in the study is the VCOR model, used to unpack the potential application of RFID within this model.

The paper is organised as follows. Section 2 presents a review of the literature focused on the value chain and RFID in SC, while in Section 3, research questions are formulated. Section 4 describes the chestnuts supply chain of the case study and its configuration.

Section 5 relates technical details of RFID deployments, while in Section 6, the operations observed are detailed. Section 7 presents the results of the study, while Section 8 discusses the managerial implications and concludes the work.

2. Literature Review

2.1. The Value Chain Modeling

The VCOR model is organized upon seven attributes, linking the three domains of product development, supply-chain management and the customer chain across the supply networks. The structure of VCOR models supports and enables companies to integrate these three critical domains using one reference model to support the vision of an integrated value chain [4]. VCOR uses a "process-based, common language" of syntax and semantics while, at the same time, creates a base for the successful service-oriented architecture game plan.

The main objective of VCOR is to increase the performance of the SC and support its evolution through four different layers:

The Top Level (TL) of the model includes all the high-level processes. It is depicted through the process categories of plan-govern-execute seen as the "Strategic Level" (SL), where high-level decisions are made on gaining competitive advantages for the whole SC. The VCOR SL has three macro-processes:

- Plan: this balances the current strategic objectives with the current asset status and produces decisions on activities to drive organizations toward the goals;
- Govern: this identifies and enables value-chain rules, policies, and procedures to control the implementation of plans and execute processes;
- Execute: this transforms customers' and product requirements into value-chain features. The executive processes operate within the limits of the management criteria.

The second level of the model contains the processes decomposed from the SL to implement the goals set into a panel of tactics. This level, defined as "Tactical Level" (TL) can be described as an "horizontal value-chain process re-engineering".

The third level of the model regards the gist of this study. This level focuses on the specific processes of the value chain and aids process improvements or process re-engineering, including new technologies deployment and KPI. Over a value chain perspective, this is the level where fine tunings occur.

The VCOR model is based on high-level generic process categories suitable for all types of firms. Yet, the feature that perhaps is the reason for its success is the capability to define the level of performances for each process of the SC and to introduce best practices for the management of productive processes. Table 1 describes the processes considered within the model.

Table 1. VCOR Processes.

Phase	Description
Market	Processes are finalized to understand market's needs and translated into product service requirements
Research	Processes used in assessing, developing and transferring technologies
Develop	Creating the virtual definition and/or prototype of the product/service
Acquire	Procuring goods and services to forecasted or actual SC demand
Build	Transforming product to a finished state to meet the demand
Fulfill	Providing finished goods and services to meet planned or actual demand
Brand	Aligning brand strategy to business strategy and customer touch points
Sell	Activities associated in product/service selling
Support	Maintaining operational/economic performances of products/services

Some interesting applications of VCOR and the value chain can be found in the seminal work of [3], in food wastes problems [5], in [6], and recently in the work of [7], in which the VCOR was implemented with green concepts.

2.2. RFID and Supply Chain

RFID may offer several contributions to SC management, through (i) the identification of products, (ii) ease of communication and (iii) real-time information [8,9].

In the last decade, RFIDs have been applied in different types of supply chains for warehouse management, inventory, and asset management [10,11].

RFID mainly acts toward an efficient location and traceability of products, as well as their visibility throughout the SC [12,13]. Through RFID, companies can achieve better SC management by storing more accurate data in their IT systems [14–16].

These studies, along with the finding of [17], indicate that reengineering models may increase the possible RFID benefits for all processes of distribution centres and retailers, thus enhancing IT-driven service innovation.

Other applications of RFID include: [18] inventory routing problems and [19] the visibility of components in an engineering-to-order SC.

RFID benefits, in terms of competitive advantages, have been assessed by [13] with an interesting investigation in retail networks, while [20] explored potential factors in a vertical SC.

Along the same lines, Ref. [21] explored the potential enabling factors of RFID in SC, when cost and competitiveness are the priorities of firms.

Based on these findings we may argue that RFID can bring the following main benefits: (i) cycle-time reduction, (ii) self-service enabling, and (iii) loss prevention. In the food industry, an interesting application of RFID is the one evaluated by [15], to improve the location of products in stores.

Still in the food sector, Refs. [12,22] reviewed RFID-based systems to address food safety. These studies considered RFID technology as an operational tool able to increase control over SC operations, thereby ensuring higher food-safety targets.

The above findings are supported also by the works of [23] and of [24], who concluded that the benefits of RFIDs are mainly in safety, operation times and labour costs. In this research context, we may argue that the main benefits of RFID are in value-chain management and this view may be supported by others [25,26].

In comparison with recent scientific contributions, the present work aimed to introduce an RFID technology within a fresh-fruit supply chain under the VCOR framework with an attempt to improve operational cycle times, gain real-time information about inventory levels, and improve service levels by tackling delivery errors. Table 2 summarizes the main research objectives of the implementation of RFID to the observed SC. In Table 2, it is worth noting that the RFID technique has not been considered yet in the framework of the VCOR model, with the aim of improving the management of warehousing operations to the best of the authors' knowledge. This paper attempts to fill this gap in the literature.

Table 2. Literature classification regarding the research objectives based on RFID.

Reference	**Research Objective**							
	Efficiency	**Productivity**	**Feasibility Study**	**Cycle Time**	**Inventory Management**	**Security**	**Traceability**	**Delivery Time**
Khan et al. (2020) [27]	✓		✓		✓	✓	✓	
Podduturi et.al (2020) [28]	✓	✓					✓	
Ali and Haseeb (2019) [29]	✓					✓	✓	✓

Table 2. *Cont.*

Reference	Research Objective							
	Efficiency	**Productivity**	**Feasibility Study**	**Cycle Time**	**Inventory Management**	**Security**	**Traceability**	**Delivery Time**
Biswal et al. (2018) [30]	✓					✓		
Tsao et al. (2017) [31]	✓		✓	✓				
Gautam et al. (2017) [32]			✓		✓		✓	
Tian (2016) [33]			✓			✓	✓	
Tanner (2016) [34]	✓				✓	✓	✓	
Shin and Eksioglu (2015) [35]		✓						
Ren (2015) [36]	✓					✓		
Rossi and Pero (2014) [19]			✓				✓	
Chen et al. (2013) [9]	✓		✓					
Laosirihongthong et.al (2013) [21]			✓					
Miaji et al (2013) [37]			✓				✓	
Liu et al. (2012) [22]						✓	✓	
Min et al. (2012) [24]		✓	✓			✓		
Neubert et al. (2011) [17]	✓		✓					
Bendavid and Boeck (2011) [23]							✓	
Sarac et al. (2010) [38]			✓		✓			
Battini et al. (2009) [11]			✓				✓	
Jindae et al. (2008) [25]							✓	
Choy et al. (2007) [16]			✓	✓	✓			✓
Shrikant et al. (2007) [18]			✓					✓

3. Research Questions

Notwithstanding that VCOR is acknowledged as a tool to optimize SC operations, few agri-food supply chains have been able to tap into these potential benefits. In general, the potential applications of IT technologies in the agri-food supply chain have never referred to this model to determine (i) how such technology can be integrated with profit; and (ii) how such a model can be applied to other potential users.

The benefits provided by RFID technology include increased supply-chain visibility, greater speed and efficiency of operations, reduced labor costs, improved security, and better customer service [39]. Some authors expect that RFID will offer more competitive advantages to companies [40,41]. To investigate the potential benefits of RFID in the Value Chain framework, a case study related to chestnuts SC was proposed.

This kind of SC, made of high-quality products with controlled origin-denomination constraints, is featured by specific constraints, such as (i) the bulk storage of fresh fruits, (ii) time-processing constraints after harvesting and (iii) time-deliveryconstraints after processing, to cite a few.

Due to such features, the firm is highly motivated to (i) improve the operations of their SC by processing and distribution sides, (ii) define suitable models for their SC, and within these models define the potential improvements points, and (iii) demonstrate, in real time, the origin of the product to avoid potential frauds by the suppliers.

Several authors have addressed the main benefits of RFID applications in SC [42,43], and the roles of RFID have been clearly highlighted by others [26,35]. Yet, the review of the literature revealed that there are not enough investigations on the potential use and the impact of RFID technologies within the value chain.

Under this framework, the first research question (RQ1) investigated the potential role of the RFID within the value chain as follows:

- RQ1: How can the fresh food SC be configured using the RFID and VCOR model?

The benefits of RFID application in agri-food are widely demonstrated through empirical approaches [24]. In particular, the SC supply chain of chestnuts includes both the fruit supply and the delivery operations to large retailers. Farmers deliver fresh fruits to the producer, who processes them, and in turn delivers them to the distribution channels. Furthermore, for such fruit, some restrictions in the distribution exist with respect to features such as size and weight, that involve an additional selection process to be carried out before processing. In fact, the selection and identification of the batch is mainly based on size and weight. Yet, the chestnuts sector has no practical approach for SC management with IT solutions, and this lack has motivated our research.

The second research question (RQ2) explores the quantitative impacts of RFID on the food-value chain as follows:

- RQ2: Within this SC, what can the impact of RFID technology on warehousing capability be?

4. Materials and Methods

This research was conducted within an SC of chestnuts considering supply, production and distribution operations.

The proposed case study regards a firm that processes and supplies fresh and cooked chestnuts to a firm producing seasonal sweets and operating within qclarge international distribution. After being receive, the fruits are delivered either to (i) distributors or (ii) to multinational firms belonging to the seasonal sweets and cakes sector.

The retailer is registered to the EU with a Protected Geographic Indication. For this reason, some restrictions regarding specific selection parameters (fruits size and weight) impose additional manual selection/calibrating process on fruits.

The SC operations begin with the supply of fresh fruit from the growers to the company. Then, the fruit is selected and dried. The processor pack and deliver the fruit to the sweets' producers or serve their local distribution channels (supermarkets and shops) after shelling, drying and cooking within two parallel ovens. The ovens, propelled by wood pellets, work for 8 h a day.

Based on the processes described, the configuration of the SC includes two types of customers: the multinational cakes industries, and the local clients made of small shops and supermarkets.

The firm produces three main varieties of chestnuts: (i) cooked, (ii) fresh and (iii) dried, where the first two account for more than 77% of the orders. Around 65% of these orders regards fresh ones, while the remaining 35% are cooked ones. The production process decreases the weight to about one-third for fresh fruits and two-thirds for cooked fruits.

Cooked fruits and fresh fruits are packaged in bags of 5 kg and 10 kg, respectively. Each pallet of cooked/fresh fruits contains 30 and 20 bags, as reported in Table 3, which also sums up the volumes of fruits processed during the harvesting season.

Table 3. Material flow in the observed chestnut SC.

SC Phase	Material Flow	
Receiving	895.4 tons	
Quality selection (% scrapes)	10%	
Treatment	Cooked 676 tons	Fresh 138 tons

Figure 1 gives the synoptic of the processing and distribution tasks, with the relative material flows for cooked and fresh fruits.

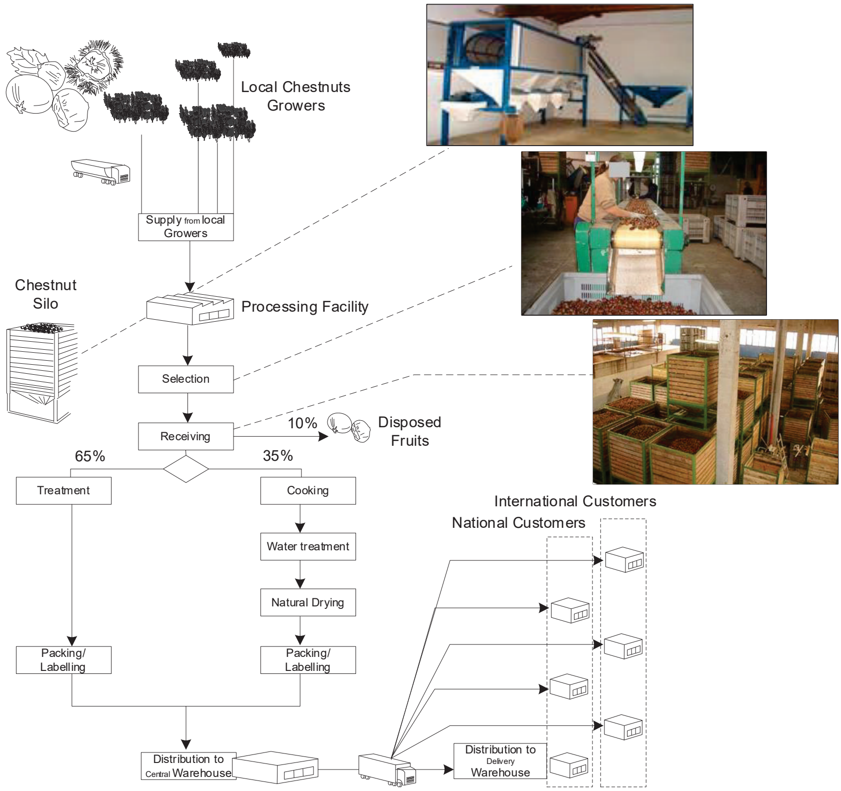


Figure 1. The chestnuts supply chain operations.

From Figure 1, we can see that after the supply of the fresh fruits from local growers, during the selection phase the fruits are separated based on their dimension and weight. The receiving and stocking process is organized into bulky wood silos. In this phase, a first selection of fruits is carried out based on size and destination.

The firm can (i) package the fruits for the main multinational firms, or (ii) make additional shelling, cooking, and packaging processes to serve national distribution centres. The VCOR modelling was developed based on the processing and distribution of chestnuts for the first six customers (in terms of volume), composed of three multinational firms and three national distributors, which together accounted for 70% of fresh and 55% of the cooked fruits processed, respectively.

Value Chain Configuration

This SC can be intended as a three-tiered configuration, in which the firm receives products from the suppliers, then it processes and store them for the distribution phase. The VCOR configuration of the SC proposed by [7], provides the supplier with the fulfill block, and the customer with the acquire block. Table 4 gives the VCOR configuration and the quantities processed at each block. In this table, the modules Acquire, Build, and Fullfill of the VCOR model are involved in the acquiring of the fruits, and in their processing/delivering to the final customers.

Table 4. VCOR configuration and quantities processed.

Supplier Fullfill		Plan Production Company						Final Customer Fullfill			
		Acquire		Build							
Shipping		Receiving		Treatment/Drying/ Cooking *		Packaging		Shipping			
Supplier ID	Fruits [tons]	Scraps	Acquired [tons]	Fresh [tons]	Cooked [tons]	Fresh	Cooked	Multinational Firms		National Distributors	
								Fresh (70%)		Cooked (55%)	
								id	[tons]	id	[tons]
1	500	1%	495	676	138	#Packages 67,600 #Pallets 2103	#Packages 27,600 #Pallets1380				
2	745	2%	730.1								
3	210	1%	207.9					1	250	1	75
4	750	2%	735								
5	400	1%	396					2	225	2	53
6	680	2%	666.4								
7	250	1%	247.5					3	201	3	26

* the values consider the loss of weights relative to the drying and cooking processes.

Based on the literature review regarding the possible benefits of RFID application, this study focuses on the following main improvements:

- Cycle time: the number of overall processes may be reduced by the automation of quantities and documents reading/writing, including data entry, verification, and reporting in the receiving, packaging, and shipping process [9];
- Service quality: Accurate inventory information, enabling efficiency measurements in real time [44];
- Process improvement: reduction of errors, fast checking of quantities, documents matching, zero paperwork [17].

Table 5 summarizes the results of this step by showing the analysis of process requirements at each stage of the logistic processes.

Table 5. Process requirements identification.

Process	Requirement	Error Detected
Fruits storage	Inventory level	+7%
Fruits Identification	Quantities identification based on processes (Fresh/Cooked)	−11%
Fresh packaging	Quantity of bags Quantity of pallets Inventory level updating	−8%
Cooked packaging	Quantity of bags Quantity of pallets Inventory level updating	−4%
Storage	Sorting pallets Pallets identification Inventory level updating	-
Fresh shipping	Quantity definition	−5%
	Pallets picking	
	Finished products inventory level updating	−6%
	Invoice emission	
	Shipping identification (customer)	5
Cooked shipping	Quantity definition	−2%
	Pallets picking	
	Finished products inventory level updating	+1%
	Invoice emission	
	Shipping identification (customer)	9

From Table 5, it can be argued that the main issue of the company lies in product identification and the management of inventory levels at the origin of the SC, where the fruits are separated with regard to fresh/cooking processes. The proper and accurate control at this phase contributes towards avoiding mistakes in updating the inventory level, that may yield bullwhip effects and errors in the other SC processes.

Table 6 shows how the shipping identification errors are double for fresh fruits than for cooked ones. This may be due to the manual counting errors resulting from packages overlapped on the unit load. By process analysis, some basic key performance indicators (KPI) were identified and linked to (i) the blocks of the VCOR and (ii) to the basic specifications of the RFID system.

Table 6. Devices locations and KPI definition.

VCOR Block	RFID Tags Location	Reading System	KPI
Acquire	Receiving warehouse	Flash card in laptop	Fruits inventory level time - For fresh process - For cooking process
Build	Central warehouse	Hand reader	Silos location time Inventory Level time (number of bags) - Fresh - Cooked Packaging time Warehouse cycle - Palletizing time - Transportation and sorting time - Quantity registering - Inventory updating
Fulfill	Shipping warehouse	RFID portal	Warehouse cycle - Quantity check - Picking, Sorting and transportation - Docs issuing - Inventory updating

In this phase, different types of RFID tags and reading systems have been investigated toward the definition of tailored solutions for each VCOR block and process.

The adoption of active RFID tags with localization system might affect such SC operations with impact on the KPI of the fulfill block of VCOR.

Nevertheless, the benefits of RFID technology may be affected by the operational and organizational procedures and the training of operators. Thus, the use of new technologies in certain SCs may imply additional procedures or changes to appraise, in full, the relative benefits.

5. Supply Chain Operations with RFID

The RFID operational environment required replacing and upgrading the traditional Electronic Data Interchange (EDI) system in both facilities (processing and distribution). Before the introduction of the RFID technology, the EDI system was not present in the processing facility, but it was working via a wired LAN in the distribution facility.

The introduction of RFID systems implemented the EDI over a wireless LAN connected with the facility management system. In this phase, traditional batch checking and paper notes are shifted into a paperless communication.

Then, the re-engineering of warehousing operations was conducted. The additional requirements by the side of the operators regarded and additional training on the use of the new technology and for the new packaging and palletizing procedure, in particular the additional training have been made for:

- All operators on the use of the laptop RFID location interface for the processing facility;
- Operators of the central warehouse for the RFID sticking and bags packaging;
- EDI employee on RFID management and maintenance.

Figure 2 shows the inbound process at the receiving warehouse. The procedure is similar for outbound operations. In Figure 2, the continuous and dashed lines indicate material and information flow, respectively, while blue dashed lines indicate the new RFID information flow.

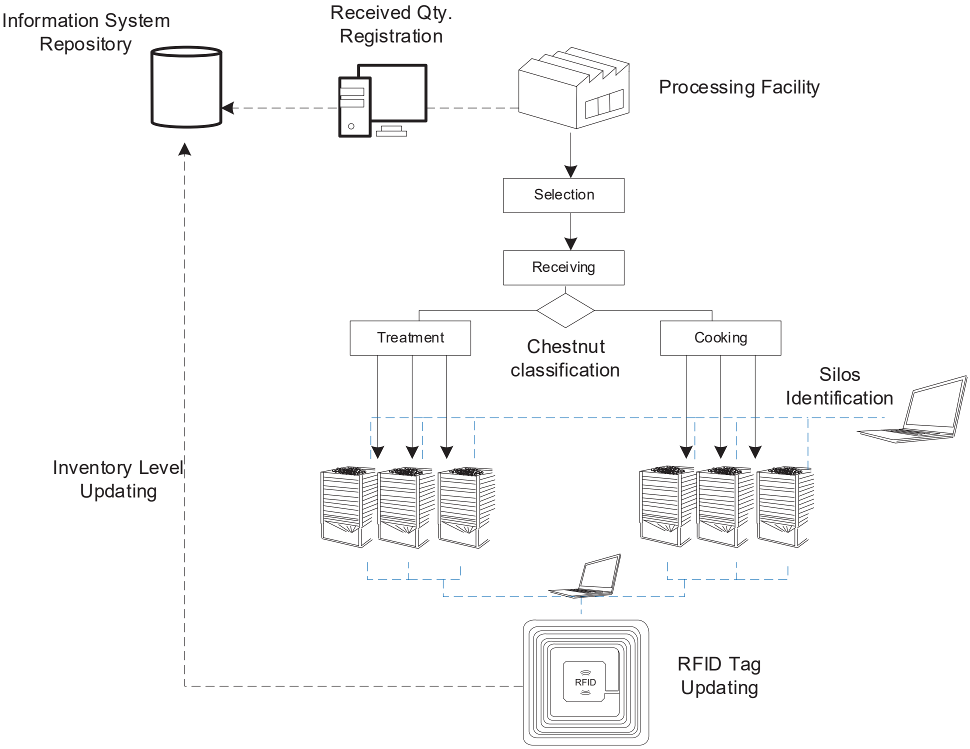


Figure 2. Receiving process with RFID.

The introduction of the RFID technology affects the receiving tasks under operators' perspective. The new procedure includes the following steps:

- Fruits arrive to the processing facility;
- The quantity is checked and registered into the information system;
- The operator moves the fruits to the selection/manual checking area;
- The selectors verify the quality of chestnuts and classify them according to the process to perform (fresh treatment/cooking);
- The warehouse operator identifies the silos where to store the fruits through the software installed on a laptop;
- The silos are then mechanically filled;
- The operator updates the RFID labelling the silos and the inventory level in real time.

Figure 3 shows how the implementation of the RFID system affects the operations within the central warehouse or distribution facility. This warehouse is typically managed according to a push approach. Due to the uncertainty of the fruit-selection process, the quantities of the two types of fruits available at the receiving warehouse may vary with the season and the supplier. As a consequence, processing operations and the shipping to the central warehouse are push-managed with regard to silo availability.

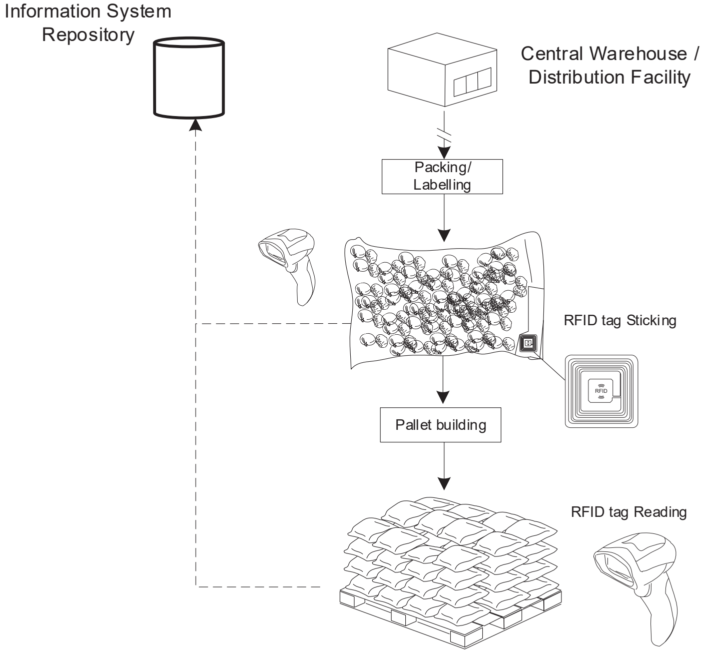

Information System Repository
Central Warehouse / Distribution Facility
Packing/ Labelling
RFID tag Sticking
RFID
Pallet building
RFID tag Reading

Figure 3. Central warehouse operations.

The warehousing operations are managed as follows:

- Warehouse operators pack the products according to the arrivals;
- An RFID is stuck on each package;
- The warehouse inventory level is updated through an RFID handy reader;
- The operator receives the order list, in which the quantities for each type of product are detailed;
- The operator composes the handling unit (HU);
- Each HU is handled and acquired through the RFID gate;
- The warehouse inventory is then updated, transportation documents printed;
- HUs are lastly loaded and shipped.

Figure 4 shows the revised procedures at the delivery warehouse, which operates following a pull approach and performs picking operations accordingly.

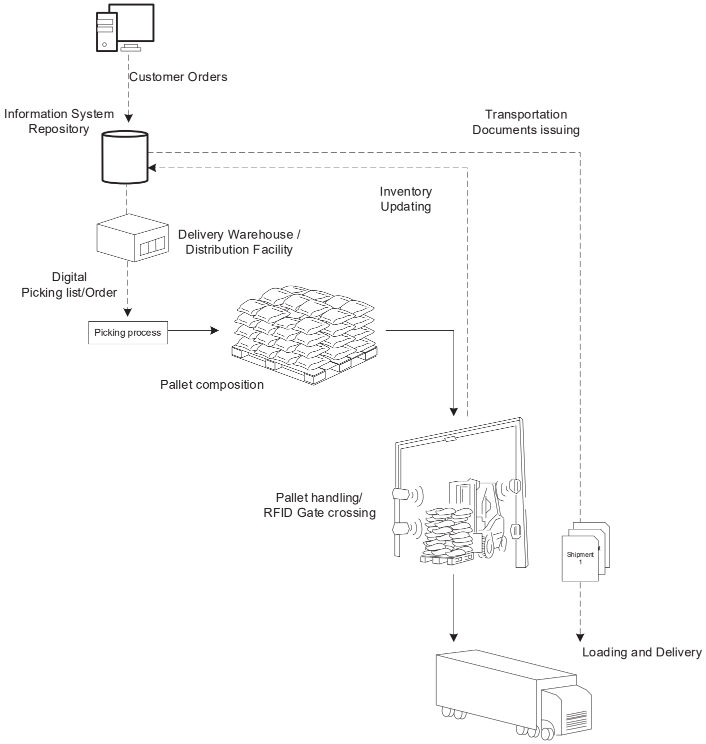

Customer Orders
Information System Repository
Transportation Documents issuing
Inventory Updating
Delivery Warehouse / Distribution Facility
Digital Picking list/Order
Picking process
Pallet composition
Pallet handling/ RFID Gate crossing
Shipment 1
Loading and Delivery

Figure 4. Shipping warehouse operations.

According to this configuration, the central warehouse can be merely intended as a buffer to front the availability uncertainties that characterize the processing activities.

RFID Testing

Under an operations management perspective, it is worth noting how RFID technology may influence: (i) the processing facility, through silos tracing and real-time inventory updating; and (ii) the delivery warehouse, where the real-time issuing of documents and the inventory levels are updated. An experimental campaign of the RFID reading test was conducted. The data in this portion of the study were also used for a preliminary assessment and quantification of the KPIs. During this phase, different locations of tags were tested to enhance the reading rate and avoid the shield effect. This issue was faced by sticking the RFID tag at the top of each bag after it was closed as shown in the Figure 5.

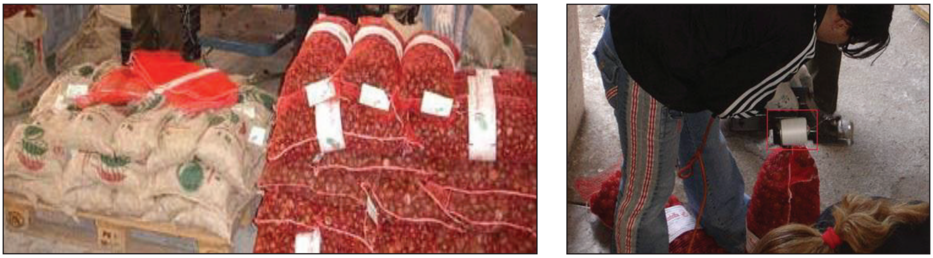


Figure 5. Examples of tagged packages and pallets.

Due to the passive tag stuck on the bags, the company defined new procedures describing ways to lock packages, attach the RFID tag, and to pick/load packages on the pallet.

In the processing facility, the assessment was conducted on five fruit supplies through 40 trails in the central warehouse on 25 fresh bags and 15 cooked bags, on 60 trails in the delivery warehouse on 20 pallets of fresh and 40 of cooked fruits.

The assessment resulted in an identification accuracy of 99.4% for bags and 98.7% for pallets.

6. Technology Specifications

Two types of RFID systems were used in this case study: an active tag for the receiving warehouse and a passive tag for bags and pallets identification in the central and shipping warehouses. The use of the passive tags for the last two blocks was encouraged by the low investment required (less than €0.90 each) for the purchasing of the tags. These tags are often lost or damaged during de-palletizing and the de-packaging processes. RFID tags include an RFID Chip that stores small amounts of data; the RFID antenna that sends and receives radio waves, allowing the tag to communicate with an RFID reader and the substrate to protect the chip and antenna from damage.

Passive tags do not have a built-in power source and rely on the energy transmitted by the RFID reader to function. The RFID reader sends out a radio wave which excites the tag and powers it. The tag uses this energy to transmit its signal to the reader.

This technology is called inductive coupling. The distance between the tag and the reader determines how much power is transferred to the tag. If the tag is too far away, it will not receive enough power to operate. Passive RFID tags are more cost effective than active tags and require no maintenance.

Therefore, passive tags were used for the last two blocks in our study. These tags are often lost or damaged during the de-palletizing and the de-packaging processes and the choice was encouraged by the low investment required (less than €0.90 each) to purchase the tags. The two warehouses were also provided with a wireless network to allow for the communication of the controller with the handy RFID readers and with the information-system repository.

6.1. Active Tag

The active RFID has a transponder embedding a position-marker technology, that is able to identify the proper silos in the receiving warehouse. This feature is necessary to avoid errors made by pickers in choosing between the fruits for the fresh/cooking process. The main features and data for the active tag are reported in Table 7.

Table 7. Main features of the transponder and the active tag.

Feature/Parameter	Value
Frequency	125 kHz
Modulation	100% AM
Range (adjustable)	up to 3.5 m
Position Data	16 bits
Loop Current	max. 6 App
Loop area	Integrated
Number of Loops	1

For the reader device, a flashcard type i-CARD M 350 has been used, with a laptop in a bundle of localization software. This card is able to receive data at distances of up to 500 m with a receiving capacity of around 700 concurrent tags.

The tracking data include location of silos, process type, class and size of fruits, actual quantity (weight) of fruits, dates, or last picking/feeding and related quantities.

6.2. Passive Tags

These tags are used for product identification and track is single package (i.e., bag).

For the specific case a roll RFID is adopted. To comply with the ISO 15963 [45] RFID tags in the range of high frequency 13.56–900 MHz were adopted with a short reading range maximum of approximately 30 cm (12 inches) to 1.5 m.

The data-transmission speed is around 106 bits per second. The antennas are made of aluminium coils. Table 8 lists the other parameters of the tags.

Table 8. Main features of the passive tag.

Feature/Parameter	Value
Frequency	13.56–900 MHz
Chip	I code SLI
Range (adjustable)	1–1.5 m
Memory	12 bytes
Dimension	86 × 54 mm

For the reader device, two commercial systems have been used for the experimental campaign (PDA HP2140 + Reader SDiD1020 beta version), and for the final installation (device PSION work about with reader HF Feig), respectively.

The reading system, compliant with the standards ISO 15693 and 14443A/B [46] and installed into the central warehouse, has been made of two couples of RFID antennas-paddles type-installed at the inbound and outbound docks of the facility.

7. Results

The assessment of the results was conducted in two steps. The first step concerned the comparison of the resulting errors in quantities evaluation and shipments before and after the introduction of the RFID technology. Table 9 reports the requirement for each process and the mean error detected with respect to the previous harvesting season.

Table 9. Improvements evaluations for warehouse management.

Process	Requirement	Mean Error	Difference before and after the RFID Technology.
Fruits storage	Inventory level	+1%	−6%
Fruits Identification	Quantities identification in warehouse based on processes (Fresh/Cooked)	−0.5%	+10.5%
Fresh packaging	Quantity of bags		
	Quantity of pallets		
	Inventory level updating	−0.5%	7.5%
Cooked packaging	Quantity of bags		
	Quantity of pallets		
	Inventory level updating	0%	+4%
Fresh shipping	Quantity definition	−0.3%	+4.7%
	Finished products inventory level updating	0%	+6%
	Shipping identification (customer)	0	2
Cooked shipping	Quantity definition	0%	+2%
	Finished products inventory level updating	0%	+1%
	Shipping identification (customer)	0	5

A set of KPIs was quantified during the as-is configuration and compared to the values tracked during the experimental campaign, the values of which are summarized in Table 9.

From the data of Table 10, we may see an increase of the packaging/palletizing phase time, which is in contrast to the shorter times of inventory updating and documents issuing. From an on-filed analysis, it emerged how such an increase was mainly due to the inexperience of workers when performing the new procedures of package closing, RFID sticking and palletizing. Transportation time was almost constant because the SC re-engineering did not involve warehouses re-layout.

Table 10. KPI of the SC model.

VCOR Block	Quantities		KPI	Values (Avg. Times [min])	
				As-Is	To-Be (RFID)
Acquire	5 conveyances [290]		Fruits inventory level time		
			- For fresh process	50	10
			- For cooking process	30	10
			Silos location time	12	4
Build	[0.32] Number of bags		Inventory Level time (number of bags)		
			- Fresh	90	2
			- Cooked	40	2
			Packaging time (per bag)	4	6
	Fresh	Cooked	Warehouse cycle		
			Palletizing time	11	13
	25	15	Transportation time	8	8
			Inventory updating	12	0
Fulfill	[8] Number of bags		Warehouse cycle		
	Fresh	Cooked	Quantity check	25	5
			Picking, Sorting and transportation time	30	30
	20	40	Docs issuing	12	2
			Inventory updating	16	0

8. Discussion

The empirical results of Table 6 answer to the RQ1 by providing the list of RFID devices and their roles/locations with regard to the VCOR blocks. While the VCOR framework typically provides generic KPIs [46], the empirical finding of Table 6 is the first attempt at defining tailored performance indicators for chestnut SC.

The whole development, implementation, and testing of the RFID technology for this SC may provide multiple answers to RQ2. The results showed that the practical solutions, in terms of operational procedures, complementary to RFID implementation, can highly affect the success of the introduction of this technology. Some of these solutions include the reengineering of packaging and palletizing operations with new procedures. Further evidence lies in the lack of general-purpose technological solutions for any SC environment and operation. The specificity of the SC application and the associated operational and infrastructural constraints are the main aspects to consider when choosing which traceability technology to adopt.

RQ2 is also addressed by Table 10. The RFID system mainly impacts on the Acquire and Fulfill blocks, wherein product tracking and identification affects operations, inventory updating and reading accuracy. Furthermore, palletizing tasks and silo-tracking could be further improved by operator training and practices.

By answering to RQ2, the following technological and managerial considerations can be made: (i) with food products stored in bulk and with different quality parameters, the active RFID technology with a localization system is more suitable for value chain analysis; (ii) for certain SCs, the positive impacts of the RFID technology is affected by the operational procedures and the training of operators in these; (iii) the use of new technologies in SC management may imply additional procedures or changes in traditional procedures to appraise in full the relative benefits.

9. Conclusions

This focused-on-practice research examined a chestnuts SC within a VCOR framework, in which a practical implementation of RFID was implemented and assessed. The SC analysis was driven towards: (i) the RFID implementation by the adoption of different types of tags and tracking methods with respect to the blocks of the VCOR model and (ii) the evaluation of the relative KPIs. The test campaign resulted in a general improvement of inventor level accuracy and updating times. Both the technology deployment and on-field tests also provided clear evidence of the basic needs for such an SC when adopting these technologies.

At the time of this study, the possibilities of fully appraising the benefits of RFID systems in some food SC niches, such as the one explored, had still to be assessed. Thus, we believe that this study can be used not only as a practical guide for RFID implementation in these SCs, but also as a guide for practitioners for the careful analysis of the specific requirements and procedures needed to make a successful application of these technologies. In this regard, one of the main lessons learned is that just well-designed IT solutions may be not sufficient for the success of these projects. In contrast, a manifold tool for the concurrent economic and efficiency analysis and the correct formation and motivation of workers, may be also basic elements that allow these technologies to be as successful as they are expected to be.

Within this study, the following main limitations are reported. First, the KPI analysis concerned a limited material flow and must be further developed. It was conducted with workers not completely trained for RFID use. This may have caused some bias in KPI values, that should be measured with a larger test campaign. Second, the study did not consider economic analysis for this implementation, such as return on investments (ROI) and/or Payback Periods (PBP). Third, the study did not consider the re-engineering of the warehouses layouts and operations that would have improved the other KPIs, such as transportation, sorting and picking.

Author Contributions: Conceptualization, M.M. and R.A.; methodology, M.M.; software, R.A.; validation, M.M., R.A. and M.M.S.; formal analysis, M.M.S.; investigation, M.M.; resources, M.M.; data curation, R.A.; writing—original draft preparation, M.M. and R.A.; writing—review and editing, M.M.S. and R.A.; visualization, R.A.; supervision, M.M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hardgrave, B.C.; Aloysius, J.; Goyal, S. Does RFID improve inventory accuracy? A preliminary analysis. *Int. J. RF Technol. Res. Appl.* **2009**, *1*, 44–56. [CrossRef]
2. Weil, K.E. *PORTER, Competitive Advantage, Creating and Sustaining Superior Performance*; Free Press: New York, NY, USA, 1985; pp. 82–84.
3. Ouzrout, Y.; Savino, M.; Bouras, A.; Di Domenico, C. Supply chain management analysis: A simulation approach to the Value Chain Operations Reference(VCOR) model. *Int. J. Value Chain Manag.* **2009**, *3*, 263–287. [CrossRef]
4. Janse van Rensburg, A.C. The value chain as an operations reference model. *Philipp. Ind. Eng. J.* **2009**, *4*. Available online: https://www.semanticscholar.org/paper/The-value-chain-as-an-operations-reference-model-Rensburg-Antonie/039da33049e04b92b566b28c4759320395ed37ae (accessed on 7 March 2023).
5. Nahman, A.; de Lange, W. Costs of food waste along the value chain: Evidence from South Africa. *Waste Manag.* **2013**, *33*, 2493–2500. [CrossRef] [PubMed]
6. Marchetti, B.; Savino, M.M.; Mazza, A. Lean manufacturing within critical healthcare supply chain: An exploratory study through value chain simulation. *Int. J. Procure. Manag.* **2014**, *8*, 3–24.

7. Savino, M.; Manzini, R.; Mazza, A. Environmental and economic assessment of fresh fruit supply chain through value chain analysis. A case study in chestnuts industry. *Prod. Plan. Control* **2015**, *26*, 1–18. [CrossRef]
8. Deng, M.; Pan Feng, P. A Food Traceability System Based on Blockchain and Radio Frequency Identification Technologies. *J. Comput. Commun.* **2020**, *8*, 17–27. [CrossRef]
9. Chen, J.; Cheng, C.; Huang, T. Supply chain management with lean production and RFID application: A case study. *Expert Syst. Appl.* **2013**, *40*, 3389–3397. [CrossRef]
10. Savino, M.M.; Menanno, M.; Chen, X.; Ragno, P. Exploring the use of RFID in SCOR-based Supply Chain within ERP environment: A case study for stamps distribution. In Proceedings of the 12th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), Phnom Penh, Cambodia, 3–5 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–7.
11. Battini, D.; Faccio, M.; Persona, A.; Sgarbossa, F. A new methodological framework to implement an RFID project and its application. *Int. J. RF Technol. Res. Appl.* **2009**, *1*, 169–193. [CrossRef]
12. Alfian, G.; Syafrudin, M.; Farooq, U.; Ma'arif, M.R.; Syaekhoni, M.A.; Fitriyani, N.L.; Lee, J.; Rhee, J. Improving efficiency of RFID-based traceability system for perishable food by utilizing IoT sensors and machine learning model. *Food Control* **2020**, *110*, 107016. [CrossRef]
13. Pfahl, L.; Moxham, C. Achieving sustained competitive advantage by integrating ECR, RFID and visibility in retail supply chains: A conceptual framework. *Prod. Plan. Control* **2014**, *25*, 548–571. [CrossRef]
14. Rahman, L.F.; Alam, L.; Marufuzzaman, M.; Sumaila, U.R. Traceability of Sustainability and Safety in Fishery Supply Chain Management Systems Using Radio Frequency Identification Technology. *Foods* **2021**, *10*, 2265. [CrossRef]
15. Hong, I.H.; Dang, J.F.; Tsai, Y.H.; Liu, C.S.; Lee, W.T.; Wang, M.L.; Chen, P.C. An RFID application in the food supply chain: A case study of convenience stores in Taiwan. *J. Food Eng.* **2011**, *106*, 119–126. [CrossRef]
16. Choy, K.L.; Stuart, C.K.; Liu, J.; Henry, L.; Kwok, S.K. Improving logistics visibility in a supply chain: An integrated approach with radio frequency identification technology. *Int. J. Integr. Supply Manag.* **2007**, *3*, 135–155. [CrossRef]
17. Neubert, G.; Dominguez, C.; Ageron, B. Inter-organisational alignment to enhance information technology (IT) driven services innovation in a supply chain: The case of radio frequency identification (RFID). *Int. J. Comput. Integr. Manuf.* **2011**, *24*, 1058–1073. [CrossRef]
18. Shrikant, J.; Scott, E.G. RFID-enabled inventory routing problems. *Int. J. Manuf. Technol. Manag.* **2007**, *10*, 92–105.
19. Rossi, T.; Pero, M. RFID technology for increasing visibility in ETO supply chains: A case study. *Prod. Plan. Control* **2014**, *25*, 892–901.
20. Quetti, C.; Pigni, F.; Clerici, A. Factors affecting RFId adoption in a vertical supply chain: The case of the silk industry in Italy. *Prod. Plan. Control* **2011**, *23*, 315–331. [CrossRef]
21. Laosirihongthong, T.; Punnakitikashem, P.; Adebanjo, D. Improving supply chain operations by adopting RFID technology: Evaluation and comparison of enabling factors. *Prod. Plan. Control* **2013**, *24*, 90–109. [CrossRef]
22. Liu, S.; Zhang, D.; Zhang, R.; Liu, B. Analysis on RFID operation strategies of organic food retailer. *Food Control* **2013**, *33*, 461–466. [CrossRef]
23. Bendavid, Y.; Boeck, H. Using RFID to Improve Hospital Supply Chain Management for High Value and Consignment Items. *Procedia Comput. Sci.* **2011**, *5*, 849–856. [CrossRef]
24. Min, Z.; Peichong, L. RFID Application Strategy in Agri-Food Supply Chain Based on Safety and Benefit Analysis. *Phys. Procedia* **2012**, *25*, 636–642.
25. Jindae, K.; Tang, K.; Kumara, S.; Shang-Tae, Y.; Tew, J. Value analysis of location-enabled radio-frequency identification information on delivery chain performance. *Int. J. Prod. Econ.* **2008**, *112*, 403–415.
26. Leung, J.; Cheung, W.; Chu, S.C. Aligning RFID applications with supply chain strategies. *Inf. Manag.* **2014**, *51*, 260–269. [CrossRef]
27. Khan, S.; Asim, M.; Manzoor, S. Impact of Information Technology on Internal Supply Chain Management Implementation of RFID Tags, EJBMR. *Eur. J. Bus. Manag. Res.* **2020**, *5*. [CrossRef]
28. Podduturi, P.R.; Maco, T.; Ahmadi, P.; Islam, K. RFID Implementation in Supply Chain Management. *Int. J. Interdiscip. Telecommun. Netw. (IJITN)* **2020**, *2*, 34–45. [CrossRef]
29. Ali, A.; Haseeb, M. Radio Frequency Identification (RFID) technology as a strategic tool towards higher performance of supply chain operations in textile and apparel industry of Malaysia. *Sci. Uncertain Supply Chain. Manag.* **2019**, *7*, 215–226. [CrossRef]
30. Biswal, A.K.; Jenamani, M.; Kumar, S.K. Warehouse efficiency improvement using RFID in a humanitarian supply chain: Implications for Indian food security system. *Transp. Res. Part E Logist. Transp. Rev.* **2018**, *109*, 205–224. [CrossRef]
31. Tsao, J.C.; Linh, V.T.; Lu, J.C. Closed-loop supply chain network designs considering RFID adoption. *Comput. Ind. Eng.* **2017**, *113*, 716–726. [CrossRef]
32. Gautam, R.; Singh, A.; Karthik, H.; Pandey, S.; Tiwari, M.K. Traceability using RFID and its formulation for a kiwifruit supply chain. *Comput. Ind. Eng.* **2017**, *103*, 46–58. [CrossRef]
33. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings of the 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
34. Tanner, D. Applications for RFID Technologies in the Food Supply Chain. In *Reference Module in Food Science*; Eleviser: Amsterdam, The Netherlands, 2016; ISBN 978-0-08-100596-5.

35. Shin, S.; Eksioglu, B. Empirical study of RFID productivity in the U.S. retail supply chain. *Int. J. Prod. Econ.* **2015**, *163*, 89–96. [CrossRef]
36. Ren, J. RFID enable food supply chain traceability and safety. International Conference on Logistics. In Proceedings of the 2015 International Conference on Logistics, Informatics and Service Sciences (LISS), Barcelona, Spain, 27–29 July 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–5.
37. Miaji, Y.; Mohamed, M.; Daud, N. RFID based improving supply chain traceability. In Proceedings of the IEEE International Conference on RFID-Technologies and Applications (RFID-TA), Johar Bahru, Malaysia, 4–5 September 2013; pp. 1–5.
38. Sarac, A.; Absi, N.; Dauzère-Pérès, S. A literature review on the impact of RFID technologies on supply chain management. *Int. J. Prod. Econ.* **2010**, *128*, 77–95. [CrossRef]
39. Bhattacharya, M.; Chu, C.H.; Hayya, J.; Mullen, T. An exploratory study of RFID adoption in the retail sector. *Oper. Manag. Res.* **2010**, *3*, 80–89. [CrossRef]
40. Ngai, E.W.; Suk, F.F.; Lo, S.Y. Development of an RFID-based sushi management system: The case of a conveyor-belt sushi restaurant. *Int. J. Prod. Econ.* **2008**, *112*, 630–645. [CrossRef]
41. Chow, H.K.H.; Choy, K.L.; Lee, W.B.; Lau, K.C. Design of a RFID case-based resource management system for warehouse operations. *Expert Syst. Appl.* **2006**, *30*, 561–576. [CrossRef]
42. Ustundag, A.; Tanyas, M. The impacts of Radio Frequency Identification (RFID) technology on supply chain costs. *Transp. Res. Part E Logist. Transp. Rev.* **2009**, *45*, 29–38. [CrossRef]
43. Rekik, Y.; Syntetos, A.; Jemai, Z. An e-retailing supply chain subject to inventory inaccuracies. *Int. J. Prod. Econ.* **2015**, *167*, 139–155. [CrossRef]
44. *ISO/IEC 15693-1:2010*; Identification Cards-Contactless Integrated Circuit Cards-Vicinity Cards-Part 1: Physical Characteristics. ISO: Geneva, Switzerland, 2010.
45. *ISO/IEC 14443-1:2008*; Identification Cards-Contactless Integrated Circuit Cards-Proximity Cards-Part 1: Physical Characteristics. ISO: Geneva, Switzerland, 2008.
46. Value Chain Group. VCOR Quick Reference V1R4. 2005. Available online: www.value-chain.org (accessed on 20 January 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

applied sciences

MDPI

Article

Open-Set Specific Emitter Identification Based on Prototypical Networks and Extreme Value Theory

Chunsheng Wang, Yongmin Wang, Yue Zhang *, Hua Xu and Zixuan Zhang

Information and Navigation College, Air Force Engineering University, Xi'an 710077, China
* Correspondence: y.zhang@nwpu.edu.cn

Abstract: Much research has focused on classification within a closed set of emitters, while emitters outside this closed set are misclassified. This paper proposes an open-set recognition model based on prototypical networks and extreme value theory to solve the problem of specific emitter identification in open-set scenes and further improve the recognition accuracy and robustness. Firstly, a one-dimensional convolutional neural network was designed for recognizing I/Q signals, and a squeeze-and-excitation block with an attention mechanism was added to the network to increase the weights of the feature channels with high efficiency. Meanwhile, the recognition was improved by group convolution and channel shuffle. Then, the network was trained with the joint loss function based on prototype learning to complete the separation of intra-class signals and the aggregation of inter-class signals in the feature space. After the training, the Weibull model was fitted for pre-defined classes by incorporating the extreme value theory. Finally, the classification results were obtained according to the known classes and the Weibull model, effectively completing the open-set recognition. The simulation results showed that the proposed model had a higher recognition performance and robustness compared with other classical models for signals collected from five ZigBee and ten USRP 310 devices.

Keywords: specific emitter identification; prototypical networks; open-set recognition; extreme value theory

Citation: Wang, C.; Wang, Y.; Zhang, Y.; Xu, H.; Zhang, Z. Open-Set Specific Emitter Identification Based on Prototypical Networks and Extreme Value Theory. *Appl. Sci.* **2023**, *13*, 3878. https://doi.org/10.3390/app13063878

Academic Editor: Junseop Lee

Received: 4 December 2022
Revised: 11 March 2023
Accepted: 14 March 2023
Published: 18 March 2023

1. Introduction

The large-scale application of wireless communication technology and the advent of the Internet of Things era have prompted the rapid development of a large number of communication devices, along with serious challenges in the fields of communication security and signal reconnaissance. Traditional MAC address and secret key authentication methods are easy to forge and crack, and relying on signal analysis methods to track and identify signals can no longer meet the needs of reconnaissance in complex electromagnetic environments. Specific emitter identification (SEI) can accomplish the authentication and identification of individual emitters by extracting the inherent fingerprint features in signals of different emitters due to hardware manufacturing and other effects [1]. In the field of electronic reconnaissance, the identification of individual features can effectively provide information on non-cooperative targets, track the spatial location of signals, analyze the electromagnetic situation on battlefields, and generate valuable intelligence. In addition, SEI combined with traditional authentication methods, such as secret key and MAC address, can strengthen the recognition and identity authentication of illegal wireless communication devices [1,2] and improve the security performance of communication systems.

According to the working state of the communication emitters, the signal fingerprint features can be divided into transient features and steady-state features. The differences in transient features are obvious and easy to distinguish, but the extraction of transient features requires high-precision equipment and acquisition conditions, since it is susceptible to noise [3–6]. In view of the difficulty of detecting the transient starting point of the signal, Ref. [7] several methods for detecting transient starting points have been developed. Among them, the energy criterion method based on the instantaneous amplitude characteristics was recently shown to be superior.

Compared with transient features, steady-state features are easy to obtain; therefore, the method of extracting RF fingerprints based on steady-state features has been widely researched and applied. For example, the high-order cumulant detection function was constructed to extract the boot signal envelope, and the envelope fractal feature was used to cluster the signal extraction results, which could identify the fingerprinting characteristics of FH radio stations [8]. The fractal features of the FH signal extracted by this method could effectively suppress the noise impact. Ref. [9] proposed square integral bispectra (SIB) to extract the unique stray features of an individual transmitted signal, and the principal component analysis (PCA) method was utilized to extract a low-dimensional classification vector. Then, a support vector machine (SVM) based on the Gaussian kernel function was implemented to complete the classification. The proposed model was highly accurate and robust even in the presence of excessive noise. Ref. [10] proposed an emitter identification based on variational mode decomposition and spectral features (VMD-SF). This method had a lower computational cost than the VMD-EM^2 method and the existing EMD-EM^2 method. However, these feature extraction and classification methods have high complexity. The extracted features are not comprehensive enough, the generalization is not strong, and the recognition accuracy is generally low.

With the rapid development of deep learning technology [11], many researchers have applied it to SEI or signal recognition. For example, Ref. [12] applied the Hilbert–Huang transform to the received signal and converted the Hilbert spectrum into a grayscale image. Then, residual networks were used to learn the visual differences reflected in the Hilbert spectrum images. The simulation results validated that the Hilbert spectrum image was a successful signal representation and demonstrated that the fingerprints extracted from raw images using deep learning were more effective and robust than the expert ones. Similarly, the differential constellation trace figure (DCTF) [13], bispectrum [14] and nonlinear features of the power amplifier, and modulator distortion features [15] of the signal are recognized by different convolutional neural networks (CNNs) for SEI, and all of these methods present substantial performance improvements over traditional methods. However, converting signals into two-dimensional forms such as images increases the model complexity and may cause the loss of some original information related to the signals. Therefore, many researchers have used neural networks to recognize the original sequence signals directly; for example, using one-dimensional CNNs to accomplish the feature extraction and classification of I/Q sequence signals [16–18]. Further, recognition methods based on hybrid networks and complex neural networks have also been proposed [19,20], such as the fusion of CNNs and LSTM. In [19], deep bidirectional long short-term memory (DBi-LSTM) and a one-dimensional residual convolution network with dilated convolution and a squeeze-and-excitation block (Conv-OrdsNet) were devised to extract temporal structure features directly from baseband I/Q samples. Moreover, a data augmentation method was used to overcome the interference of unreliable features. The proposed model could effectively extract reliable RF fingerprinting features from I/Q samples, and the classification results were better than those of most existing methods. Meanwhile, ensemble neural networks were proposed for the recognition of the fusion features of graphs and the sequence features of signals [21]. These methods made use of powerful feature extraction techniques, the self-learning of deep learning, and corresponding data processing methods, which greatly improved their classification performance. In addition, a multi-channel model was established to reduce the effect of channel changes on individual recognition, which effectively improved the recognition accuracy and robustness of the models under the conditions of channel changes and noise [22]. Based on the communication of the physical layer and the support vector data description (SVDD) algorithm, Ref. [23] established a radio frequency fingerprint authentication model for communication devices. Ref. [24] proposed a light-weight radio frequency fingerprinting identification (RFFID) scheme combined with a two-layer model to realize authentication for a large number of resource-constrained terminals under a mobile edge computing (MEC) scenario. The results showed that the novel method could achieve a higher recognition rate than that of the traditional RFFID method by using the wavelet feature effectively, which demonstrated the efficiency of the proposed method. Ref. [25] defined a device-specific unique fingerprint by analyzing solely the inter-arrival time of packets as a feature to identify a device. Thus, they obtained a superior identification model compared with ResNet 50-layer and basic CNN 5-layer architectures.

Most previous research on SEI was based on closed-set scenes, i.e., the same classes of samples were used for both validation and training. However, recognition algorithms for closed-set scenes are difficult to apply to actual electromagnetic environments with open-set properties. In open-set scenes, the samples to be tested may contain new classes that do not appear in the training set, and models trained in a closed set will recognize the new samples as known classes, thus seriously affecting the recognition accuracy. Several researchers have started to research SEI in open-set scenes. Refs. [26,27] used OpenMax [28] based on the extreme value theory (EVT) to recognize the communication emitters and high-resolution range profiles of radar, achieving performance advantages compared with the traditional open-set recognition model. In order to enhance the discriminative power of deeply learned features, Ref. [29] proposed center loss for face recognition tasks. The center loss simultaneously learned a center for deep features of each class and penalized the distances between the deep features and their corresponding class centers. It significantly improved upon previous results and is expected to be used for open-set recognition. Ref. [30] proposed an unsupervised class-distance learning method, which used an auxiliary dataset containing only open classes to learn the decision boundary between closed and open sets and achieved improved results.

In recent years, prototypical networks combining prototype learning ideas and deep neural networks have been used for image recognition under few-shot conditions [31], class-incremental learning [32], and open-set recognition [33]. These methods have achieved better recognition performance compared with traditional CNNs. Prototypical networks have obvious advantages in solving few-shot problems and improving generalization performance. Additionally, the classification principle of prototypical networks is more favorable for open-set recognition.

Based on this, we propose an open-set SEI model for one-dimensional sequence signals by combining prototypical networks and EVT. We creatively introduced an attention mechanism and ShuffleNet into a one-dimensional neural network and combined this prototype network and extreme value theory for the first time to obtain a higher recognition performance and robustness. The results of the experiments on the dataset collected by 5 ZigBee devices and 10 USRP 310 devices showed that the proposed model had a higher recognition accuracy than other models such as OpenMax. The recognition accuracy of the five ZigBee devices reached 95% at 0 dB, and it reached over 90% at a mixed SNR of -4–10 dB for the 10 USRP 310 devices. The contributions of the proposed model are as follows:

1. A one-dimensional CNN integrating an attention mechanism was designed. Meanwhile, group convolution and channel shuffle were introduced into the network, which reduced the complexity and overfitting and effectively improved the recognition performance.
2. Prototype learning was combined with the one-dimensional CNN. Distance-based cross-entropy loss and prototype loss were used to train the network to complete the separation of inter-class signals and the aggregation of intra-class signals in the feature space.
3. Combining EVT, Weibull models were fitted for each known class based on the distance from the sample features to the mean features. The open-set recognition was completed based on the Weibull models and the distance between the features of the test samples and the mean features of known classes.

The rest of the paper is organized as follows. Section 2 introduces the classification principle of the prototypical networks and the basic theory for applying EVT to open-set recognition. Section 3 presents the design of the open-set recognition model, including the network structure, classification algorithm, and loss function. Simulation experiments on five ZigBee devices and an analysis of the simulation results are provided in Section 4. Finally, a brief conclusion is presented in Section 5.

2. Prototypical Networks and Extreme Value Theory

2.1. Prototypical Networks

Prototypical networks, combining neural networks and prototype learning, use the distance between the sample features and the prototypes to measure the attribution of samples, leading to a wide range of applications in fields such as few-shot learning [26]. Prototype learning is a classical algorithm in pattern recognition [34]. With the development of neural networks, prototype learning methods have been integrated into the CNN framework for better performance. Previous CNN models used SoftMax to normalize the output of the fully connected layer and classify the input sample x with the highest probability. The classification is based on:

$$\begin{cases} x \in class \arg \max\limits_{y=1}^{N} p(y|x) \\ p(y|x) = \frac{\exp(\xi_y)}{\sum\limits_{i=1}^{N} \exp(\xi_i)} \end{cases} \tag{1}$$

where $p(y|x)$ represents the probability that sample x belongs to the class y; ξ_i represents the network output of class i, where $i \in \{1, 2, \cdots, N\}$; and N represents the number of known classes. When using prototypical networks for classification, the networks can learn a prototype a_i for each class. Then, the samples can be classified into the class with the closest prototype. The process can be expressed as:

$$x \in class \arg \max_{i=1}^{N} g_i(x) \tag{2}$$

where $g_i(x)$ is the classification function of class i [33]. It can also be expressed as:

$$g_i(x) = -\|f(x;\theta) - a_i\|_2^2 \tag{3}$$

where $f(x;\theta)$ represents the neural network feature extractor, and θ represents the network parameters. $f(x;\theta)$ and the prototype a_i can be learned jointly [33]. During the learning process, the prototype of a certain class is continuously pushed towards the sample features of that class, while the prototypes of other classes are kept away from the sample features of that class.

Prototype learning transforms the classification into the nearest neighbor problem in the feature vector space. The addition of the feature extraction advantages of neural networks can effectively improve the generalization performance and alleviate overfitting. We can also see that the classification principle of prototypical networks and the metrics method based on distance are more conducive to recognizing unknow classes.

2.2. Extreme Value Theory

EVT is a theory dealing with the maximum and minimum values of a probability distribution and is mainly used to predict the probability of extreme events. In 1928, R.A. Fisher and L.H.C. Tipper published their famous paper on EVT [35], which showed that low-probability events obeyed another probability distribution. By analyzing the occurrence of past extreme events and finding their distribution patterns, it is possible to calculate the probability that an extreme event may occur in the future, including the possibility of new events. For example, using historical data of the lowest temperature in a particular location, it is possible to predict the future lowest temperature, including the probability of the record lowest temperatures occurring.

EVT is related to many widely used distributions such as the Weibull distribution. The authors of [36] indicated that within multiple independent distributions, the set of extreme values necessarily converges to an extreme value distribution. Usually, the extreme values in a set of data can be represented by the Weibull distribution. The probability density of the Weibull distribution is expressed as:

$$f_1(x;\alpha,\beta) = \begin{cases} \frac{\beta}{\alpha}\left(\frac{x}{\alpha}\right)^{\beta-1}e^{-\left(\frac{x}{\alpha}\right)^{\beta}} & x \geq 0 \\ 0 & x < 0 \end{cases} \tag{4}$$

where x is the random variable, $\alpha > 0$ is the scale parameter, and $\beta > 0$ is the shape parameter. The cumulative distribution function of the Weibull distribution is expressed as:

$$f_2(x;\alpha,\beta) = \begin{cases} 1 - e^{-\left(\frac{x}{\alpha}\right)^{\beta}} & x \geq 0 \\ 0 & x < 0 \end{cases} \tag{5}$$

According to the properties of the Weibull cumulative distribution function, the Weibull model can be fitted using several maximum values of each class. When the input is far from the distribution of a class, it is probably judged as an extreme value or an outlier by the Weibull model. Thus, the network output of the test samples can be weighted according to the probability, and the score of the samples belonging to the unknown classes can be obtained, which effectively enhances the robustness of open-set recognition.

3. Recognition Model

3.1. Model Framework

The proposed open-set SEI model uses the prototypical networks as the basic structure and incorporates EVT to achieve open-set recognition for I/Q sequence data. The model framework is shown in Figure 1 and is divided into three main modules.

The data-processing module preprocesses the data and then forms the training set and test set according to the preset ratio. In the following training process, classification is performed by the distance from the sample features to the prototypes, and a tight feature space is learned for each class using the joint loss function. After the training, the Weibull model is fitted for each class separately. Thirdly, the testing module obtains the network output of the test samples. Then, the distance of the test samples to the mean features of all known classes is calculated, and the Weibull cumulative distribution probability of the test samples is obtained based on this distance. Finally, the network output is revised by this probability, and the scores of the test samples belonging to the known and unknown classes are obtained.

3.2. Network Structure

The structure of the open-set recognition network is shown in Figure 2. In this study, we directly processed the sequence data with low complexity, so the designed network structure was based on a relatively simple one-dimensional CNN. Four convolution layers exist in the network, and the number of convolutional kernels in each layer is 32, 64, 128, and 256, respectively. A maximum pooling layer with a kernel of two was added after each convolutional layer to reduce the complexity and overfitting of the model, and the final output dimension was reduced by the four-layer network to fully extract the deep features of the data.

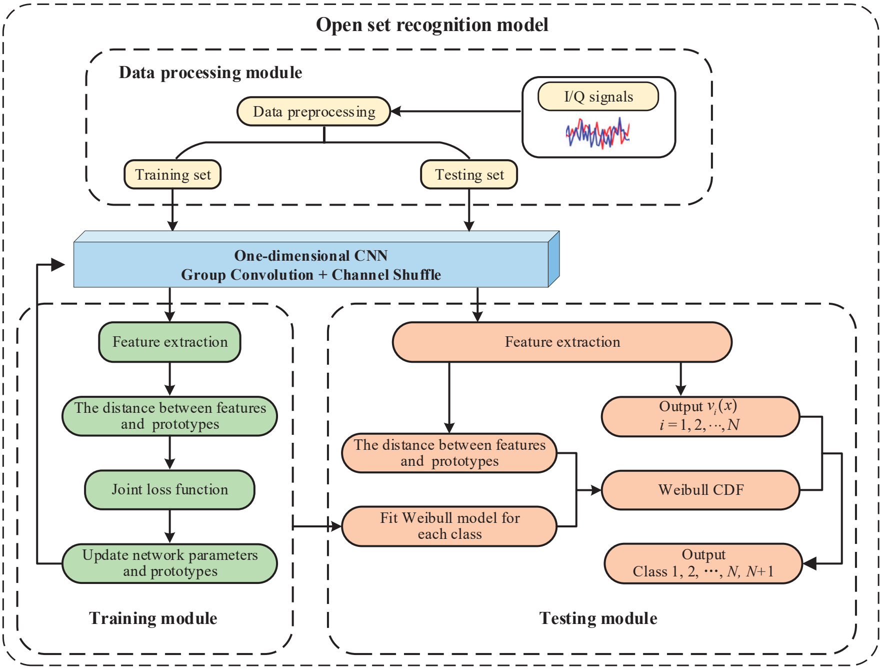

Open set recognition model
Data processing module
I/Q signals
Data preprocessing
Training set
Testing set
One-dimensional CNN
Group Convolution + Channel Shuffle
Feature extraction
The distance between features and prototypes
Joint loss function
Update network parameters and prototypes
Training module
Feature extraction
Output $v_i(x)$ $i=1,2,\cdots,N$
The distance between features and prototypes
Weibull CDF
Fit Weibull model for each class
Output Class 1, 2, ⋯, N, N+1
Testing module

Figure 1. Open-set recognition model based on prototypical networks and EVT.

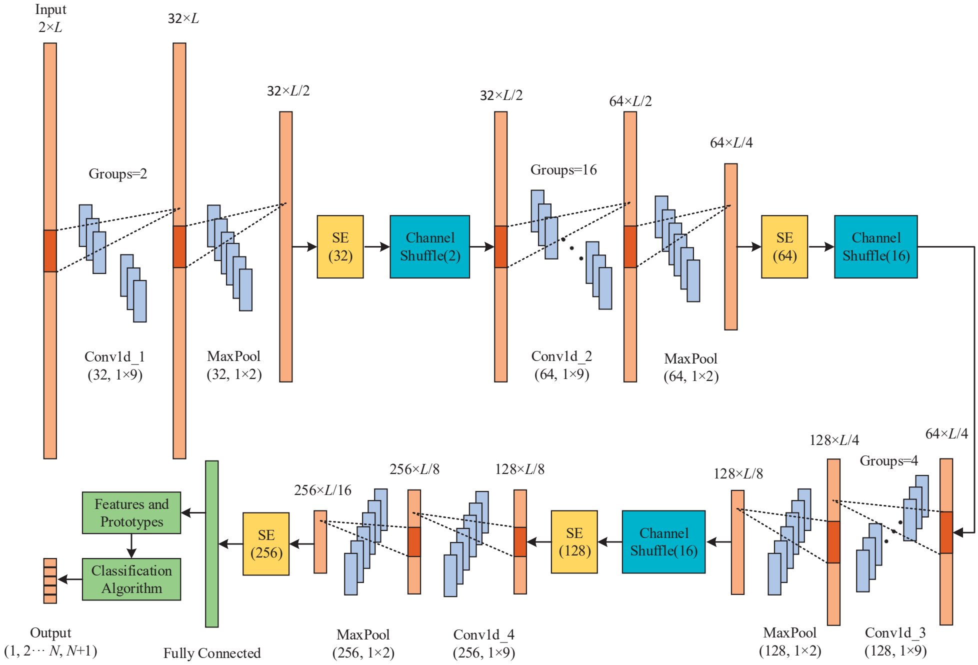


Figure 2. The network structure for open-set recognition.

The convolution kernel size of each convolution layer is 1 × 9. Using larger convolutional kernels allows one to fully extract the temporal information from sequence data. The SE [37] module was added after each pooling operation to further improve the recognition accuracy by adjusting the weights of each channel. The edges of each sample datapoint were complemented by 0 in the convolution operation to ensure that the features were fully extracted and the length of the sample remains unchanged after convolution.

After the convolution layer, the PReLU activation function is used. Its slope is learnable between 0 and 1 at negative values. In neural networks, the weights may be negative when initializing and updating. Using the PReLU activation function ensures that not every output is 0 when the input of the activation function is negative, which can retain the features extracted by the network more comprehensively. After all the convolution operations are completed, the features of the previous layer are dimensionally transformed by the fully connected layer. The fixed-dimension features are outputted, and the updated prototypes are also obtained. Finally, the classification results are provided based on the Weibull model.

3.2.1. Group Convolution and Channel Shuffle

In order to reduce the parameters, complexity, and overfitting, and further improve the recognition accuracy, we introduced the ideas of group convolution and channel shuffle derived from ShuffleNet [38], as shown in Figure 3.

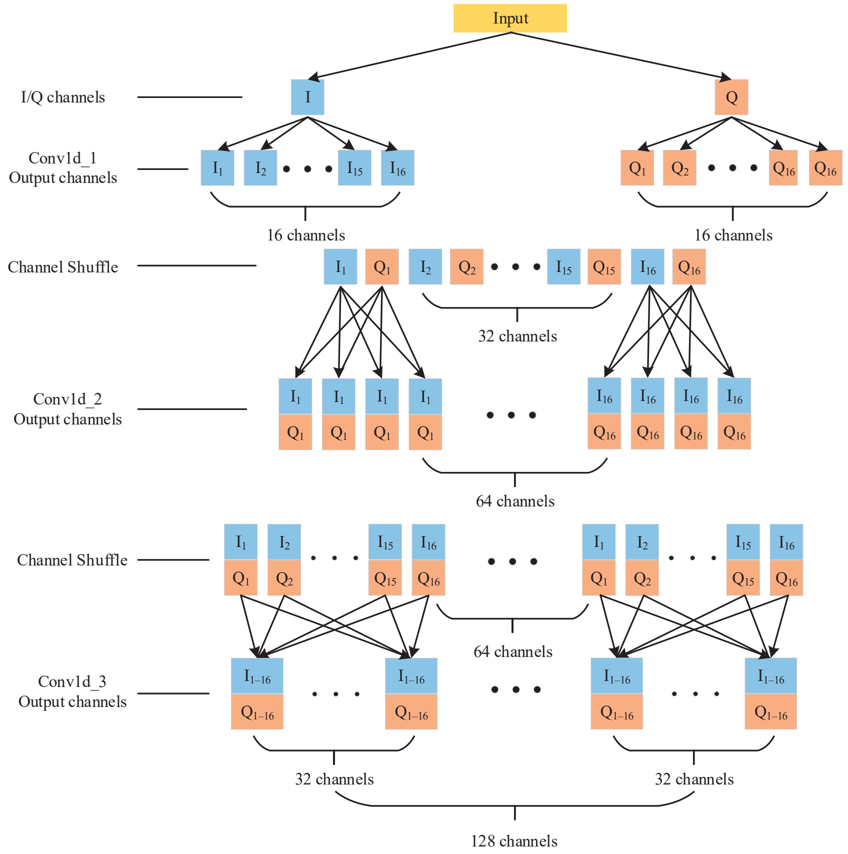


Figure 3. Schematic of group convolution and channel shuffle.

Given that there are two channels of I/Q signals, two convolutional groups extract features for I and Q signals, respectively, in the first convolutional layer. This means that the input and output channels are divided into two groups. Then, the two sets of convolutional kernels are used to perform convolutional operations on the two input channels, respectively, after which their outputs are inputted into the next convolutional layer. The output channels of the first convolutional layer number 32, so there are 16 channels to recognize the I and Q signals, respectively. However, if the next convolutional layer continues to use group convolution, it separates the feature information of the I and Q signals, and the output channels only contain part of the information of the input channels, which subsequently affects the recognition accuracy.

Therefore, we introduced the method of channel shuffle. In the first convolution layer, the output channels with I and Q information are combined in turn to ensure that they are arranged at intervals. In the second convolution layer, group convolution is also used. It is ensured that each group contains I and Q information, leading to 16 groups in this layer. Because the output channels number 64, each group has four output channels. After the convolution operation, the same method of channel recombination is used on the output channels, thus forming four new groups containing information about each previous group. In the third convolution layer, the number of convolution groups is set to four, and the four groups are convolved separately.

3.2.2. Attention Mechanism

The SE module incorporated in the network adopts an attention mechanism, whose main purpose is to automatically obtain the importance of each feature channel in the convolution process through continuous learning. Then, the weights of each channel are learned based on the importance level, which can increase the influence of the effective channel and suppress the channel features with a lesser effect. The one-dimensional SE model is shown in Figure 4, where the input data are $\boldsymbol{X} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_{C'})$, and the features extracted after the convolution operation are $\boldsymbol{U} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_C)$. C and C' represent the channel dimensions. L and L' represent the feature dimensions of each channel. The module is divided into three steps. Firstly, a squeeze operation $F_{sq}(\cdot)$ is performed to compress the feature dimension of each channel to 1. Then, an excitation operation $F_{ex}(\cdot, \boldsymbol{W})$ is performed, leading to a normalized weight between 0 and 1. Finally, the normalized weight is use to weight the features of each channel by the $F_{scale}(\cdot, \cdot)$ operation.

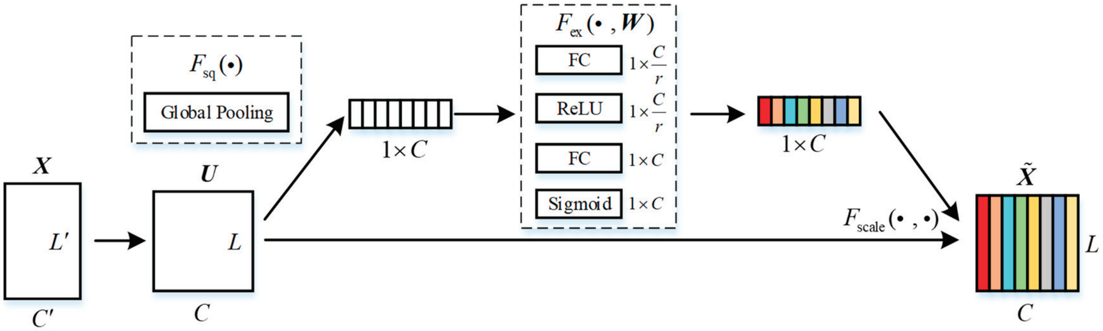


Figure 4. One-dimensional SE model.

3.3. Loss Functions

3.3.1. Distance-Based Cross-Entropy Loss (DCEL)

In prototypical networks, distance is used to measure the similarity between samples and prototypes [30]. Therefore, the distance between the sample (x, y) and the prototype a_i can measure the probability of the sample belonging to the prototype, where x is the sample and y is the label corresponding to x. Based on the analysis in [31], the DCEL can be defined as:

$$l((x,y);\theta,A) = -\frac{1}{K}\sum_{k=1}^{K}\sum_{n=1}^{N} q(y)\log p(y|x) \tag{6}$$

where $A = \{a_i | i = 1, 2, \cdots, N\}$ represents the set of prototypes, $q(y)$ represents the distribution of sample labels, $p(y|x)$ represents the probability that sample x belongs to class y, and K represents the number of samples in a batch.

3.3.2. Prototype Loss (PL)

To further improve the recognition performance of the network while completing open-set recognition, the distance between the intra-class sample features can be reduced by PL [32] during the training period, which expands the inter-class distance by compacting the intra-class signals. Meanwhile, the spatial distribution of the unknown class is expanded based on reducing the feature space of known classes through the constraint of the loss function, which is more favorable to the detection and rejection of unknown classes. PL is defined as:

$$\mathrm{pl}((x,y);\theta,A) = \|f(x) - a_y\|_2^2 \tag{7}$$

where a_y is the prototype of the class y. Minimizing $\mathrm{pl}((x,y);\theta,A)$ reduces the distance between the sample features and the prototypes to which they belong.

3.3.3. Joint Loss

Based on the analysis above, DCEL and PL are combined to train the model. The joint loss [32] can be defined as:

$$L((x,y);\theta,A) = l((x,y);\theta,A) + \lambda\mathrm{pl}((x,y);\theta,A) \tag{8}$$

where λ is the hyperparameter controlling the weight of PL.

By combining DCEL and PL, the recognition accuracy and robustness of the network are further improved. In addition, PL, as a regularization term and a constraint function on the sample space of known classes, alleviates the overfitting of the model. According to the analysis of Equation (8), the intra-class distribution is not tight enough to achieve better recognition performance when λ is too small. However, too large a λ value also excessively increases the tightness of the feature space, aggravates overfitting, and reduces the recognition performance.

3.4. Classification Algorithm

In prototypical networks, a distance threshold determines whether a test sample belongs to an unknown class. However, the robustness of the method is not high enough when a single distance threshold is considered. In addition, the uncertainty of the neural network causes substantial fluctuations in the results of each training and testing procedure. To address this problem, we combined prototypical networks and EVT to obtain the probability of test samples belonging to known and unknown classes through the Weibull model, which further increased the credibility of the classification.

In [28], the Weibull model was fitted using the distance between the activation vector and the mean vector in the penultimate layer of the network. In contrast, our model uses the distance between the feature and the mean feature to fit the Weibull model, which makes each Weibull model more independent under the joint loss function. For a sample outside the class, the probability that it belongs to that class is smaller, which is more robust compared to the OpenMax model. The algorithm in this paper is divided into two main stages: (1) training the network and fitting Weibull model and (2) testing and classification.

3.4.1. Training the Network and Fitting the Weibull Model

The entire process is shown in Algorithm 1. Firstly, parameter r is set to fit the Weibull model, which represents the number of top distances. Then, the network is optimized by the joint loss function, and the prototypical networks are trained using the Euclidean distance. The prototypes are first constructed and initialized for each class according to the feature dimension and the number of classes. After the training samples undergo feature extraction by the network, the distances between the features and each prototype are calculated, along with DCEL and PL. Finally, the network is trained and optimized by DCEL and PL, while updating the network parameters and prototypes a_i. After the training is completed, each class of signals is intra-class tight and inter-class separable in the feature space. The features $f(x_{ij};\theta)$ of correctly classified samples in each class are also obtained, where $j \in \{1, 2, \cdots, J\}$, with J representing the number of correctly classified samples in each class.

Afterwards, the mean features μ_i of the correctly classified samples in each class are calculated, and the distances $d_{ij} = \left\|f(x_{ij};\theta) - \mu_i\right\|$ between the mean features and the features of the correctly classified samples in each class are measured. Then, the set of distances in each class is sorted, and the r largest distances are selected to fit Weibull model, which includes the Weibull shape and scale parameters α_i and β_i.

Algorithm 1 Training the network and fitting the Weibull model

```
step 1: Set the value of $r$ to fit the Weibull model.
step 2: Initialize prototype $a_i$ and network parameters.
step 3: Train the network by minimizing DCEL and PL.
step 4: Update the network parameters and prototypes $a_i$.
step 5: Extract the features $f(x_{ij};\theta)$ of sample $x_{ij}$, with correct classification for each class.
step 6: for $i = 1 \cdots N$ do
            Compute mean features $\mu_i = mean_i\Big(f(x_{ij};\theta)\Big)$
            Fit Weibull model $\rho_i(\alpha_i;\beta_i) = g\Big(\Big\|f(x_{ij};\theta) - \mu_i\Big\|, r\Big)$
        end for
        Return mean features $\mu_i$ and Weibull model $\rho_i$
```

In Algorithm 1, $g\big(\left\|f(x_{ij};\theta) - \mu_i\right\|, r\big)$ is the fitting function [28]. In the fitting process of a class, the samples corresponding to the r largest distances are taken as extreme samples, and the fitted model is used to generate the probability that the test samples belong to this class. The parameter r has an impact on the recognition performance of the model. When the number of samples used gradually increases, the model's ability to reject unknown samples is enhanced, but it also increases the risk of recognizing samples of known classes as unknown ones. Therefore, an appropriate value of r needs to be selected according to the distribution of the data.

3.4.2. Testing and Recognition

The entire process is shown in Algorithm 2. Firstly, the features $f(x;\theta)$ are obtained, and the $v_i(x)$ values of the test sample x are output using the trained prototypical networks. The output values $v_i(x)$ are the probability that the sample belongs to the known classes after the distance measurement by the sample and prototypes, as shown in Equations (2) and (3). Then, the parameter κ is set, where the value of κ suggests the total number of "top" classes to revise. The distances d_i from the test samples to the mean feature of each known class are calculated.

Furthermore, $w_i = 1$ is predetermined, and the network outputs are ranked in descending order. The revision of the Weibull CDF probability is only required for the top κ classes, because the other classes are far from the test samples and have a lesser impact on the classification. Then, the probability $p_{h(t)}$ that the samples belong to outliers of the top κ classes is obtained from the distance calculated in the previous step and the Weibull model of each class. The probability can be expressed as:

$$p_{h(t)} = \rho(d_{h(t)}; \alpha_{h(t)}; \beta_{h(t)}) \tag{9}$$

where $p_{h(t)}$ is the probability that the test sample does not belong to a known class [28]. Then, decreasing weights are needed to scale $p_{h(t)}$, and the revised probability is $p'_{h(t)} = \frac{\kappa-t+1}{\kappa} p_{h(t)}$. The probability of classes far away from the test sample is reduced, because these categories have less impact on the final output score. The revised probability of the test sample belonging to a known class is:

$$\begin{aligned} w_{h(t)}(x) &= 1 - p'_{h(t)} \\ &= 1 - \tfrac{\kappa-t+1}{\kappa} p_{h(t)} \end{aligned} \tag{10}$$

The prototypical network outputs of the test samples are weighted with $\boldsymbol{w}(x)$ to obtain the final outputs of the test samples belonging to the known classes, which represent the attribution of the test samples for each known class. In this step, the robustness of recognition is further enhanced by weighting the network output with revised probability. When the distance between a test sample and the prototype to which the sample belongs is greater than the distance from other prototypes, the sample is incorrectly identified. Adding probability weighting changes the attribution of the test sample, increasing the likelihood that the test sample is recognized as the correct class.

In the following step, the network outputs of the test samples are weighted with $1 - w_i(x)$, which represents the probability that the test samples do not belong to a class, and then the weighted outputs are summed to obtain the final outputs of the test samples belonging to the unknown class. The probability of the classes with a large distance from the test samples is reduced, because those classes have a lesser impact on the classification results.

Lastly, the final probability scores of the test samples belonging to the known and unknown class are obtained by the SoftMax function, and the test samples are classified as the class with the highest probability. In this paper, label 0 was set as the unknown class.

Algorithm 2 Testing and Recognition

```
step 1: Calculate the features $f(x;\theta)$ and outputs $v_i(x)$ of the test samples through the prototypical networks.
step 2: Set the parameter $\kappa$ to revise "top" classes.
step 3: Calculate the distance $d_i$ between $f(x;\theta)$ and $\mu_i$.
step 4: Let $h(t) = \text{argsort}(v_i(x))[:: -1]$, $w_i = 1$
        for $t = 1 \cdots \kappa$ do
            $w_{h(t)}(x) = 1 - \frac{\kappa-t+1}{\kappa}\rho(d_{h(t)};\alpha_{h(t)};\beta_{h(t)})$
        end for
step 5: Revise network outputs $\hat{\boldsymbol{v}}(x) = \boldsymbol{v}(x)\boldsymbol{w}(x)$.
step, 6: Unknown class scores $\hat{v}_o(x) = \sum_{i=1}^{N} v_i(x)(1 - w_i(x))$.
step 7: Compute the final probability $p(y = i|x) = \frac{e^{\hat{v}_i(x)}}{\sum_{n=0}^{N} e^{\hat{v}_n(x)}}$.
step 8: Let $y^* = \arg\max_i p(y = i|x)$; $x$ is classified as an unknown class if $y^* = 0$.
```

4. Experimental Results Analysis

4.1. Experimental Platform and Data Preprocessing

In this section, the performance of the open-set model is evaluated. The dataset used in the experiments came from the signals of five ZigBee devices [13], with a sampling rate of 10 M samples/s, representing ten times the oversampling of the ZigBee 1M chip rate. The carrier frequency of the ZigBee device was set as 2505 MHz with offset quadrature phase-shift keying (OQPSK) modulation, following the IEEE 802.15.4 standard, and the Ettus Research N210 USRP device was used to capture RF waveforms from different ZigBee devices at 2505 MHz. Five segments of signals were available for each device, and each segment was divided into nine small sub-segments, each with about 40,000 sampling points. In the laboratory environment, affected by channel noise, the received signal contained the RF fingerprint characteristics of the devices and the transmission channel characteristics in the indoor environment. In the experiment, three of the five devices were selected as known classes. Four segments of signals from each known class were used as the training set, and the fifth segment of signals from all five devices was selected for the test set.

Meanwhile, in order to verify the generalization of the model, we also used an open-source dataset from the literature [17]. The transmitter used was a USRP 310. The transmitted signal was processed by the MATLAB WLAN toolbox to generate a standard frame, which conformed to the IEEE 802.11a standard. The RF frequency was 2.45 GHz. The signal was received by the B210 radio receiver with a sampling rate of 5 M sample/s. Finally, the RF signal was converted into baseband I/Q data. The experiment used 10 types of signals in the dataset, of which seven were known for training, and the other three were unknown. There were 15,000 samples for each known class and 3750 samples for each unknown class. In order to simulate a more realistic electromagnetic environment, data of mixed SNRs were used for training and testing, and the SNR was evenly distributed between -4 and 10 dB.

All the signals were processed by matlabR2019a. Firstly, the signal power was normalized to eliminate the effect caused by different signal powers. Then, the signals were sliced and supplemented with Gaussian noise. Finally, the signals were processed into fixed-length sequence samples, and the data format of each I/Q sample was 2×800. The performance comparison of the different parameters in the following experiments was conducted on the ZigBee dataset.

The experimental platform contained an NVDIA GeForce RTX3070 GPU, AMD Ryzen 7 5800H CPU. The deep learning framework was PyTorch 1.9.1, with the programming language Python.

Network training parameters: training times N_{epoch} = 40, batch size N_{batch} = 64. The optimizer was Adam [39], and the optimization objective was to minimize the joint loss $L((x, y); \theta, A)$. Adam is an algorithm for the first-order gradient-based optimization of stochastic objective functions, based on adaptive estimates of lower-order moments. The initial learning rate was 0.0005, which was reduced by 50% after each 10 iterations. In Adam, beta1 = 0.9 and beta2 = 0.999, which are the exponential decay rates for the moment estimates, and Epsilon = 1×10^{-8}, which is a term added to the denominator to increase the stability of a numerical calculation. Finally, the weight decay = 1×10^{-5} is a penalty item added to the parameter when it is updated.

4.2. Comparison of Recognition Performance under Different Parameters

4.2.1. Comparison of Recognition Accuracy under Different Loss Functions

In this paper, for ZigBee devices and USRP 310 devices, we set $\kappa = 3$ and $\kappa = 5$, respectively. Meanwhile, the recognition performance was better when $r = 10$ after preliminary experiments. The recognition accuracy is shown in Figure 5, corresponding to different λ values when the SNR varied between −6 and 6 dB. It can be seen that the experimental results verified the theoretical analysis of the PL. The λ value determined the degree of aggregation of each class, which in turn affected the distribution of the distance within and between classes, making the recognition performance vary under different λ values. It was concluded that the recognition accuracy was the highest when λ was about 0.005.

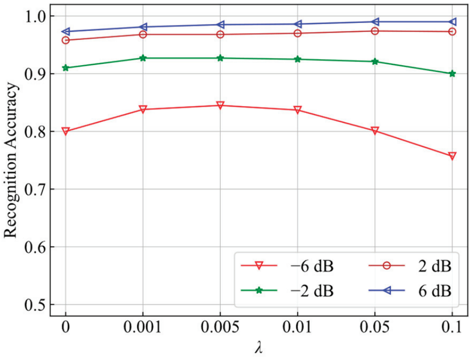
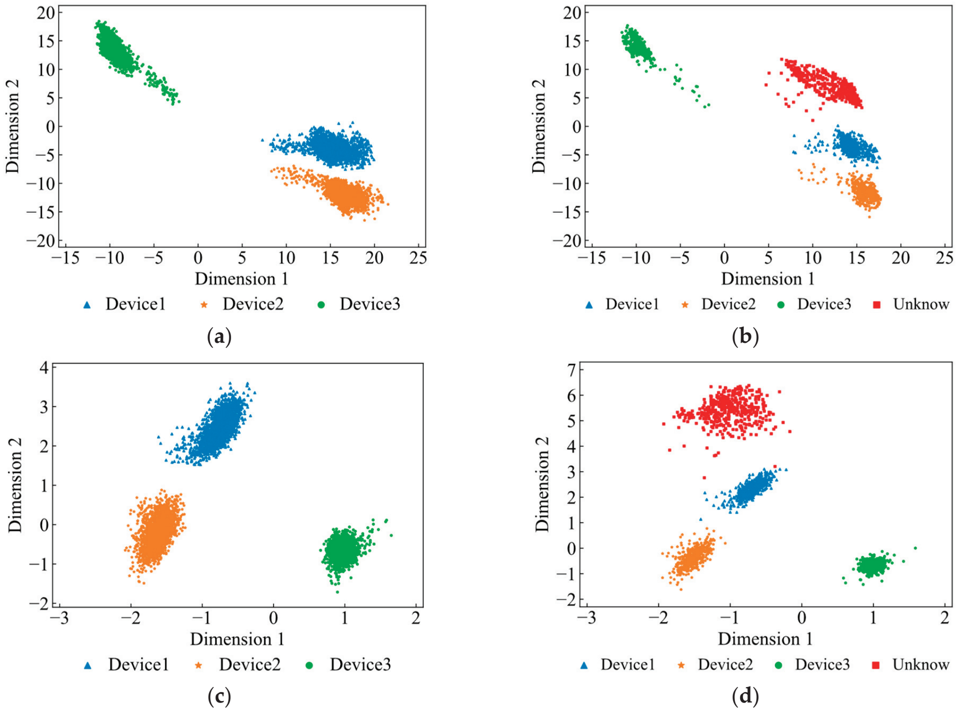


Figure 5. Comparison of recognition accuracy for different values of λ.

When λ increased from 0, the intra-class tightness of each class gradually increased, which then expanded the inter-class distances, improving both the classification ability for known classes and the rejection ability for unknown classes. With the further increase in λ, the recognition performance tended to be stable. When λ was too large, the feature space was excessively tightened in the training period, which resulted in overfitting. Similarly, the influence was more pronounced at a low SNR, so choosing the appropriate λ is critical.

As shown in Figure 6, we extracted the output features of the full connection layer and drew the feature distribution maps under different λ values. According to the analysis of feature distribution, it was concluded that DCEL could complete classification and recognition. When PL was added, the inter-class distances and the distribution of unknown space were amplified by improving the intra-class compactness, which also further separated the known and unknown classes in the feature space and improved the classification performance.



(**a**) (**b**) (**c**) (**d**)

Figure 6. Feature distribution under different values of λ: (**a**) training features when λ was 0; (**b**) testing features when λ was 0; (**c**) training features when λ was 0.005; (**d**) testing features when λ was 0.005.

4.2.2. Comparison of Recognition Accuracy for Different *r* Values

Before fitting the Weibull model for each class, the distances between the correctly classified samples and the corresponding mean features during the training process needed to be sorted, and the Weibull model was fitted using the *r* largest distances of the samples after sorting. The λ value was set to 0.005, and the comparison of the effect of *r* on the recognition performance is shown in Figure 7.

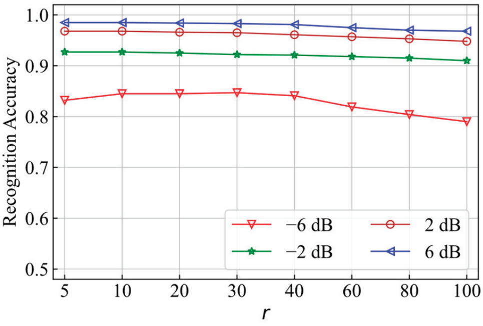


Figure 7. Comparison of recognition accuracy for different *r* values.

The experimental results showed that the recognition accuracy was optimal when *r* was 10–20, and gradually decreased when *r* was too large. This also verified the previous analysis of *r*. Fitting the Weibull model with a large number of samples of known classes increased the probability that the known classes were recognized as unknown ones.

4.2.3. Comparison of Recognition Accuracy with Different Feature Dimensions

In the training and testing process, we used the distances between the sample features and the prototypes to measure the attribution, and the dimensionality change of the features also had an impact on the recognition performance. The experiments were conducted when the other parameters were optimal. Figure 8 shows the recognition performance of the network when the feature dimensions were 2, 3, 4, and 5 and the SNR was −4 dB and 0 dB, respectively. It can be seen that using a lower feature dimension could achieve a higher recognition accuracy, and a higher feature dimension improved only the computational complexity of the network rather than the recognition performance.

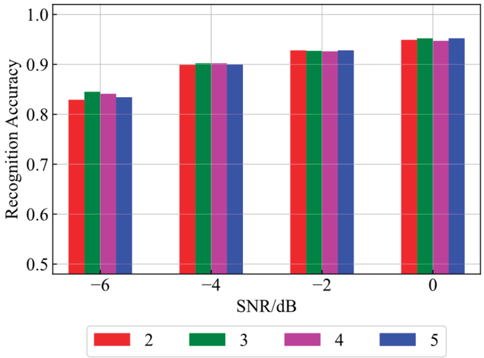


Figure 8. Comparison of recognition accuracy with different feature dimensions.

As shown in Figure 8, the feature dimension had a certain impact on the recognition performance at a low SNR, and the impact became smaller at a high SNR. At the same time, according to the results of several experiments, the recognition accuracy of three-dimensional features was slightly improved compared with that of two-dimensional features. When the dimensions continued to increase, the recognition accuracy did not change significantly, but this increased the network complexity. Therefore, three-dimensional features were finally chosen for the model.

4.3. Comparison of Recognition Performance of Different Models

4.3.1. Comparison of Recognition Accuracy

The comparison of the results from the ZigBee devices is shown in Figure 9. The model in this paper is called EVT-Shuffle-SE. To verify the recognition performance of EVT-Shuffle-SE, the model was first compared with EVT-Shuffle without the SE module and EVT-SE without group convolution and channel shuffle. Then, EVT-Shuffle-SE was also compared with OpenMax [26,27], Center_Loss [29], and CPN [33]. We used the same network structure as CPN, OpenMax, and Center_Loss. It can be seen that the recognition accuracy of the model was effectively improved by introducing the attention mechanism after adding the SE module. EVT-Shuffle-SE with group convolution and channel shuffle also showed a slight improvement over EVT-SE with fewer network parameters. Meanwhile, the model proposed in this paper had an advantage over the other models at a lower SNR. When the SNR was greater than 0 dB, the recognition accuracy of our model reached more than 95%.

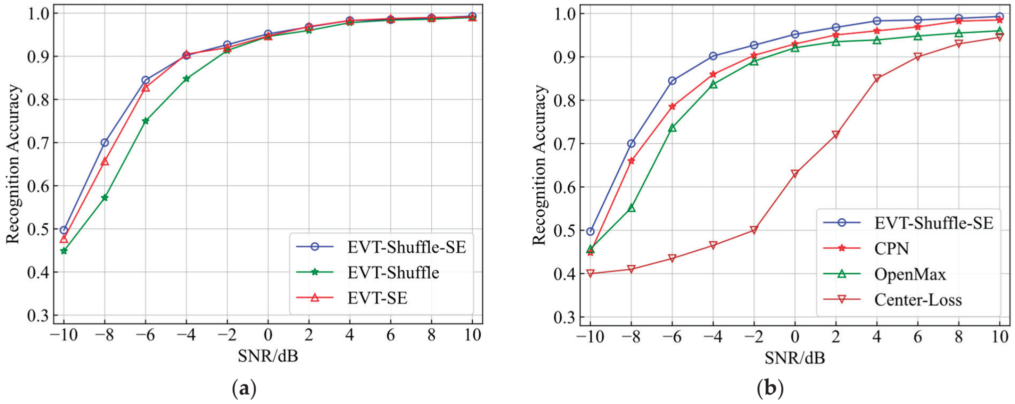


Figure 9. Comparison of recognition accuracy of different models: (**a**) comparison under different modules; (**b**) comparison with other models.

In Figure 10, the confusion matrix for open-set recognition is plotted at −6 dB, −2 dB, 2 dB, and 6 dB, respectively. It can be seen that device 1 and device 2 were easily confused, and device 3 was more independent. Even at a lower SNR, the signals from device 4 and device 5 were successfully rejected as an unknown class.

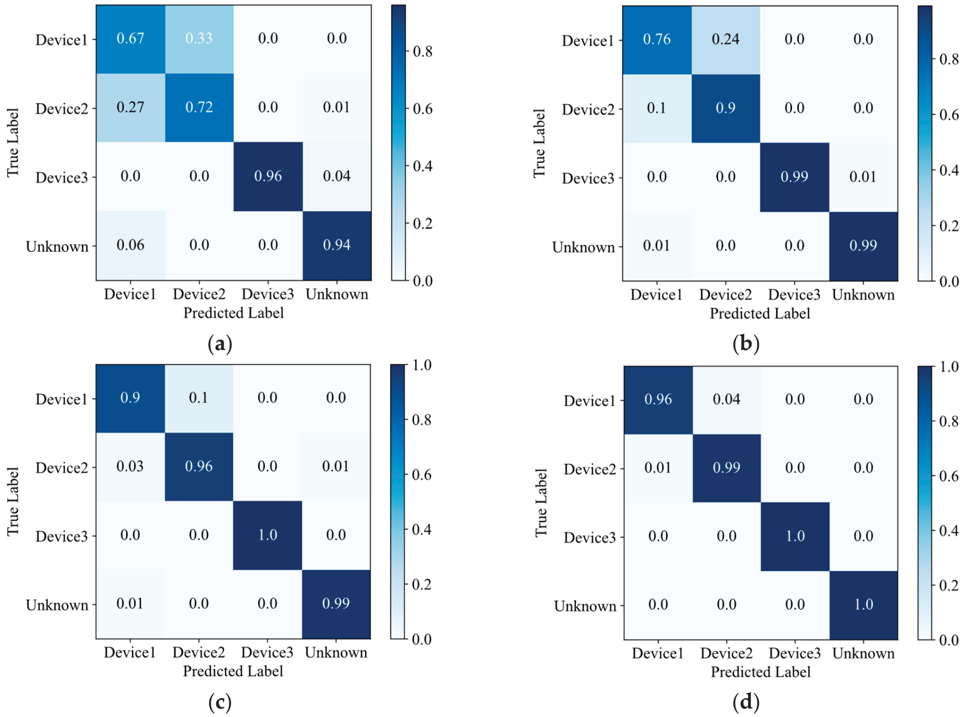


Figure 10. Confusion matrix under different SNRs: (**a**) confusion matrix at −6 dB; (**b**) confusion matrix at −2 dB; (**c**) confusion matrix at 2 dB; (**d**) confusion matrix at 6 dB.

We also conducted experiments on the USRP 310 device. As shown in Table 1, the experimental results demonstrated that the recognition accuracy of the model still reached more than 90% for the 10 types of devices under mixed SNRs. The model also had better recognition performance.

Table 1. Comparison of recognition accuracy of different models.

Models	EVT_PN_Shuffle	OpenMax	CPN	Center_Loss
Recognition Accuracy	90.3%	85.8%	78%	81.5%

Figure 11 shows the confusion matrix for 10 types of devices. It can be seen that the rejection rate for the three unknown devices reached 84%.

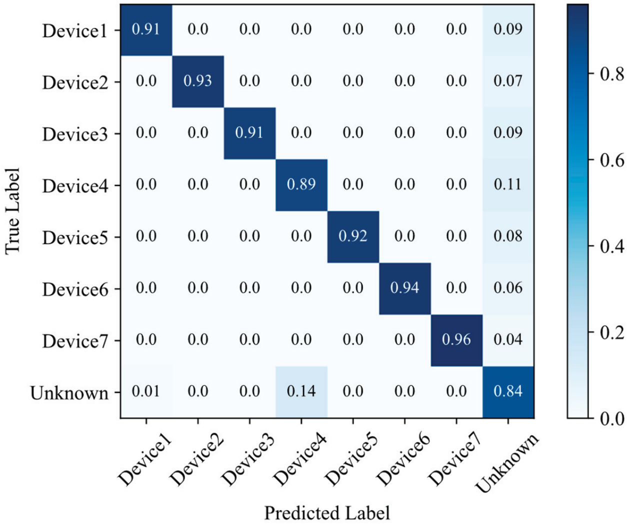


Figure 11. Confusion matrix under mixed SNRs of −4–10 dB.

4.3.2. Comparison of Robustness

During the training process, the initialization of the networks has a severe impact on the results, and it is difficult to ensure that the network achieves optimal recognition by fixing the initial network parameters and weights.

In the CPN model, a fixed distance threshold was used to detect the unknown samples, but the distribution of the sample features changed significantly during each training process. Therefore, the test results after each training fluctuated. In this paper, we incorporated EVT to improve the classification rules. Firstly, prototypical networks and joint loss were used to make the feature space of each class more independent and separate. Meanwhile, the distance was also more suitable for measuring the attribution. Finally, the classification results were weighted and revised by the probability from the Weibull model. Thus, our algorithm effectively increased the robustness and alleviated the influence of the model using the initial parameters, SNR, and instability of the network.

As shown in Figure 12, the test results of the three models were compared after multiple experiments at −4 dB and 0 dB using the ZigBee dataset. The comparison showed that the test results of EVT-Shuffle-SE were more robust, while the CPN and OpenMax models fluctuated more. The fluctuation increased as the SNR decreased. Therefore, the recognition performance of our model was more stable.

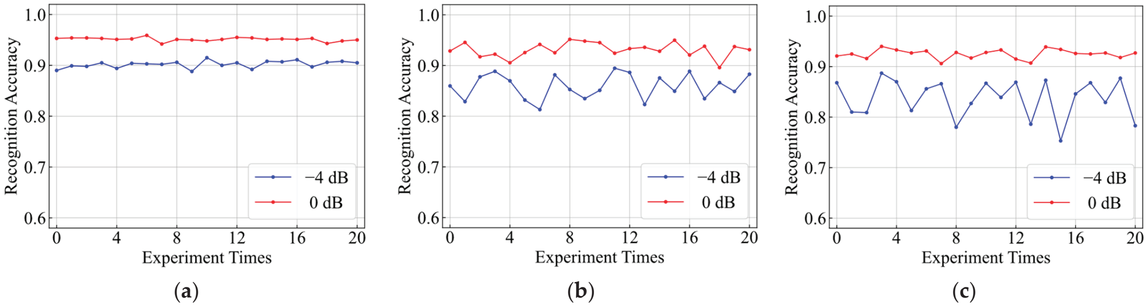


Figure 12. Robustness comparison of different models: (**a**) ours model; (**b**) CPN; (**c**) OpenMax.

5. Conclusions

In this paper, we combined prototypical networks and EVT to achieve open-set SEI. The SE module was added to the one-dimensional CNN to strengthen the classification ability by adjusting the channel weights. Group convolution and channel shuffle strengthened the recognition of I and Q channels, reducing the network complexity and overfitting. In addition to prototype learning, the network was trained by joint loss to complete the separation of inter-class signals and the aggregation of intra-class signals in the feature space. The Weibull models were fitted for each class with the assistance of EVT, and the joint loss function also ensured the independence of each Weibull model. Finally, the weights and Weibull CDF probability were used to revise the network outputs of the test samples, which effectively realized the open-set recognition and improved the stability. Follow-up work should further classify the unknown signals, and the modeling and analysis of these unknown signals should be enhanced.

Author Contributions: Conceptualization, C.W. and Y.W.; methodology, C.W., Z.Z. and Y.Z.; software, C.W. and Z.Z.; validation, C.W. and Z.Z.; formal analysis, C.W. and Y.Z.; investigation, C.W. and Y.W.; resources, C.W. and H.X. data curation, C.W.; writing—original draft preparation, C.W.; writing—review and editing, C.W., Y.Z. and H.X.; visualization, C.W. and Z.Z.; supervision, H.X. and Y.W.; project administration, C.W. and Y.W.; funding acquisition, H.X. and Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, grant number 61906156, and the Postgraduate Innovation Practice Fund of the Air Force Engineering University, grant number CXJ2021075.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Talbot, K.I.; Duley, P.R.; Hyatt, M.H. Specific emitter identification and verification. *Technol. Rev.* **2003**, *113*, 113–130.
2. Nouichi, D.; Abdelsalam, M.; Nasir, Q.; Abbas, S. IoT Devices security using RF fingerprinting. In Proceedings of the 2019 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 26 March–10 April 2019; pp. 1–7.
3. Bihl, T.J.; Bauer, K.W.; Temple, M.A. Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions. *IEEE Trans. Inf. Secur.* **2016**, *11*, 1862–1874. [CrossRef]
4. Patel, H.J.; Temple, M.A.; Baldwin, R.O. Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting. *IEEE Trans. Rel.* **2015**, *64*, 221–233. [CrossRef]
5. Ramsey, B.W.; Temple, M.A.; Mullins, B.E. PHY foundation for multi-factor ZigBee node authentication. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 795–800.

6. Danev, B.; Capkun, S. Transient-based identification of wireless sensor nodes. In Proceedings of the 2009 International Conference on Information Processing in Sensor Networks, San Francisco, CA, USA, 13–16 April 2009; pp. 25–36.
7. Mohamed, I.; Dalveren, Y.; Catak, F.O.; Kara, A. On the Performance of Energy Criterion Method in Wi-Fi Transient Signal Detection. *Electronics* **2022**, *11*, 269. [CrossRef]
8. Yang, Y.S.; Guo, Y.; Li, H.G.; Sui, P. Fingerprint feature recognition of frequency hopping based on high order cumulant estimation. In Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12–14 October 2018; pp. 2175–2179.
9. Xu, S.H.; Huang, B.X.; Xu, L.N.; Xu, Z.G. Radio transmitter classification using a new method of stray features analysis combined with PCA. In Proceedings of the MILCOM 2007-IEEE Military Communications Conference, Orlando, FL, USA, 29–31 October 2007; pp. 1–5.
10. Udit, S.; Nikita, T.; Gagarin, B. Specific emitter identification based on variational mode decomposition and spectral features in single hop and relaying scenarios. *IEEE Trans. Inf. Secur.* **2018**, *14*, 581–591.
11. Lecun, Y.; Bottou, L. *Gradient-Based Learning Applied to Document Recognition*; IEEE: New York, NY, USA, 1998; Volume 86, pp. 2278–2324.
12. Pan, Y.W.; Yang, S.H.; Peng, H.; Li, T.Y.; Wang, W.Y. Specific emitter identification based on deep residual networks. *IEEE Access* **2019**, *7*, 54425–54434. [CrossRef]
13. Peng, L.N.; Zhang, J.Q.; Liu, M.; Hu, A.Q. Deep learning based RF fingerprint identification using Differential Constellation Trace Figure. *IEEE Trans. Veh. Technol.* **2019**, *69*, 1091–1095. [CrossRef]
14. Ding, L.D.; Wang, S.L.; Wang, F.G.; Zhang, W. Specific emitter identification via convolutional neural networks. *IEEE Commun. Lett.* **2018**, *22*, 2591–2594. [CrossRef]
15. Chen, Y.; Chen, X.; Lei, Y. Emitter Identification of Digital Modulation Transmitter Based on Nonlinearity and Modulation Distortion of Power Amplifier. *Sensors* **2021**, *21*, 4362. [CrossRef]
16. Merchant, K.; Revay, S.; Stantchev, G.; Nousain, B. Deep learning for RF device fingerprinting in cognitive communication networks. *IEEE J. Sel. Top. Signal Process.* **2018**, *12*, 160–167. [CrossRef]
17. Sankhe, K.; Belgiovine, M.; Zhou, F.; Angioloni, L.; Restuccia, F.; D'Oro, S.; Melodia, T.; Ioannidis, S.; Chowdhury, K. No Radio Left Behind: Radio fingerprinting through deep learning of Physical-Layer hardware impairments. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *6*, 165–178. [CrossRef]
18. Qing, G.W.; Wang, H.F.; Zhang, T.P. Radio frequency fingerprinting identification for Zigbee via lightweight CNN. *Phys. Commun.* **2021**, *44*, 101250. [CrossRef]
19. Liu, Y.H.; Xu, H.; Qi, Z.S.; Shi, Y.H. Specific emitter identification against unreliable features interference based on Time-Series classification network structure. *IEEE Access* **2020**, *8*, 200194–200208. [CrossRef]
20. Wang, Y.; Gui, G.; Gacanin, H.; Ohtsuki, T.; Dobre, O.A.; Poor, H.V. An efficient specific emitter identification method based on Complex-Valued neural networks and network compression. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 2305–2317. [CrossRef]
21. Xing, C.; Zhou, Y.; Peng, Y.; Hao, J.; Li, S. Specific Emitter Identification Based on Ensemble Neural Network and Signal Graph. *Appl. Sci.* **2022**, *12*, 5496. [CrossRef]
22. Gutierrez del Arroyo, J.A.; Borghetti, B.J.; Temple, M.A. Considerations for Radio Frequency Fingerprinting across Multiple Frequency Channels. *Sensors* **2022**, *22*, 2111. [CrossRef] [PubMed]
23. Tian, Q.; Lin, Y.; Guo, X.; Wang, J.; AlFarraj, O.; Tolba, A. An Identity Authentication Method of a MIoT Device Based on Radio Frequency (RF) Fingerprint Technology. *Sensors* **2020**, *20*, 1213. [CrossRef] [PubMed]
24. Chen, S.; Wen, H.; Wu, J.; Xu, A.; Jiang, Y.; Song, H.; Chen, Y. Radio Frequency Fingerprint-Based Intelligent Mobile Edge Computing for Internet of Things Authentication. *Sensors* **2019**, *19*, 3610. [CrossRef] [PubMed]
25. Aneja, S.; Aneja, N.; Bhargava, B.; Chowdhury, R.R. Device fingerprinting using deep convolutional neural networks. *Int. J. Comm. Netw. Distr. Syst.* **2022**, *28*, 171–198. [CrossRef]
26. Hanna, S.; Karunaratne, S.; Cabric, D. Open set wireless transmitter authorization: Deep learning approaches and dataset considerations. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 59–72. [CrossRef]
27. Chen, W.; Wang, Y.H.; Song, J.; Li, Y. Open set HRRP recognition based on convolutional neural network. *J. Eng.* **2019**, *2019*, 7701–7704. [CrossRef]
28. Bendale, A.; Boult, T. Towards open set deep networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 26 June–1 July 2016; pp. 1563–1572.
29. Wen, Y.; Zhang, K.; Li, Z.; Qiao, Y. A Discriminative Feature Learning Approach for Deep Face Recognition. In *European Conference on Computer Vision*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 499–515.
30. Draganov, A.; Brown, C.; Mattei, E.; Dalton, C.; Ranjit, J. Open set recognition through unsupervised and class-distance learning. In *2nd ACM Workshop on Wireless Security and Machine Learning*; ACM: New York, NY, USA, 2020; pp. 7–12.
31. Snell, J.; Swersky, K.; Zemel, R.S. Prototypical networks for few-shot learning. *arXiv* **2017**, arXiv:1703.05175.
32. Yang, H.M.; Zhang, X.Y.; Yin, F.; Liu, C.L. Robust classification with convolutional prototype learning. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018; pp. 3474–3482.
33. Yang, H.M.; Zhang, X.Y.; Yin, F.; Yang, Q.; Liu, C.L. Convolutional prototype network for open set recognition. *IEEE Trans. Pattern Anal. Mach. Intell.* **2020**, *44*, 2358–2370. [CrossRef] [PubMed]

34. Liu, C.L.; Nakagawa, M. Evaluation of prototype learning algorithms for nearest-neighbor classifier in application to handwritten character recognition. *Pattern Recognit.* **2001**, *34*, 601–615. [CrossRef]
35. Fisher, R.A.; Tippett, L.H.C. Limiting forms of the frequency distribution of the largest or smallest member of a sample. In *Mathematical Proceedings of the Cambridge Philosophical Society*; Cambridge University Press: Cambridge, UK, 1928; Volume 24, pp. 180–190.
36. Scheirer, W.J.; Rocha, A.R.; Micheals, R.J.; Boult, T.E. Meta-recognition: The theory and practice of recognition score analysis. *IEEE Trans. Pattern Anal. Mach. Intell.* **2011**, *33*, 1689–1695. [CrossRef]
37. Hu, J.; Shen, L.; Albanie, S.; Albanie, S.; Wu, E.H. Squeeze-and-excitation networks. *IEEE Trans. Pattern Anal. Mach. Intell.* **2020**, *42*, 2011–2023. [CrossRef]
38. Zhang, X.Y.; Zhou, X.Y.; Lin, M.X.; Sun, J. ShuffleNet: An extremely efficient convolutional neural network for mobile devices. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018; pp. 6848–6856.
39. Kingma, D.P.; Ba, J. Adam: A Method for Stochastic Optimization. In Proceedings of the International Conference on Learning Representations, San Diego, CA, USA, 7–9 May 2015.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

applied sciences

Article

Fast and Effective Tag Searching for Multi-Group RFID Systems

Na Yan, Honglong Chen *, Kai Lin, Zhe Li and Yuping Liu

College of Control Science and Engineering, China University of Petroleum (East China), Qingdao 266580, China
* Correspondence: chenhl@upc.edu.cn

Abstract: In RFID-assisted applications, the customers often request to provide the tag searching service to determine which specific tags are present in the system. In practice, tags are usually divided into different groups to represent different categories or brands. We found that the traditional tag searching protocols are not very appropriate for multi-group RFID scenarios because they cannot ensure that the searching results of each group satisfy the predefined reliability requirements. Therefore, we develop a series of effective multi-group tag searching schemes. B-Search is a basic method that leverages the filter vector and the indicator vector to perform tag searching for each group sequentially. G-Search and A-Search are two parallel multi-group tag searching schemes. G-Search selects the longest frame length as the frame length of all groups, while A-Search can adaptively adjust the frame length of each group to improve the searching efficiency. We evaluate the performance of the proposed protocols through theoretical analysis and discuss the optimal parameter settings to minimize the execution time. Extensive simulations illustrate that both G-Search and A-Search can achieve fast and effective multi-group tag searching.

Keywords: RFID systems; tag searching; target tags; multi-group

1. Introduction

After years of development, a variety of Internet of Things (IoT) technologies [1–4] are fully applied in different industries. As the central supporting technology for IoT applications [5–7], radio frequency identification (RFID) has received widespread attention. RFID is a kind of short-range radio communication technology, which can automatically identify target objects and obtain relevant data through radio frequency signals, without manual intervention in the process. Compared with bar codes and QR codes, RFID technology has the advantages of larger data storage capacity, wider communication range, and nonline-of-sight transmission.

An RFID system generally consists of a reader and several tags [8,9]. By emitting electromagnetic waves, the reader can provide energy for tag operations and communicate with tags. The tag is the data carrier in the system that can send the stored data to the reader in a non-contact manner. Tags can be attached to products to indicate some certain information. With the price of RFID tags becoming lower and lower, RFID technology is deployed in a wide range of industries, such as identity recognition, cardinality estimation, inventory control, supply chain management, object localization, and object tracking [10–12].

Tag searching is a new problem derived from RFID-assisted warehouse management systems. For instance, a manufacturer has produced some sub-standard products, and these products have been delivered to some warehouses. The manufacturer manager wants to find out the sub-standard products in the warehouse. For the manager, the tag IDs of the sub-standard products are known, and the tag IDs of the other non-relevant products in the warehouse are unknown. With these known IDs, the manufacturer manager can perform tag searching in the warehouse to find out these sub-standard products. In summary, the tag searching problem is to determine which known tags are present in a given local tag set. There are two simple ways to solve the problem: local tag identification and wanted tag polling [13,14], but they are time-consuming. In recent years, researchers have proposed

Citation: Yan, N.; Chen, H.; Lin, K.; Li, Z.; Liu, Y. Fast and Effective Tag Searching for Multi-Group RFID Systems. *Appl. Sci.* **2023**, *13*, 3540. https://doi.org/10.3390/app13063540

Academic Editors: Junseop Lee and Jia Liu

Received: 30 December 2022
Revised: 28 February 2023
Accepted: 8 March 2023
Published: 10 March 2023

a lot of tag searching algorithms [13–17], including iterative algorithms and segmented algorithms, which have greatly improved the efficiency of tag searching.

Sometimes, tags are divided into different categories based on the type or brand of products to which they are attached. For the scenario, we may need to perform some operations for a certain category of tags. For example, the reader samples information, performs tag searching, and determines if a missing tag event occurs in a category. Typically, this scenario is referred to as the multi-group RFID system. In the system, researchers are most interested in the missing tag detection problem, and many effective multi-group missing tag detection protocols have been proposed [18–20]. The tag searching problem is much more complex and worthwhile. Obviously, the traditional tag searching focuses on studying single-group RFID systems, which is a special case of multi-group RFID systems. Currently, there is hardly a protocol which can effectively and pertinently solve the multi-group tag searching problem to ensure that the searching results in each group satisfy the predefined reliability requirements.

To overcome this challenge, we deliver a comprehensive analysis on tag searching in multi-group scenario and investigate how to devise optimal tag searching algorithms. Of course, the three multi-group tag searching protocols we proposed are still appropriate in the single-group situation.

The main contributions in our paper are summarized as follows:

- We expand the application scenario of tag searching and systematically formulate the multi-group tag searching problem;
- We use the segmented tag searching protocol to solve the multi-group tag searching problem and develop B-Search protocol. All groups are searched sequentially. For tag searching within a group, the reader first performs the deactivation of non-wanted tags and then further performs the verification of target tags;
- Meanwhile, we propose two parallel multi-group tag searching protocols called G-Search and A-Search, respectively. G-Search selects the longest frame length as the frame length of all groups. A-Search can adaptively adjust the frame length of each group, thus improving the searching efficiency when the number of local tags and the number of wanted tags are different.
- We conduct theoretical analysis to optimize the parameter settings of the three proposed protocols, and extensive simulations demonstrate that our best protocols can achieve fast and effective multi-group tag searching.

The rest of our paper is organized as follows: Section 2 gives a brief overview of traditional tag searching protocols and multi-group missing tag detection protocols. In Section 3, we construct the system model and define the multi-group tag searching problem. We propose a basic multi-group tag searching protocol called B-Search and give parameter optimizations in Section 4. Section 5 describes our parallel multi-group tag searching protocol called G-Search. In Section 6, we propose an adaptive multi-group tag searching protocol called A-Search to further improve the searching efficiency. Extensive simulations and analysis are presented in Section 7. Finally, we conclude this paper in Section 8.

2. Related Work

Previous researchers have studied RFID systems deeply, and have proposed a large number of algorithms for practical applications, such as tag identification, tag cardinality estimation, and so on. We will introduce the protocols associated with the multi-group tag searching in the following: the traditional tag searching protocols and the multi-group missing tag detection protocols.

2.1. Traditional Tag Searching Protocols

Traditional tag searching is to determine the intersection of wanted tag set and local tag set in a large-scale RFID system with the minimum time while satisfying the certain reliability requirements. Existing tag searching protocols can be classified into iterative protocols and segmented protocols, which are summarized as follows:

Iterative tag searching protocols perform iterative filtering in a variety of ways to dynamically approximate the target tag set, which is currently the most mainstream tag searching approach. Min et al. [13] designed a novel technique called a filtering vector and proposed an iterative tag searching protocol called Iterative Tag Search Protocol (ITSP). ITSP filters non-wanted tags and non-target tags by filtering vectors and then keeps repeating the process until the searching results satisfy the reliability requirements. Yu et al. [15] proposed a probabilistic tree-based tag searching approach called Tree-based Tag Search Protocol (TTS), which hashes multiple tags into each internal tree node and performs batched verification to verify target tags. Liu et al. [16] developed a time-effective tag searching protocol called Compact Exclusive Validation Protocol (CEV). CEV utilizes the Ordering Indicator and KEY-Filter to filter out non-wanted tags so that the target tags are verified without interference.

The segmented tag searching protocols implement interference tag deactivation and target tag verification, respectively. Compared with iterative tag searching protocols, segmented tag searching protocols can avoid repetitive verification of target tags. Zheng et al. [17] developed a solution calledompact Approximator-Based Tag Searching Protocol (CATS). CATS first filters the non-wanted tags through a Bloom filter and then forms a virtual Bloom filter from the remaining local tags to determine the target tags. Subsequently, BFSearch+ tag searching protocol was proposed by Yan et al. [14]. They designed new techniques called composite filter vector and indicator vector. The composite filter vector can complete non-wanted tag deactivation efficiently. The indicator vector is able to assign all the wanted tags to a singleton slot for verification and determine the target tags.Zheng et al. developed a solution called CATS in [17]. CATS first filters the non-wanted tags through a Bloom filter and then forms a virtual Bloom filter from the remaining local tags to determine the target tags. Subsequently, BFSearch+ tag searching protocol was proposed by Yan et al. in [14]. They designed new techniques called composite filter vector and indicator vector. The composite filter vector can complete non-wanted tag deactivation efficiently. The indicator vector is able to assign all the wanted tags to a singleton slot for verification and determine the target tags. BFSearch+ is the best time-effective traditional tag searching protocol available.

2.2. Missing Tag Detection Protocols in Multi-Group RFID System

In the scenario of multi-group RFID systems, the most popular problem investigated by researchers is the missing tag detection. The objective of missing tag detection is to determine if a missing tag event has occurred in the system. When the number of missing tags in the system is larger than a certain threshold, a missing tag event is considered to have occurred. Missing tag detection is flexible and useful in some practical scenarios.

For multi-group RFID systems, the reader needs to recognize whether a missing tag event occurs within a group. To solve this problem, researchers have proposed many multi-group missing tag detection protocols. Yu et al. [18] developed a series of missing tag detection protocols by incorporating an improved Bloom filter design and parameter tuning in multi-group and multi-region RFID systems. Shortly after, a Simultaneous Missing Tag Detection protocol (SMTD) was proposed by Liu et al. [19]. It can decode out multiple frame occupation vectors from one actual time frame, and each frame occupation vector can complete the missing tags detection within a group. Combined with the Category Clustering protocol (CC) which can cluster the tag categories into one batch, SMTD can significantly reduce the time for multi-group missing tag detection. Lin et al. [20] developed an Accurate and Expeditious Multi-group Missing Tag Detection protocol (AEMD), which implants a built-in vector to tags in the offline phase, and the reader implements multi-group missing tag detection by collecting the built-in vectors of tags.

3. Preliminary

In this section, the multi-group RFID system model and the multi-group tag searching problem statement are described in detail.

3.1. System Model

Normally, a multi-group RFID system [14,16] is composed of a back-end server, several readers, and lots of tags, which are divided into multiple groups in the interrogation region. Because readers are connected to the back-end server, we consider the readers and the back-end server as a whole and refer to it generically as the reader, which has great computing power and storage capacity. For the case of multiple readers, we can employ the existing reader scheduling algorithms to schedule readers without conflicts. Therefore, in our paper, we consider the case of a single reader.

The communication between the reader and tags complies with Class 1 Generation 2 (C1G2) standard and adopts listen-before-talk communication mode [21]: firstly, the reader initiates communication by broadcasting query command and related parameters, including the frame length f and random seed R, and then tags perform the hash function $\big(H(ID, R) \bmod f\big)$ to select a time slot and respond in the slot, where the ID represents a 96-bit unique identification for each tag. Because of the randomness of slot selection, we usually divide the time slots into empty slots, singleton slots and collision slots, according to the number of tags responding in a slot. Only in a singleton slot, the tag can send the message to the reader successfully. There are usually three types of messages sent by tags: 1-bit short response, 16-bit long response, and 96-bit tag ID. We denote the time duration for transmitting a 96-bit tag ID as t_{id} and the time duration for transmitting a 1-bit short response as t_s.

In practice, products are often located together with the same category in a warehouse. For the convenience of management, the tag ID is required to express the group information, and it contains two components: the group ID denoted by ID_s and the member ID denoted by ID_m. The group ID indicates the group to which the tag belongs, and the member ID is the unique identification sequence of the tag in a group. Tags with the same group ID share the same group information, which may be the category, the brand, or the manufacturer of the tagged products [22]. The group information is deterministic and preloaded into tags to wait for query by readers after tags are put into service. The length of the group ID can be adjusted appropriately according to the practical requirements. In this paper, we assume that the category ID has 16 bits.

3.2. Problem Statement

Assume that the tags in the interrogation region are divided into G groups, with no overlap between groups. Each group has a group ID as a unique identification for the group. According to the knowledge of traditional tag searching, the local tag set represents the set of tags in the interrogation region, denoted by L. We suppose that the reader only knows the number of local tags in group g, denoted by $|L_g|$, and does not know anything else about them. We use W to denote the set of wanted tags, which represent the tags that we are interested in, and we want to check whether they are in the interrogation region. The reader not only knows the number of wanted tags in group g, denoted by $|W_g|$, but also knows the IDs of the wanted tags in group g, $g \in \{1, 2, ..., G\}$. That is to say, the group state of the wanted tags is known, while the group state of the local tags is unknown. However, since the tag grouping is completed according to the actual situation before the tags are put into application, the reader has the knowledge of all group IDs. Moreover, the ultimate goal of tag searching is to determine the intersection of local tags and wanted tags in group g, and we refer to the tags in the intersection as target tags, represented by T_g, i.e., $T_g = W_g \bigcap L_g$. The reader can obtain the number of target tags in each group, denoted by $|T_g|$, through performing the target tag estimation protocol. In addition, we refer to the tags in the local tag set except for the target tags as non-wanted tags, and the tags in the wanted tag set except for the target tags as non-target tags. Figure 1 briefly illustrates the tag searching problem in a multi-group RFID system.

We are interested in tag searching event for each group. In other words, multi-group tag searching protocols need to discover the common part of the local tag set and the wanted tag set in group g under the predefined reliability requirement.

The multi-group tag searching problem is defined as: In a large-scale RFID system with G-group tags, given a wanted tag set, determine $T_g = W_g \bigcap L_g$ for group g with the minimum time while satisfying the following two requirements:

(1) All target tags for group g in the interrogation region must be identified. To put it simply, for group g, the final searching result T_g^* must contain all the target tags, i.e., $T_g \subseteq T_g^*$.

(2) The tag searching result for group g has to satisfy the predefined reliability requirement P_{req} $(0 < P_{req} < 1)$, namely

$$\frac{|T_g^* - T_g|}{\min(|W_g|, |L_g|)} \leq 1 - P_{req}, \tag{1}$$

where $|\cdot|$ denotes cardinality of the set and $g \in \{1, 2, \ldots, G\}$. The phenomenon that the target tags in tag searching results are more than target tags in practice is due to the false positive during the tag searching, which means non-target tags and non-wanted tags are mistaken for target tags. Equation (1) indicates that the probability of the appearance of the false positive tags should be within the allowable range of reliability. Other than that, we define the target tag ratio as λ, i.e., $\lambda = \frac{|T_g|}{\min(|W_g|, |L_g|)}$ and the group interval as r. Group interval is the increment size of the number of tags between different groups.

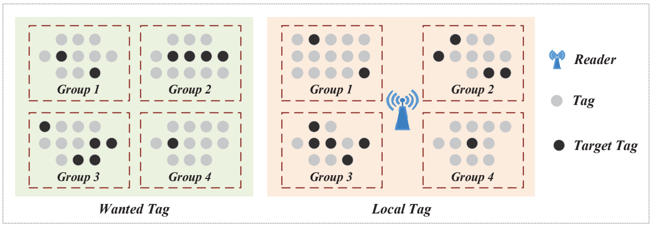


Figure 1. Illustration of the tag searching problem in a multi-group RFID system.

4. B-Search

In this section, we propose a baseline approach to solve the multi-group tag searching problem, called B-Search. The overall concept of the approach is that the tag searching is performed separately in order for each group, with only one group searched at a time. Specifically, B-Search consists of three phases: in phase I, the reader wakes up the tags in a group; in phase II, the reader eliminates the interference of non-wanted tags, laying the foundation for phase III; and, in phase III, the reader further determines the target tags in the group. Details are as follows.

4.1. Protocol Description

Phase I: Initiate the tag searching within a group. The reader broadcasts a group ID. After broadcasting, the tag in the interrogation region checks whether its group ID matches. The matching tags remain active and execute the algorithms of phases II and III. After the tag searching in this group is completed, the reader broadcasts the next group ID to initiate tag searching for the next group.

Phase II: Eliminate the interference of non-wanted tags in the group. First, the reader constructs a virtual filter vector by performing multiple hash operations on the wanted tag set. The reader initiates a query with the parameter f_g, k_g and R_1, where f_g indicates the frame length of this query, k_g indicates the number of independent hash functions used in this query, and R_1 denotes the random seed in this query. The different hash functions in the query use the same random seed R_1. Based on the slots selected by the wanted tags, the reader can construct a vector. Each bit in the vector corresponds to a slot. The slot with tag responses is denoted by 1 and without tag responses is denoted by 0. The reader sequentially performs l queries by random seeds $\{R_1, R_2, \ldots, R_l\}$ to obtain l vectors. By synthesizing the information of these vectors, the reader can derive a filtering vector, denoted by V_1. If the first bit of the first vector is 0, the first slot in the filter vector V_1 is represented by 1. If the first bit of the first vector is not 0, but the first bit of the second vector is 0, the first slot of the filter vector is represented by 2, and so on. If the first bit of all vectors is not 0, the first slot in the filter vector is denoted by 0. In summary, each slot in the filter vector indicates where the first "0" occurs. Then, the reader broadcasts the related parameters and filter vectors V_1 to the local tags in this group. The local tag performs $k \times l$ hash operations in turn to select $k \times l$ slots in V_1 for confirming whether it is the non-wanted tag. If the number in the slot it chooses is the same as the number of the random seed it uses, the tag is a non-wanted tag and will be deactivated immediately.

Phase III: Determine the target tags in the group. First, the reader assigns all the wanted tags to a slot for verification. The reader initiates many queries on the wanted tag set by some random seed $\{R'_1, R'_2, \ldots\}$, where the frame length is f'_g. In first query, the reader can acquire an indicator vector based on the slots selected by the wanted tags, denoted by V_2. Each bit in the vector corresponds to a slot. The slot with only one wanted tag response is represented by 1, and the rest of the slots are represented by 0. The singleton slot which is selected by only one wanted tag is the verification slot of the wanted tag. The reader then removes the singleton slots and the wanted tags in the singleton slot, and initiates the second query with the remaining wanted tags and new frame length. At the end of the second query, the reader marks the bit in the indicator vector V_2 corresponding to singleton slots as 2. The reader no longer performs queries until all the wanted tags are assigned to a singleton slot. Assume that a total of h_g hash operations have been performed with a h_g random seed. Apparently, each bit in the indicator vector V_2 refers to the random seed number used by the wanted tag in the slot. The reader then broadcasts the corresponding parameters to the local tags in this group. The tag selects slots using these random seeds in turn and determines its response slot based on whether its corresponding bit in the indicator vector matches its random seed number. After determining the response slot, the tag forms a response vector. In the response vector, the response bits of the tag are marked as 1, and the others are marked as 0. The response vectors of all local tags are packaged into some 96-bit messages and sent to the reader at the same time. Depending on the local tag response, the reader can determine exactly which tags are the target tags.

Figure 2 illustrates the specific process of multi-group tag searching by the B-Search protocol.

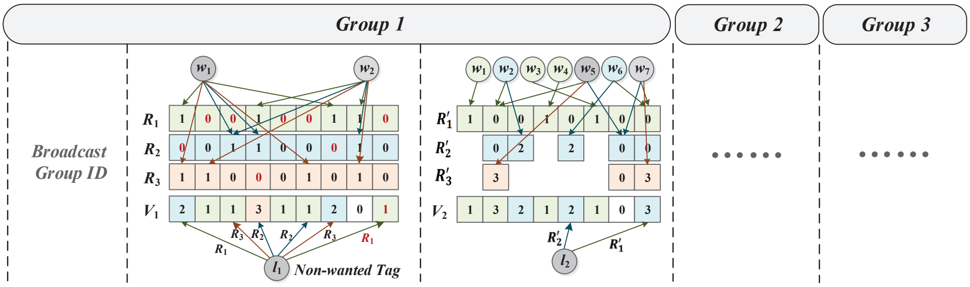


Figure 2. Illustration of the B-Search tag searching protocol.

4.2. Parameter Optimization

First, the reader needs to broadcast the group ID to notify the tags in the group performing tag searching. T_0 denotes the time taken to broadcast the group IDs:

$$T_0 = 16 \cdot G \cdot T_s. \tag{2}$$

B-Search protocol performs tag searching sequentially in groups. Only one group is searched at a time. Thus, we can take the g-th group as an example for parameter optimization.

Actually, the filter vector V_1 is an important method for non-wanted tag deactivation, which is obtained by combining multiple vectors. The probability that any bit in a vector equals 1 is denoted by P_v, which is calculated as follows:

$$P_v = 1 - \left(1 - \frac{1}{f_g}\right)^{k_g \cdot |W_g|} \approx 1 - e^{-\frac{k_g \cdot |W_g|}{f_g}}. \tag{3}$$

Subsequently, if the third bit of the filter vector V_1 is equal to r, it means that the third bits in the vectors constructed by the first $r-1$ queries in the phase II all equal 1, and the third bit in the vector constructed by the r-th query equals 0. It represents the third bit in the vector constructed by the r-th query is adopted by the filter vector V_1. A non-wanted tag cannot be deactivated if all slots that the tag selects are not adopted by the filter vector V_1. We denote the probability that a non-wanted tag will not be deactivated as P_d. As we know,

$$P_d = \prod_{r=1}^{l} \left(1 - (1 - P_v) \cdot P_v^{r-1}\right)^k. \tag{4}$$

Thus, the number of non-wanted tags in the g-th group that are not deactivated is $P_d \cdot (|L_g| - |T_g|)$. In multi-group tag searching, the search results for each group need to satisfy predefined reliability requirements P_{req}, so

$$\frac{P_d \cdot (|L_g| - |T_g|)}{\min(|W_g|, |L_g|)} \leq 1 - P_{req}. \tag{5}$$

As shown in Equation (5), we need to choose the appropriate parameters l, k, and f_g, so that P_d satisfies the reliability requirements.

In [14], Yan et al. revealed that, when $l \geq 3$, the decrease of P_d is not significant as l increases through simulations. Therefore, it is quite appropriate for us to set l to 3.

The time spent by the g-th group in phase II is denoted as T_g, which is

$$T_g = \left(1 + \lceil \frac{f_g \cdot \lceil log_2(l+1) \rceil}{96} \rceil \right) \cdot T_{tag}. \tag{6}$$

We can find the optimal frame length f_g^* and the number of hash functions k^* by integer programming.

$$\begin{aligned} (k^*, f_g^*) &= \arg\min_{k, f_g} \left(\left(1 + \lceil \frac{f_g \cdot \lceil log_2(l+1) \rceil}{96} \rceil \right) \cdot T_{tag} \right), \\ s.t. &\quad \begin{cases} k \in N^+, f_g \in N^+ \\ P_d \leq (1 - P_{req}) \cdot \frac{\min(|W_g|, |L_g|)}{(|L_g| - |T_g|)} \end{cases}, \end{aligned} \tag{7}$$

where N^+ denotes the set of positive integers.

In phase III of B-Search, we only need to determine the frame length f_g'. Because the response vectors of all local tags are packaged into some 96-bit messages, f_g' can be taken as:

$$f_g' = \lceil \frac{|W_g|}{96} + p \rceil \cdot 96 \qquad p \in N^+, \tag{8}$$

where p is an adjustment factor. We denote the time spent of the g-th group in the target tag verification phase by T'_g. It is easy to know that:

$$\begin{aligned} T'_g &= \left(\lceil \frac{f'_g \cdot \lceil \log_2(h_g+1) \rceil}{96} \rceil + 1\right) \cdot T_{tag} + \lceil \frac{f'_g}{96} \rceil \cdot T_{tag} \\ &\le \left(\lceil \frac{\lceil \log_2(h_g+1) \rceil}{96} \rceil + 2\right) \cdot \lceil \frac{f'_g}{96} \rceil \cdot T_{tag} \\ &\approx \lceil \frac{\log_2(h_g+1)}{96} + 2 \rceil \cdot \left(\lceil \frac{|W_g|}{96} \rceil + p\right) \cdot T_{tag}. \end{aligned} \tag{9}$$

From the analysis of Yan et al. in [14], we know that T'_g can be taken to the minimum value when $p = 0$.

Assume that the time to perform the B-Search protocol in a large-scale RFID system with G-group tags is T_B. According to the analysis above, T_B can be calculated as:

$$T_B = T_0 + \sum (T_g + T'_g), \qquad g \in \{1, 2, \dots, G\}. \tag{10}$$

5. G-Search

B-Search is a basic multi-group tag searching protocol, and each group is searched separately in order. B-Search is time-consuming because each group needs to broadcast the relevant parameters to initialize tag searching. In short, these parameters have to be broadcast G times, and the tag searching has to be performed G times. In this section, we propose a parallel multi-group tag searching protocol called G-Search, which performs tag searching only once in all groups simultaneously. G-Search can be divided into three phases. In phase I, the reader arranges the order for groups and assigns a response slot segment to each group. In phase II, the reader removes the interference of the non-wanted tags in all groups through one query. In phase III, the target tags in all groups are identified at once. The details of each phase are described below.

5.1. Protocol Description

Phase I: Assign a slot segment to a group. We consider the tags within a group as a whole. All operations at this phase are directed at a group, not a tag. The reader initializes a query with the parameter settings $\{f_s, R_{s1}, R_{s1}, \dots\}$. The reader performs a hash operation with R_{s1} on all groups, i.e., $H(ID_s, R_{s1})$ mod f_s and assigns them to a virtual frame. Those groups that are assigned to a singleton slot determine their response slot segment. Next, the reader removes the singleton slots from this frame and the groups in the singleton slot, and then performs the second hash operation. Similarly, in the second hashing, those groups that choose a singleton slot determine their response segments. Until all groups are assigned to a singleton slot, the operations are finished. Assume that a total of h' hash operations have been performed. Depending on the hashing number with which each group determines its response slot segment, the reader can construct a group segment indicator vector, denoted by V_s. For example, in Figure 3, the first bit in V_s is 1, which means that Group 2 selected the first response segment by the first hash operation. The reader broadcasts the relevant parameters and the group segment indicator vector V_s to the local tags. The local tag can determine the slot segment based on its group ID.

Phase II: Eliminate the interference of the non-wanted tags in all groups at once. First, the reader calculates the frame length required for each group to complete the tag searching with the specified reliability requirement, and takes the maximum frame length f_m as the length of every group response segment. Thus, the total practical frame length of the phase II is $f_m \cdot G$. If tags within a group responds in the n-th slot segment, the exact response slot of the tags is $[(n-1) \cdot f_m + 1, n \cdot f_m]$. The reader performs multiple hashing operations on the wanted tags set to construct a filter vector. Subsequently, the reader initiates a query on local tag set. According to the filter vector, local tags can distinguish whether they are non-wanted tags or not. If so, they will remain quiet for the rest of the phase.

Phase III: Determine the target tags in all groups at once. First, the reader selects a group with the most wanted tags and determines the frame length f'_m for the group to complete the target tag determination. The overall frame length of this phase is $f'_m \cdot G$. Then, the response slot of the n-th response segment is $[(n-1) \cdot f'_m + 1, n \cdot f'_m]$. The reader then assigns all the wanted tags to a singleton slot, broadcasts the parameters and the indicator vector V_2 to initiate a round query, and verifies whether they are the target tags through the responses of local tags.

Figure 3 illustrates the detailed process of multi-group tag searching by the G-Search protocol.

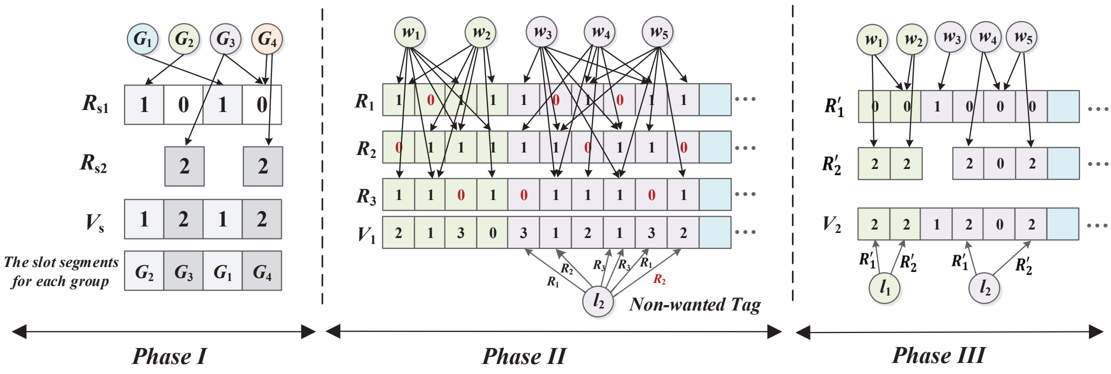


Figure 3. Illustration of the G-Search tag searching protocol.

5.2. Parameter Optimization

In G-Search, we first need to assign the response slot segments to groups, and the time spent in this process is denoted by $T_{o'}$, which is easily obtained as:

$$T_{o'} = \left(\lceil \frac{f_s \cdot \lceil \log_2(h'+1) \rceil}{96} \rceil + 1 \right) \cdot T_{tag}. \tag{11}$$

According to the analysis in Section 4.2, it is easy to know that

$$f_s = \lceil \frac{|G|}{96} \rceil \cdot 96. \tag{12}$$

In this section, a parallel approach is taken for multi-group tag searching. We use the group with the longest frame length f_m as a sample for satisfying the reliability requirements. Therefore,

$$\begin{aligned} &(k^*, f_g^*) = \underset{k, f_g}{\arg\min} \left(\lceil \frac{f_g \cdot \lceil log_2(l+1) \rceil}{96} \rceil \cdot T_{tag} \right), \\ &s.t. \quad \begin{cases} k \in N^+, f_g \in N^+ \\ P_d \leq (1 - P_{req}) \cdot \frac{\min(|W_g|, |L_g|)}{(|L_g| - |T_g|)} \end{cases}, \end{aligned} \tag{13}$$

where N^+ denotes the set of positive integers.

$$f_m = max(f_g) \qquad g \in \{1, 2, ..., G\}. \tag{14}$$

$$f'_m = max\left(\lceil \frac{|W_g|}{96} \rceil \cdot 96 \right) \qquad g \in \{1, 2, ..., G\}. \tag{15}$$

Equations (14) and (15) indicate that we take the maximum frame length f_m as the length of the group response segment in phase II and f'_m as the length of the group response segment in phase III. We still set l to 3 and allow that each group chooses the suitable k according to the reliability requirements.

The time spent by G-Search for the multi-group tag searching is denoted by T_s.

$$\begin{aligned} T_{s'} = &\left(\lceil \frac{f_s \cdot \lceil \log_2(h'+1) \rceil}{96} \rceil + 1 \right) \cdot T_{tag} \\ &+ \left(1 + \lceil \frac{f_m \cdot \lceil log_2(l+1) \rceil}{96} \rceil \cdot G \right) \cdot T_{tag} \\ &+ \left(\lceil \frac{f'_m \cdot \lceil \log_2(h+1) \rceil}{96} \rceil \cdot G + 1 \right) \cdot T_{tag} + \lceil \frac{f'_m}{96} \rceil \cdot G \cdot T_{tag}. \end{aligned} \tag{16}$$

6. A-Search

G-Search provides a new approach to multi-group tag searching, which performs tag searching for all groups in parallel by assigning each group a response slot segment. To satisfy the reliability requirements, G-Search selects the group with the longest frame length as a template and uses the longest frame length to construct the whole frame. For the other groups, the frame length is actually redundant and a smaller frame length is sufficient for the reliability requirements. If each group can choose the frame length that best suits themselves, the whole frame will be shorter and the multi-group tag searching protocol will be more efficient. Therefore, we propose a new protocol called A-Search, which also has three phases. Phase I is used to assign a response slot segment to each group, phase II is used to deactivate non-wanted tags for all groups, and phase III is used to confirm the target tags for all groups. The frame lengths for each group in both phase II and phase III are adaptive. In Section 6.1, we introduce the details of the A-Search protocol.

6.1. Protocol Description

Phase I: Assign a slot segment to a group. This phase is exactly the same as the phase I of G-Search. The reader regards a group as a whole, and assigns each group to a singleton slot by performing multiple hashing operations based on the group IDs. Ultimately, the reader can assign a response slot segment to each group.

Phase II: Eliminate the interference of the non-wanted tags in all groups at once. The reader calculates the most suitable frame length $\{f_1, f_2, \ldots, f_G\}$ for each group to perform the non-wanted tags deactivation while satisfying the reliability requirement. The practical frame length in phase II is $\sum f_g$, $g \in \{1, 2, \ldots, G\}$. Then, the reader constructs the filter vector V_1 in the wanted tag set. The reader performs a query in local tag set with parameter settings $\{f_1, f_2, \ldots, k_1, k_2, \ldots, R_1, R_2, \ldots\}$ and the filter vector V_1 to deactivate the non-wanted tags.

Phase III: Determine the target tags in all groups at once. The reader selects the most appropriate frame length $\{f'_1, f'_2, \ldots, f'_G\}$ for each group. The practical frame length in phase III is $\sum f'_g$, $g \in \{1, 2, \ldots, G\}$. Then, the reader assigns each wanted tag to a singleton slot by multiple hashing operations and constructs an indicator vector V_2. Finally, the reader broadcasts the relevant parameters, and then the local tag calculates its response time slot and replies with a response vector. The wanted tags can confirm whether it is the target tag depending on the response vectors.

Figure 4 illustrates the process of multi-group tag searching by the A-Search protocol.

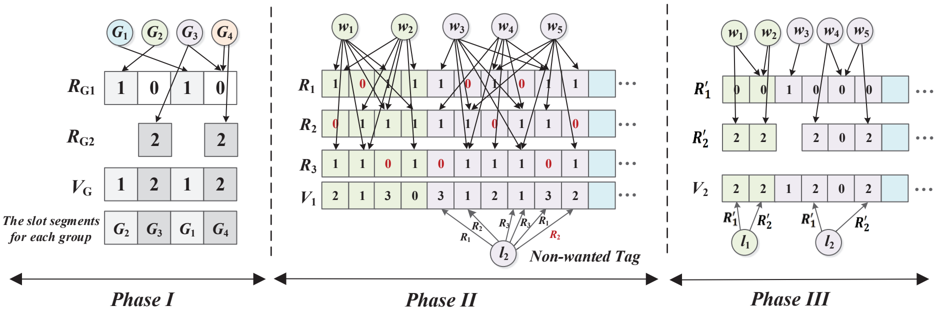


Figure 4. Illustration of the A-Search tag searching protocol.

6.2. Parameter Optimization

The tag searching process of A-Search is similar to G-Search, and they both use the parallel approach. However, A-Search is an improvement of G-Search in that each group can adaptively choose the frame length that best fits itself. In phase II and III of A-Search, the reader needs to send the frame length of each group to local tags in addition to the regular parameters.

We use T_a to represent the time spent by A-Search for multi-group tag searching, and can be expressed as:

$$\begin{aligned} T_a = & \left(\lceil \frac{f_s \cdot \lceil \log_2(h'+1) \rceil}{96} \rceil + 1 \right) \cdot T_{tag} \\ & + \left(\lceil \frac{\sum \lceil (log_2(f_g+1)) \rceil}{96} \rceil + \lceil \frac{\sum f_g \cdot \lceil log_2(l+1) \rceil}{96} \rceil \right) \cdot T_{tag} \\ & + \left(\lceil \frac{\sum \lceil (log_2(f'_g+1)) \rceil}{96} \rceil + \lceil \frac{\sum f'_g \cdot \lceil \log_2(h+1) \rceil}{96} \rceil \right) \cdot T_{tag} \\ & + \lceil \frac{\sum f'_g}{96} \rceil \cdot T_{tag}. \end{aligned} \tag{17}$$

7. Performance Evaluation

In this section, we conduct extensive simulations in a large-scale multi-group RFID system to evaluate the performance of B-Search, G-Search, and A-Search in terms of execution time. To make the simulation results more convincing, we repeat the simulations with the same parameter settings 100 times and take the average value as the final results.

7.1. Simulation Setting

In our simulations, the communication parameters settings follow the specification of the EPCglobal C1G2 standard [23]. The transmission rate between the reader and the tag is asymmetric because of the physical implementation. Generally speaking, the transmission rate of tag-to-reader is 40∼460 kb/s for FM0 and the transmission rate of reader-to-tag is 5∼320 kb/s for a Miller-modulated subcarrier. In our paper, we adopt 62.5 kb/s as the tag-to-reader and reader-to-tag date transmission rate. Thus, the time taken by the reader and the tags to send 1-bit data are 0.016 ms, denoted by T_c. It is well known that any two consecutive transmissions are separated by a 0.184 ms time interval, denoted by T_i, whether reader-to-tag or vice versa. To sum up, we can set $T_s = 0.2$ ms and $T_{id} = 2.42$ ms .

7.2. Validity Verification of the Proposed Protocols

As we know, existing tag searching protocols cannot effectively solve the multi-group tag searching problem because they cannot ensure the searching results in each group satisfy the predefined reliability requirements. To demonstrate the multi-group tag searching validity of the B-Search, G-Search and A-Search, we propose a baseline protocol for comparison.

The reader can confirm whether a wanted tag is the target tag by polling it. To reduce the time spent on polling, the reader can first broadcast the group ID. Local tags immediately check whether their group ID matches the broadcast one. If so, it remains active. The reader then broadcasts the member ID of wanted tags in the group, and the active local tag checks if its own member ID is the same as the broadcast one. For each member ID, we can reserve a one-bit slot for identifying. When the local tag's member ID are polling, the tag replies with "1". Otherwise, the tag replies with "0". T_{bl} indicates the time taken by the baseline protocol to complete the multi-group tag searching. Simply,

$$T_{bl} = (16 \cdot T_c + T_i) \cdot G + (80 \cdot T_c + T_i + T_s) \cdot \sum |W_g|, \qquad g \in \{1, 2, \ldots, G\}. \tag{18}$$

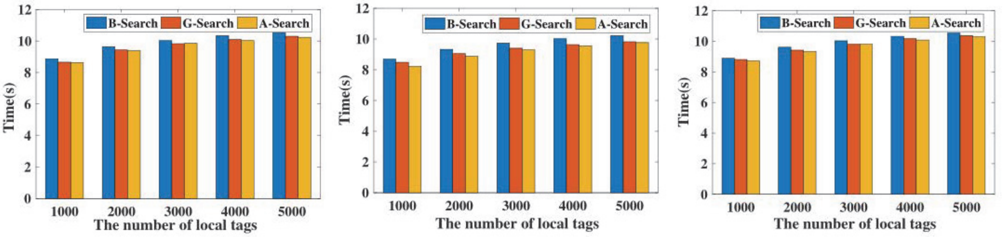
Based on Equation (18), the tag searching efficiency of the baseline protocol is only associated with the number of wanted tags in each group and the number of groups. In Table 1, we set the target tags ratio $\lambda = 0.3$, the reliability requirement $P_{req} = 0.9999$, the group interval $r = 10$, and the number of local tags in each group $|L_g| = 1000$. The table shows the searching time of baseline protocol, B-Search, G-Search, and A-Search. It is obvious that our proposed three multi-group tag searching protocol is far superior to the baseline protocol.

Table 1. The searching time of baseline protocol, B-Search, G-Search, and A-Search.

	$G = 21, W_g = 1000$	$G = 21, W_g = 5000$	$G = 41, W_g = 1000$	$G = 41, W_g = 5000$
Baseline	34.95	174.73	68.24	341.14
B-Search	10.86	53.17	21.23	103.81
G-Search	10.71	53.00	20.90	103.46
A-Search	10.72	53.01	20.92	103.49

7.3. Simulation Results

In Figure 5, we set the target tags ratio $\lambda = 0.3$ and the reliability requirement $P_{req} = 0.999$. Then, we explore its impact on the time efficiency of our protocols by changing the number of local tags in each group from 1000 to 5000 by 1000 in Figure 5a,c and from 500 to 2500 by 500 in Figure 5b. It should be noted that the number of local tags in each group here refers to the average number. Taking Figure 5a as an example, we set the number of groups $G = 21$, the group interval $r = 10$, and the number of wanted tags in each group $|W_g| = 1000$. It means that there are 21 groups in the local tag set, and the number of local tags in these groups is changing from 900 to 1100 by 10. We set the number of groups $G = 41$, the group interval $r = 10$ and the number of wanted tags in each group $|W_g| = 500$ in Figure 5b, and set the number of groups $G = 21$, the group interval $r = 20$, and the number of wanted tags in each group $|W_g| = 1000$ in Figure 5c. As you can see, the number of local tags for each group in Figure 5b is different from the other two figures because the group number in Figure 5b is different from the other two, and we must ensure the total number of local tags is consistent overall. This also applies to the number setting of wanted tags. We find that A-Search performs the best, followed by G-Search, and B-Search ranks third. In Figure 5a, when the number of local tags in each group $|L_g| = 2000$, the time cost of B-Search, G-Search, and A-Search equals 9.63 s, 9.43 s, and 9.39 s. The time cost of A-Search is 97.47% of B-Search and 99.57% of G-Search.



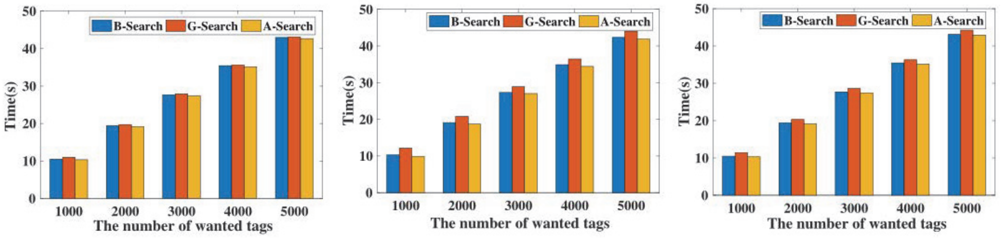
(a) G = 21 and r = 10

(b) G = 41 and r = 10

(c) G = 21 and r = 20

Figure 5. The time efficiency of each protocol under different numbers of local tags.

In Figure 6, we set the target tag ratio $\lambda = 0.3$ and the reliability requirement $P_{req} = 0.999$. Then, we set the number of group $G = 21$, the group interval $r = 10$, and the number of local tags in each group $|L_g| = 5000$ in Figure 6a. Set the number of groups $G = 41$, the group interval $r = 10$, and the number of local tags in each group $|L_g| = 2500$ in Figure 6b. Set the number of groups $G = 21$, the group interval $r = 20$, and the number of local tags in each group $|L_g| = 5000$ in Figure 6c. We explore its impact on the time efficiency of our protocols by changing the number of wanted tags from 1000 to 5000 by 1000 in Figure 6a,c and from 500 to 2500 by 500 in Figure 6b. Clearly, A-Search outperforms the other protocols. In Figure 6a, when the number of wanted tags $|W_g| = 2000$, the time cost of B-Search and G-Search are 19.40 s and 19.72 s. The time cost of A-Search is 19.14 s, which is 98.65% of B-Search and 97.06% of G-Search. In this case, G-Search does not perform as well as B-Search. Because our method is not well suited for the situations where wanted tags are too many, and the fact that G-Search applies the longest frame length to all groups, inadvertently magnifying this disadvantage even more.



(a) G = 21 and r = 10

(b) G = 41 and r = 10

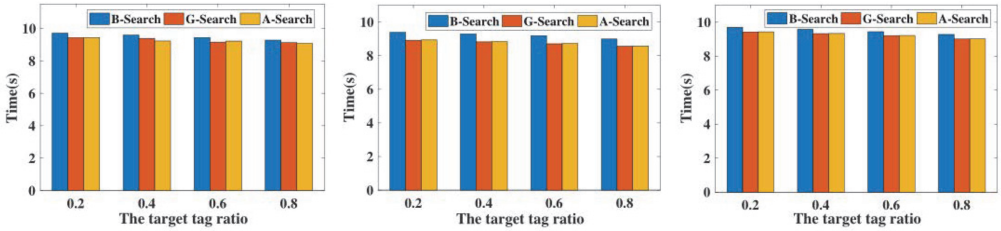
(c) G = 21 and r = 20

Figure 6. The time efficiency of each protocol under different numbers of wanted tags.

In Figure 7, we set the number of local tags in each group $|L_g| = 2000$, the number of wanted tags in each group $|W_g| = 1000$, and the reliability requirement $P_{req} = 0.999$, while changing the target tag ratio from 0.2 to 0.8 by 0.2. Then, we set the number of groups $G = 21$ and the group interval $r = 10$ in Figure 7a, set the number of groups $G = 41$ and the group interval $r = 10$ in Figure 7b, and set the number of groups $G = 21$ and the group interval $r = 20$ in Figure 7c. We find that A-Search and G-Search always perform well. In Figure 7a, when the target tag ratio $\lambda = 0.4$, the time cost of B-Search, G-Search, and A-Search is 9.59 s, 9.39 s, and 9.23 s. Compared with B-Search and G-Search, the time cost of A-Search reduces by 3.75% and 1.69%.

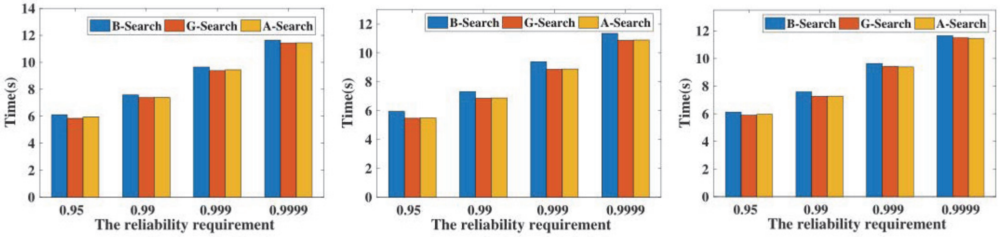
In Figure 8, we set the number of local tags in each group $|L_g| = 2000$, the number of wanted tags in each group $|W_g| = 1000$, and the target tag ratio $\lambda = 0.3$. Then, we set the number of groups $G = 21$ and the group interval $r = 10$ in Figure 8a, set the number of groups $G = 41$ and the group interval $r = 10$ in Figure 8b, and set the number of groups $G = 21$ and the group interval $r = 20$ in Figure 8c. We evaluate the time efficiency of our protocols when the reliability requirement P_{req} is 0.95, 0.99, 0.999, and 0.9999, respectively. We find that A-Search and G-Search both perform well, and the time efficiencies of

A-Search and G-Search are almost the same. In Figure 8a, when the reliability requirement $P_{req} = 0.99$, the searching time of B-Search, G-Search, and A-Search is 7.58 s, 7.38 s, and 7.39 s. The time cost of A-Search is 97.43% of B-Search and 100.11% of G-Search.



(a) $G = 21$ and $r = 10$ (b) $G = 41$ and $r = 10$ (c) $G = 21$ and $r = 20$

Figure 7. The time efficiency of each protocol under target tag ratios.



(a) $G = 21$ and $r = 10$ (b) $G = 41$ and $r = 10$ (c) $G = 21$ and $r = 20$

Figure 8. The time efficiency of each protocol under different reliability requirements.

In the above two situations, the time efficiency of A-Search and G-Search are not comparable. The number of wanted tags and local tags in each group is the same, and the frame length selected by G-Search is appropriate for each group. In contrast, A-Search takes time to broadcast frame lengths for each group so that A-Search would not have the advantage.

8. Conclusions

In this paper, we have formulated the tag searching problem arising in large-scale multi-group RFID systems. With the segmented tag searching method, we propose a suite of three multi-group tag searching protocols: B-Search, G-Search, and A-Search. G-Search and A-Search innovatively adopt the parallel approach for tag searching in multiple groups, and achieve excellent performance. In our future work, we plan to study tag searching problems in the case of multiple mobile readers and multiple regions, and propose effective tag searching algorithms.

Author Contributions: Conceptualization, H.C. and N.Y.; methodology, N.Y.; software, N.Y.; validation, K.L., Z.L. and Y.L.; formal analysis, H.C.; investigation, H.C.; resources, H.C.; data curation, N.Y.; writing—original draft preparation, N.Y.; writing—review and editing, N.Y., K.L., Z.L. and Y.L.; visualization, N.Y. and K.L.; supervision, H.C.; project administration, H.C.; funding acquisition, H.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Shandong Provincial Natural Science Foundation, China under Grant No. ZR2022YQ61, NSFC, China under Grant Nos. 61772551 and 62111530052, the Major Scientific and Technological Projects of CNPC under Grant No. ZD2019-183-003, and the Fundamental Research Funds for the Central Universities, China under Grant No. 22CX01003A-9.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sun, P.; Che, H.; Wang, Z.; Wang, Y.; Wang, T.; Wu, L.; Shao, H. Pain-FL: Personalized Privacy-preserving Incentive for Federated Learning. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 3805–3820. [CrossRef]
2. Xia, F.; Yu, S.; Liu, C.; Lee, I. CHIEF: Clustering With Higher-Order Motifs in Big Networks. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 990–1005. [CrossRef]
3. Xiao, Q.; Chen, S.; Chen, M. Joint Property Estimation for Multiple RFID Tag Sets Using Snapshots of Variable Lengths. In Proceedings of the ACM MobiHoc, Paderborn, Germany, 17–19 July 2016.
4. Huang, Y.; Chen, H.; Ma, G.; Lin, K.; Ni, Z.; Yan, N.; Wang, Z. OPAT: Optimized Allocation of Time-dependent Tasks for Mobile Crowdsensing. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2476–2485. [CrossRef]
5. Yao, J.; Xu, J.; Luo, S.; Wang, L.; Yang, C.; Wu, K.; Lou, W. Comprehensive Study on MIMO-related Interference Management in WLANs. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2087–2110. [CrossRef]
6. Liu, J.; Xia, F.; Feng, X.; Ren, J.; Liu, H. Deep Graph Learning for Anomalous Citation Detection. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *33*, 2543–2557. [CrossRef] [PubMed]
7. Ai, X.; Chen, H.; Lin, K.; Wang, Z.; Yu, J. Nowhere to Hide: Efficiently Identifying Probabilistic Cloning Attacks in Large-Scale RFID Systems. *IEEE Trans. Inf. Forensics Secur.* **2021**, *26*, 714–727. [CrossRef]
8. Chen, H.; Ai, X.; Lin, K.; Yan, N.; Wang, Z.; Jiang, N.; Yu, J. DAP: Efficient Detection Against Probabilistic Cloning Attacks in Anonymous RFID Systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 345–355. [CrossRef]
9. Liu, X.; Chen, S.; Liu, J.; Qu, W.; Xiao, F.; Liu, A.X.; Cao, J.; Liu, J. Fast and Accurate Detection of Unknown Tags for RFID Systems–Hash Collisions Are Desirable. *IEEE/ACM Trans. Netw.* **2020**, *29*, 126–139. [CrossRef]
10. Xue, H.; Chen, H.; Dai, Q.; Lin, K.; Li, J.; Li, Z. CSCT: Charging Scheduling for Maximizing Coverage of Targets in WRSNs. *IEEE Trans. Comput. Soc. Syst.* **2022**, *1*, 1–11. [CrossRef]
11. Yu, X.; Liu, J.; Zhang, S.; Chen, X.; Zhang, X.; Chen, L. Encoding-based Range Detection in Commodity RFID Systems. In Proceedings of the IEEE INFOCOM, London, UK, 2–5 May 2022.
12. Zhang, X.; Liu, J.; Chen, X.; Li, W.; Chen, L. SAH: Fine-grained RFID Localization with Antenna Calibration. In Proceedings of the IEEE INFOCOM, London, UK, 2–5 May 2022.
13. Chen, M.; Luo, W.; Mo, Z.; Chen, S.; Fang, Y. An Efficient Tag Search Protocol in Large-Scale RFID Systems With Noisy Channel. *IEEE/ACM Trans. Netw.* **2016**, *24*, 703–716. [CrossRef]
14. Yan, N.; Chen, H.; Lin, K.; Ni, Z.; Li, Z.; Xue, H. BFSearch: Bloom Filter Based Tag Searching for Large-scale RFID Systems. *Ad Hoc Netw.* **2023**, *139*, 103022. [CrossRef]
15. Yu, J.; Wei, G.; Liu, J.; Lin, C. Fast and Reliable Tag Search in Large-Scale RFID Systems: A Probabilistic Tree-based Approach. In Proceedings of the IEEE INFOCOM, Honolulu, HI, USA, 15–19 April 2018.
16. Liu, X.; Yin, J.; Liu, J.; Zhang, S.; Xiao, B. Time Efficient Tag Searching in Large-scale RFID Systems: A Compact Exclusive Validation Method. *IEEE Trans. Mob. Comput.* **2020**, *21*, 1476–1491. [CrossRef]
17. Zheng, Y.; Li, M. Fast Tag Searching Protocol for Large-Scale RFID Systems. *IEEE/ACM Trans. Netw.* **2013**, *21*, 924–934. [CrossRef]
18. Yu, J.; Chen, L.; Zhang, R.; Wang, K. On Missing Tag Detection in Multiple-Group Multiple-Region RFID Systems. *IEEE Trans. Mob. Comput.* **2017**, *16*, 1371–1381. [CrossRef]
19. Liu, X.; Guo, K.; Liu, Z.; Zhou, X.; Xue, W. Fast and Accurate Missing Tag Detection for Multi-category RFID Systems. In Proceedings of the IEEE SmartIoT, Xi'an, China, 17–19 August 2018.
20. Lin, K.; Chen, H.; Yan, N.; Li, Z.; Jiang, N. Fast and Reliable Missing Tag Detection for Multiple-Group RFID Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2656–2664. [CrossRef]
21. Liu, J.; Chen, X.; Liu, H.; Gong, H.; Chen, L. Time-efficient Range Detection in Commodity RFID Systems. *IEEE/ACM Trans. Netw.* **2022**, *30*, 1118–1131. [CrossRef]
22. Liu, J.; Chen, S.; Xiao, Q.; Chen, M.; Xiao, B.; Chen, L. Efficient Information Sampling in Multi-Category RFID Systems. *IEEE/ACM Trans. Netw.* **2019**, *27*, 159–172. [CrossRef]
23. EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID Standard. Available online: https://www.gs1.org/sites/default/files/docs/epc/gs1-epc-gen2v2-uhf-airinterface_i21_r_2018-09-04.pdf (accessed on 17 December 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

applied sciences

MDPI

Article

An Admission-Control-Based Dynamic Query Tree Protocol for Fast Moving RFID Tag Identification

Jiabin Peng, Lijuan Zhang *, Mingqiu Fan, Nan Zhao, Lei Lei, Qirui He and Jiangcheng Xia

College of Electronic and Information Engineering/College of Integrated Circuits, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
* Correspondence: lijuanzhang6@gmail.com

Abstract: As one of the key techniques used in the perception layer of the Industrial Internet of Things (IIoT), radio frequency identification (RFID) has been widely applied for object tracing, smart warehouse management, product line monitoring, etc. In most applications, conveyor belts are prevalently implemented to accelerate the sorting efficiency for goods management. However, in such a system, tags quickly go through the reader's reading range resulting in constant changing of the tag set and limited participating time of moving tags. As a result, it poses more challenges to the tag identification problem in mobile systems than in traditional static applications. In this work, a novel admission-control-based dynamic query tree (ACDQT) protocol is proposed for fast-moving tag identification. In ACDQT, two main strategies are developed, i.e., multi-round admission control (MRAC) and dynamic query tree recognition (DQTR). In MRAC, the reading process of multiple rounds is analyzed, and the number of admitted tags in each round is optimized. Thus, the tag lost ratio is guaranteed, and the identification process can be effectively accelerated. In DQTR, colliding tags are grouped into multiple subsets with the help of consecutive colliding bits in tag responses. By constructing a dynamic query tree, the number of collision slots is greatly reduced, and the identification efficiency in a single round is improved significantly. With MRAC and DQTR, ACDQT can support higher tag flow rate in mobile systems than existing works. Both theoretical analyses and simulation results are presented to demonstrate the effectiveness of ACDQT.

Keywords: IIoT; Industry 4.0; mobile RFID system; conveyor belt; tag identification; anti-collision

Citation: Peng, J.; Zhang, L.; Fan, M.; Zhao, N.; Lei, L.; He, Q.; Xia, J. An Admission-Control-Based Dynamic Query Tree Protocol for Fast Moving RFID Tag Identification. *Appl. Sci.* **2023**, *13*, 2228. https://doi.org/10.3390/app13042228

Academic Editor: Jia Liu

Received: 18 December 2022
Revised: 1 February 2023
Accepted: 4 February 2023
Published: 9 February 2023

1. Introduction

Industry 4.0, which is triggered by the Industrial Internet of Things (IIoT) , has become the current trend of automation and data exchange in manufacturing technologies [1]. Thanks to the automatic identification techniques, such as radio frequency identification (RFID) and wireless sensors, used in the perception layer of the IIoT [2], the efficiency of modern manufacturing is greatly improved. As a non-contact identification technology, RFID has been widely used in various applications, such as object tracking, smart warehouse management, product line monitoring, etc. A typical RFID system usually consists of readers, tags and a back-end server. Each tag is identified by a unique identifier and sends data information by backscattering the reader's signal. The back-end server is used to store tag information for further processing and analyses.

In RFID systems, the reader usually needs to recognize a large number of unknown tags within its reading range. When multiple tags reply simultaneously, a collision occurs where the reader cannot successfully decode the received message [3]. Unknown tag identification has always been one of the most critical techniques to enable object tracing and goods management in RFID systems. In recent research, lots of RFID tag identification protocols have been proposed. Among them, tree-based ones that make use of bit tracking technology [4,5] exhibit better performance, e.g., higher system efficiency and shorter identification delay. In such protocols, the reader usually divides colliding tags into multiple subsets with tree splitting. Thanks to the position information of colliding bits in the received message, the splitting process is more efficient. The most representative tree-based protocols are collision tree (CT) [4], collision window tree (CwT) [5] and M-ary collision tree (MCT) [6]. These algorithms use one or more colliding bits to split colliding tags into multiple subsets to accelerate the identification process. Recently, Su et al. proposed some tree-based algorithms, e.g, the dual prefix probing (DPPS) [7] and group-based tree splitting (GBSA) [8] to quickly identify tags. However, existing works make little use of the collision information. There is still room for improvement in bit-tracking-based tree splitting algorithms. Moreover, these works only consider the identification efficiency of a single reading round in static environments. The impact of tag mobility on the identification process lacks intensive study.

In most applications, conveyor belts are widely used to accelerate the sorting efficiency for goods management [9–11]. For example, more and more airports have used RFID technology to place luggage on conveyor belts for fast identification, and other applications have also identified tagged goods on conveyor belts, such as the traditional retail giant Walmart [9]. In such systems, one or more RFID readers are mounted above or beside the conveyor belt in some fixed positions. Objects attached with RFID tags move with the conveyor belt. Readers are responsible for collecting the ID information of all passing tags. Usually, tags' IDs are unknown, and all tags send messages to the reader only when they receive the reader's query request. Without any prior information, the reader cannot aim at any specific tag in its query request. One common strategy is carrying a query prefix in the reader's query request. If a tag matches with the received prefix, it replies to the reader. When more than one tag replies simultaneously, a collision occurs which increases the identification delay.

The identification task is more challenging in mobile systems where tags quickly go through the reader's reading range. Tags have a very limited time to participate in the identification process. Therefore, a tag may be unrecognized after it moves out of the reader's reading range, i.e., becomes a lost tag [12]. With higher moving speed, the tag lost probability is larger. In the literature, some works try to reduce the tag lost ratio in mobile systems with either mathematic modeling or group scheduling strategies. For example, Aloson et al. analyzed the tag lost ratio with a Markov chain model [12]. Gotfryd et al modeled a dynamic RFID system for an optimal configuration [13]. In [14,15], some two-phase identification protocols are proposed. However, the tag lost ratio of existing works is large, especially when the tag's moving speed increases.

In this work, we improve the identification efficiency of mobile RFID systems in two aspects, i.e., controlling the participating tags and accelerating the recognition process in each reading round. In general, we propose a novel admission-control-based dynamic query tree (ACDQT) protocol for mobile RFID tag identification. The main contributions are as follows,

- The identification process in mobile systems is analyzed, and a new multi-round admission control (MRAC) algorithm is developed to optimize the number of tags admitted in each reading round. With MRAC, the tag lost ratio is guaranteed, and the identification efficiency in each round is effectively improved;
- A dynamic query tree recognition (DQTR) algorithm is proposed to reduce the identification delay in each reading round. With DQTR, colliding tags are divided into more subsets based on the number of consecutive colliding bits; thus, the tag recognition efficiency is improved;
- Theoretic analysis is conducted to analyze the performance of DQTR in a single reading round. Moreover, numerous simulation results are presented to demonstrate the effectiveness of the proposed algorithm. Compared with existing benchmark works, the proposed ACDQT is proven to support higher tag flow rate with a lower tag lost ratio.

The remainder of this work is organized as follows: Section 2 introduces some representative tag identification protocols in both static and mobile systems. In Section 3, a fast-moving RFID tag identification system model is exhibited, and the frame structure and commands are described. Next, in Section 4, the proposed ACDQT protocol including the admission control and recognition strategies is described in detail. Then, theoretical analysis is conducted to obtain the identification delay of a single reading round in Section 5. The simulation results are illustrated in Section 6. Finally, Section 7 gives some conclusion remarks.

2. Related Works

In this section, we review some representative tag identification protocols for both static and mobile RFID systems.

In static systems, the tag set is assumed unchanged during the identification process. In such systems, the key problem is to reduce tag collisions, especially when the number of tags is large. In general, tag identification protocols mainly consist of two categories, i.e., the aloha-based, and the tree-based ones. In the first category, the reader identifies tags with a frame-slotted manner, and a tag replies to the reader with a randomly selected slot in each frame. However, using a random response manner, aloha-based protocols are of low efficiency. To improve the performance, some tag number estimation and frame adjustment strategies are proposed based on the statistical information of tag responses. For example, the Q-algorithm dynamically adjusts frame length with the feedback of slot status [16]. The maximum likelihood estimation algorithm estimates the number of tags with the Bayes method to optimize frame length settings in a dynamic frame-slotted aloha protocol [17]. In the second category, the reader identifies tags with a tree splitting method by grouping colliding tags into smaller subsets, such as query tree (QT) [18], binary tree splitting (BTS) [19], collision tree (CT) [4], etc. The identification process of these protocols follows a tree splitting structure in which each non-leaf vertex in the tree corresponds to a collision slot, and each leaf vertex refers to a successful or idle slot.

With a bit tracking technique, identification efficiency of tree-based protocols is efficiently improved. In the collision tree (CT) protocol [4], the reader splits colliding tags into two subsets based on the position of the first colliding bit without generating any idle slots. However, the splitting process is slow, and many collision slots are generated. Next, Landaluce et al. proposed a collision window tree (CwT) protocol [5] that uses a heuristic bit window strategy in the collision tree splitting process in order to reduce identification time and tags' communication overhead. In CwT, the number of total slots are increased, and the reader has to transmit more query messages to identify all tags. To further reduce collision slots, Su et al. proposed a dual prefix probing (DPPS) protocol [7] that makes use of the first two consecutive colliding bits to split colliding tags into more subsets. In [6], Zhang et al. proposed an M-ary collision tree (MCT) protocol to further accelerate the splitting process by making use of more colliding bits information. Recently, Su et al. also proposed a modified dual prefixes matching (MDPM) algorithm [20] that makes a bit query strategy in the M-ary query tree. Liu et al. designed a multi-bit identification collision tree (MICT) algorithm [21] and Hailemariam et al. developed a knowledge-based query tree algorithm [22]. However, these works only consider a static situation. In mobile systems, the tag set changes dynamically and tag participating time is very limited. These works cannot effectively identify tags in such situations.

In mobile situations, when the reader begins a new reading round, tags that have been recognized in preceding rounds may still be in the reader's reading range which results in duplicate recognition. Meanwhile, some newly arrived tags may join the identification process which further aggravates the tag collision situation. How to effectively control participating tags and quickly identify moving tags is very challenging. In the past decade, some works considered the moving tag identification problem. In [23], Saranga et al. first proposed an aloha-based framework for both static and mobile environments. Next, Alonso et al. analyzed the tag lost ratio in dynamic RFID systems and gave optimal configurations of frame-slotted aloha algorithms [24–26]. Later on, Kang et al. developed a reliable splitting strategy in an aloha algorithm to accelerate the identification process of moving tags [27]. Gotfryd also modeled the dynamic RFID system in [13]. However, these works only consider a basic aloha-based algorithm in which the identification efficiency is low. In [28], Zhu et al. developed a schedule-based RFID anti-collision protocol to maximize tag moving speed. They considered the identification deadlines of moving tags and scheduled an optimal number of tags to compete for the channel accordingly. With a schedule strategy, the identification efficiency is greatly improved.

In recent research, some new strategies have been developed for mobile RFID systems. In [14], Liu et al. proposed a blocking collision tracking tree algorithm to divide the identification process into two phases, one for staying tags and one for arriving tags. Making use of bit tracking to split tags into appropriate subsets, the identification efficiency is increased. In [6], Zhang et al. further improved the tag identification efficiency with a bit tracking technique. They developed an efficient bit-detecting (EBD) algorithm to quickly recognize unknown tags in each reading round. Thus, the proposed algorithm can support a much higher tag flow rate in mobile systems. Later on, Jia proposed a dynamic collision tree protocol to deal with arriving tags [29]. Yu et al. developed a dynamic tag population estimation algorithm with a Kalman filter [30]. In [31], Liu et al. designed a rate-adaptive algorithm to revisit the reading rate with mobility. Chen et al. also proposed a collision avoidance algorithm for mobile RFID devices [32]. However, the control strategies and reading methods of these works need further improvement to support higher tag moving speeds. To sum up, Table 1 compares different RFID tag identification protocols in static and moving situations.

Table 1. Comparison of different RFID tag identification protocols in static and moving situations.

	Static Situation		**Moving Situation**		
	ALOHA-Based	**Tree-Based**	**Frame Adjustment**	**Tree Enhancement**	**Scheduled**
features	tags reply to the reader in randomly selected slots	tags are continuously split into smaller groups	frame length in each reading round is dynamically adjusted	tree splitting process is enhanced in each reading round	using rate-adaptive or schedule strategies in each round
advantages	easy to implement, tags only need random number generator and counter	tags are identified deterministically with good performance	taking advantage of tag number estimation in preceding rounds, slot utilization is improved	with adaptive splitting or bit tracking, the identification process is accelerated in each round	identification process is scheduled with the information of ongoing rounds
efficiency	low → high		low → high		
complexity	simple → complex		simple → complex		

3. System Model

In this work, we consider the widely used conveyor belt applications and present a fast-moving RFID tag identification system model in this section. Then, the frame structure and some commands used in the tag identification process are described.

3.1. A Fast Moving RFID Tag Identification System

Among massive RFID applications, conveyor belt systems with RFID readers and tags are popular in various industries. In these applications, objects with RFID tags attached are placed on a conveyor belt. One or more RFID readers are usually mounted in a fixed position above (or beside) the conveyor belt. As the conveyor belt quickly moves, tags continuously move into and out of the reader's reading range. As is demonstrated in Figure 1, a general conveyor belt system is considered. Assume that each object has one tag attached that has a 96-bit unique identifier. The objects are denoted by their attached tags hereafter. In the model, tags are placed on the conveyor belt in series, and the distance between two adjacent tags is d m. The moving speed of the conveyor belt is v m/s. For simplicity, a single reader that is mounted above the conveyor belt is considered, and its coverage range is L m.

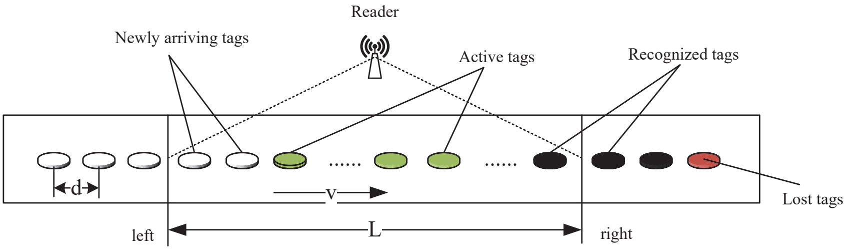


Figure 1. Conveyor-belt-oriented fast-moving RFID system model.

Tags first enter from the left side of the reader's reading range, then pass through a limited signal area and finally leave from the right side of the reading range. Affected by the moving speed and limited reading range, there may be situations where some tags pass through the reader's coverage area without been recognized. We define this type of tags as lost tags, and the tag lost ratio α is defined as the ratio of the number of tags passing through the reader's coverage area without being identified to the total number of tags passing through the reader's reading range within a certain time. The identification efficiency is defined as the average number of tags successfully identified per second. The goal of this work is to increase tag identification efficiency while minimizing the tag lost ratio in fast-moving RFID systems.

Compared with traditional static RFID systems, tag identification in mobile RFID systems is more challenging. The main reasons are twofold, as in the following.

- *Limited participating time*: RFID tags stay in the reader's reading range for a limited time, especially in high mobility situations. They enter from the left side of the reading range and leave from the right side. Tags will receive commands sent by the reader only when they are within the reader's reading range. With collision signals, the probability that a tag's response signal can be successfully recognized by the reader is low. For traditional static RFID systems, tags are always within the coverage range of the reader and can repeatedly contend to send response signals until being recognized since there is no participating time limitation.
- *Random access manner*: In each reading round, tags with various positions in the reading range will not have different priorities to access the channel. All tags within the reading range have the same chance, i.e., the same identification possibility. This random access property will lead the reader to identify newly arrived tags and earlier entered ones within the range in the same reading round. Thus, tags entering at the early stage may not be identified after they leave the reading range, which will aggravate the tag lost situation.

To facilitate the identification process, tags are limited to being recognized at most one time. When a tag is recognized by the reader, it will keep silent and not participate in subsequent identification processes until it leaves the reading range. Thus, the recognized tags will not affect the identification process of other participating tags.

3.2. Transmission Model

In this work, we use a frame-slotted model similar to the de facto standard EPC Global C1G2 [16]. In the model, time is divided into multiple frames, and each frame consists of several synchronized slots. The interaction between the reader and tags in each frame is shown in Figure 2, where three types of frames are illustrated, i.e., frames with two, four and eight slots. Here, the number of time slots in a frame is determined by the frame length parameter fl contained in the *Query* command.

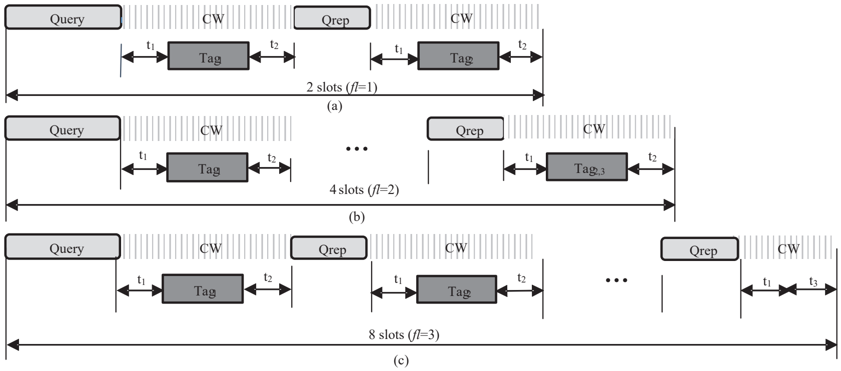


Figure 2. Frame slot structure: (**a**) when $fl = 1$, the frame consists of two slots; (**b**) when $fl = 2$, the frame consists of four slots; (**c**) when $fl = 3$, the frame consists of eight slots.

As shown in Figure 2, each frame begins with the reader's *Query* command and is followed with *k* consecutive slots, and each slot starts with the short *Qrep* command except for the first slot of a frame. This is because the first slot starts automatically right after the *Query* command. Each slot has three states, i.e., collision, idle and successful. A collision slot means that two or more tags reply simultaneously in the same slot. In such slots, the reader cannot effectively decode the received signal. In a successful slot, there is only one tag response so that the reader can successfully recognize this tag. Note that we do not consider capture effect as most works in the literature [3–7] since it has a similar effect on comparable protocols. Finally, an idle slot means that there is no tag response. In each frame, it takes the reader t_Q and t_R time to transmit *Query* and *Qrep* commands, respectively. The time for tag response message transmission is t_T. According to [16], t_1 is the time taken from the reader transmission to the tag response, t_2 is the interrogator response time required if a tag is demodulating the interrogator signal, and t_3 is the time a reader waits after t_1 if there is no tag response.

Moreover, the structures of commands and tag response messages are given in Table 2. The *Query* command consists of five components, i.e., head information, length of matching prefix *Lpre*, matching prefix *pre*, number of consecutive colliding bits *cbit* and CRC-16. The head segment contains the command, address, mask and other information as defined in [16]. The *pre* and *cbit* inform tags with the common prefix of the attending tags and the number of slots in the current frame, respectively; L_{pre} informs tags with the length of *pre*, which guarantees that tags can correctly obtain *pre* in the *Query* command. *Qrep* only contains command information. In the tag response, a 9-bit preamble accompanied by the remaining tag ID is transmitted. Note that we do not use CRC in the tag's response message because the Manchester coding used in tag-to-reader message transmission has the ability to check errors in a bit-wise manner.

Table 2. Command and data frame structure.

Query command	Head	L_{pre}	*pre*	*cbit*	CRC-16
	37 bits	8 bits	Var.	2 bits	16 bits
Qrep command	Command	Tag's response		Preamble	Data
	4 bits			9 bits	Var.

4. Admission-Control-Based Dynamic Query Tree Protocol for Fast Moving Tag Identification

In this section, a novel admission-control-based dynamic query tree (ACDQT) protocol is developed to effectively identify fast-moving tags while maintain a minimum tag lost ratio. In conveyor belt systems, the tag set constantly changes during the identification process. For easy implementation, the reader divides the identification process into multiple reading rounds. In each round, there may be three types of tags in the reader's coverage area, that is, deactivated tags that were recognized in preceding rounds, active tags that are participating in the recognition of the current round and newly arrived tags that are not participating in the recognition of this round as illustrated in Figure 1.

The main idea of ACDQT is to restrict the number of participating tags with admission control and recognize them with a high-efficiency dynamic query tree protocol in each reading round. In general, the reader first performs three rounds to estimate the tag flow rate. Next, it controls the number of admitted tags based on the estimation and system requirement. Each subsequent round only needs to control a similar number of incoming tags to ensure that the entire system meets the minimum tag lost ratio requirement. When there are enough tags entering the reader's reading range, a new round begins. In each round, a dynamic query tree protocol is designed to quickly identify tags. When collision occurs, the reader first checks the position of the first colliding bit k and the number of consecutive colliding bits after that position. Then, it divides these tags into smaller groups according to the number of consecutive collision bits. Compared with existing bit tracking protocols, the number of subsets of ACDQT is more flexible and appropriate. Thus, the proposed protocol can significantly reduce the number of collision slots and speed up the identification process. Before describing the proposed ACDQT protocol, Table 3 defines some symbols, functions and commands used in the paper.

Table 3. Symbol definitions.

Symbol	Definition
ID	Tag's unique identifier, d_i refers to the ith bit position
pre	Matching prefix transmitted by the reader at the beginning of each round, q_i denotes the i^{th} bit, and L_{pre} is the length of pre
Q	Query queue maintained by the reader to record (pre, k) of each frame
TC	Slot index
$Query()$	Frame start command broadcast by the reader to start each frame and to inform tags of the frame parameters.
$Qrep$	Slot start command broadcast by the reader to start each slot within a frame
$PUSH(a, Q)$	Push a into Q with first-in-first-out manner
$POP(Q)$	Obtain the first item and delete it from Q
$bin2dec(a)$	Convert binary string a to decimal number
$dec2bin(n, m)$	Convert decimal number n to an m-bit binary string

4.1. Multi-Round Admission Control Algorithm

In conveyor belt systems, tags continuously move through the reader's reading range. The participating time of a tag greatly affects the identification efficiency. In traditional methods, a newly arriving tag directly joins the current round or waits to participate in the subsequent round. If tag flow rate and identification efficiency differ widely, the identification process will be inefficient with much idle time or collisions. In this work, a multi-round admission control (MRAC) algorithm is proposed to improve the identification efficiency.

The identification process of MRAC is abstracted in Figure 3, where n is the number of tags participating in each round, and T is the time interval of two consecutive rounds. At the beginning, there is no tag in the reading range. With the conveyor belt moving for T_0 s, there are n_1 tags arrived, and the reader starts the first round immediately. Suppose after T_1 s, the reader recognized all n_1 tags and starts the second round. During this time, the number of newly arrived tags is n_2. Similarly, if the second round takes T_2 s, the number of newly arrived tags in this round is n_3, and the recognition time in round 3 is T_3. Suppose the conveyor belt keeps moving at a constant speed, the tag flow rate r_t is obtained by

$$r_t = n_2/T_1 = n_3/T_2 \text{ (tags/s)} \tag{1}$$

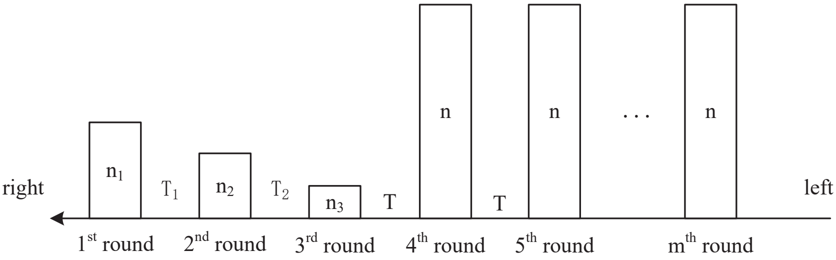


Figure 3. Multi-round tag recognition for conveyor belt systems.

The average time needed to identify one tag in the first three rounds is

$$T_{ave} = (T_1 + T_2)/(n_2 + n_3) \tag{2}$$

With the estimation results and system requirement, the number of tags admitted to participate in the subsequent round can be calculated. In what follows, we analyze the influence of participating tag number n on the tag lost ratio α in one round. As given in Figure 4, the identification process in a single round is considered in three cases, i.e., $n > N$, $n = N$ and $n < N$, where N is the maximum number of tags that the reader can recognize in a normal situation. In Figure 4, the shadowed rectangles give the number of participating tags, the white rectangles represent the number of slots used to identify tags, and L is the reader's coverage range.

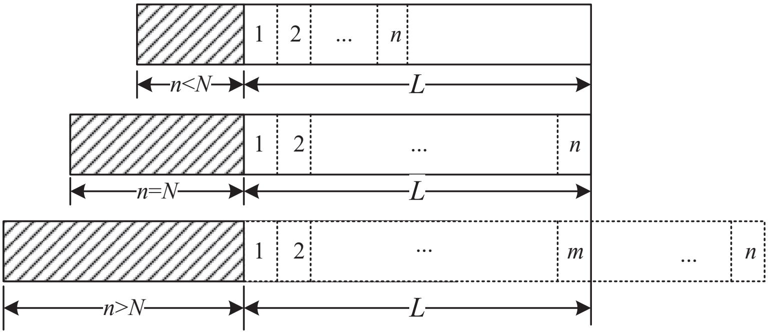


Figure 4. Recognition process in a single round.

When $n < N$, the reader can recognize all participating tags before they move out of its reading range. There is some time left before the reader starts the next round. Thus, the system does not reach its optimal situation. When $n = N$, the reader completely recognizes all participating tags and makes full use of time in such a reading round. There is no slot waste, and the tag lost ratio $\alpha = 0$. However, when $n > N$, the time needed to recognize all n tags is greater than the maximum staying time of these tags. Therefore, some of them may become lost. To balance the tag lost ratio and identification efficiency, the number of admitted tags in each round is critical.

When $n > N$, the number of tags that can be successfully recognized by the reader is m, $m < N$. Since more tags will worsen the collision situation, the actual number of recognized tags is smaller than the maximum value that a reader can recognize in a normal situation. In different positions of the reading range, the tag lost possibility varies. The first entering tag in a reading round will move for $l_1 = L - n \cdot d$ distance to leave the reading range. During this time, the average number of tags that can be identified by the reader is given by

$$S_1 = \frac{l_1}{T_{ave} \cdot r_t} = \frac{L - n \cdot d}{T_{ave} \cdot r_t}. \tag{3}$$

Since all tags will move into this position and experience a similar identification process, for a tag in the first position, its lost probability is given by

$$p_1 = \frac{n - S_1}{n} \tag{4}$$

Therefore, the average number of lost tags in the first position is $n_{lost}^1 = 1 \cdot p_1$. Similarly, in the ith position of the tag line, the tag will move for $l_i = L - n \cdot d + (i-1)d$ distance to leave the reading range. Then, the average number of tags identified during this time is

$$S_i = \frac{l_i}{T_{ave} \cdot r_t} = \frac{L - (n - i + 1) \cdot d}{T_{ave} \cdot r_t}. \tag{5}$$

Then, when a tag is in the ith position, the probability of being unrecognized after it moves out of the reader's reading range is given by

$$p_i = \frac{n - (i-1) + \left[(i-1) - \sum\limits_{j=1}^{i-1} n_{lost}^j \right] - S_i}{n - (i-1)} = \frac{n - \sum\limits_{j=1}^{i-1} n_{lost}^j - S_i}{n - (i-1)} \tag{6}$$

Note that $\mathcal{A} = (i-1) - \sum\limits_{j=1}^{i-1} n_{lost}^j$ is the number of lost tags prior to the ith position. The number of tags that will participate in the identification process of the ith position can be calculated by $n - (i-1) - \mathcal{A}$. The average number of lost tags in the ith position is $n_{lost}^i = 1 \cdot p_i$. Then, the tag lost ratio is

$$\alpha = \frac{\sum\limits_{i=1}^{n-m} n_{lost}^i}{n}. \tag{7}$$

Substituting (5) and (6) into (7), the tag lost ratio of a single reading round is obtained. By solving (7), the number of tags participating in each round is determined to meet the system requirement on the tag lost ratio. With MRAC, the reader waits for a short time to allow enough tags to enter the reading range and starts the identification process in each subsequent round.

4.2. Dynamic Query Tree Recognition Algorithm

In this section, we propose a dynamic query tree recognition (DQTR) algorithm to effectively identify tags in each round. DQTR follows the query tree recognition process with multiple branches. In general, the reader divides tags in each colliding slot with the help of consecutive colliding bits in the tags' responses. When the reader detects a collision, it first checks the position of the first colliding bit p and the number of consecutive collision bits k after this position. Then, it divides colliding tags into 2^k subsets to accelerate the identification process. Compared with existing bit tracking protocols, DQTR solves colliding tags with a more flexible and appropriate manner which significantly reduces time costs. The detailed algorithm is given as follows.

At the beginning of a reading round, the reader initializes queue $Q = \{(\varepsilon, 0)\}$. Then, it obtains $(pre,\ k) = Queueout(Q)$ and broadcasts $Query(pre, k)$ to start the first frame. Note that $Queueout(Q)$ is to obtain the first item and delete it from queue Q.

On receiving the reader's *Query* command, tags execute matching, indexing and replying operations in sequence as shown in Figure 5.

- *Matching*: A tag first compares its ID with the matching prefix *pre*. If it matches, the tag transits to the transmission state and will participate in the current frame. Otherwise, it waits for the next *Query* command.
- *Indexing*: If a tag is in the transmission state, it checks the slot index from $p+1$ to $p+k$ bits in its ID and converts into a decimal number g, i.e.,

$$g = bin2dec(d_{p+1}, d_{p+2}, \cdots, d_{p+k}) \tag{8}$$

- *Replying*: If $g = 0$, the tag replies its remaining ID, i.e., $(d_{p+k+1}, d_{p+k+2}, \cdots, d_L)$, to the reader. Otherwise, it waits for the reader's *Qrep* command, and reduces g byone after receiving this command until zero.

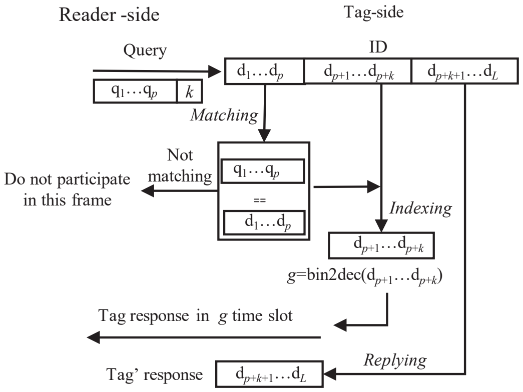


Figure 5. Tag's operation after receiving the reader's Query command.

After receiving tags' responses in each slot, the reader determines the state of the current slot and identifies tags. In summary, there are four types of slots to appear.

- *Singleton slot*: If there is only one tag reply, the received message can be successfully decoded. Then, the reader identifies the tag and recovers its ID with

$$pre \,||\, dec2bin(g,k) \,||\, (d_{p+k+1},\ d_{p+k+2},\ \cdots,\ d_L) \tag{9}$$

  where || is the concatenating operation.
- *Two readable slot*: There are replies from two tags in the slot, and the received message contains only one colliding bit. Since the tag's ID is unique, the reader can recognize the two tags in one slot. For example, the message received by the reader is "10x101", where "x" is the colliding bit. The two tag IDs to be identified are

$$ID = pre||dec2bin(g,k)||\begin{cases}10\underline{1}101\\10\underline{0}101\end{cases} \tag{10}$$

- *Idle slot*: If the reader receives no message at the slot, it is an idle slot.
- *Collision slot*: When more than two tags reply simultaneously in the slot, a collision slot occurs since the reader cannot recover any ID information. In this slot, the reader checks the position of the first colliding bit and the number of consecutive colliding bits after this position. Next, it obtains the parameters for subsequent frames. For

example, if the decoded message is ”$1xx01$”, the frame parameters are obtained by calculating

$$pre' = pre|| + dec2bin(g,\ k)||1,\ k' = 2. \tag{11}$$

Then, the reader pushes (pre', k') to Q.

After executing all slots in the current frame, the reader checks whether Q is empty. If Q is empty, it terminates the identification of this round since all the tags are identified. Otherwise, it obtains frame parameters (pre, k) by $Queueout(Q)$ and sends $Query(pre, k)$ command to start the next frame. More specifically, Algorithms 1 and 2 give the pseudocodes of the reader's and tags' operations in DQTR, respectively. The whole identification process of ACDQT is also given in Figure 6.

Algorithm 1: Reader's Operations

```
initiate $Q = \{(\varepsilon, 0)\}$;
while $Q$ is not empty do
    Obtains $(pre, k) = Queueout(Q)$, and broadcasts $Query(pre, k)$;
    for $s = 0 : 2^k - 1$ do
        Waits for tag responses and checks state of the slot;
        if Singleton slot then
            identifies the tag with (9) ;
        else if Two readable slot then
            identifies the tags with (10);
        else if Collision slot then
            obtains $(pre', k')$ with (11) and Queuein($(pre', k')$, Q);
        end
        Send $Qrep$;
    end
end
```

Algorithm 2: Tags' Operations

```
After receiving $Query(pre, k)$;
if $(d_1,\ d_2,\ \cdots,\ d_p) == pre$ then
    $g = bin2dec(d_{p+1}, d_{p+2}, \ldots, d_{p+k})$;
    if $g = 0$ then
        $Reply(d_{p+k+1}, d_{p+k+2}, \cdots, d_L)$;
    else if receive $Qrep$ then
        $g = g - 1$;
    end
else
    wait for the next $Query()$ command;
end
```

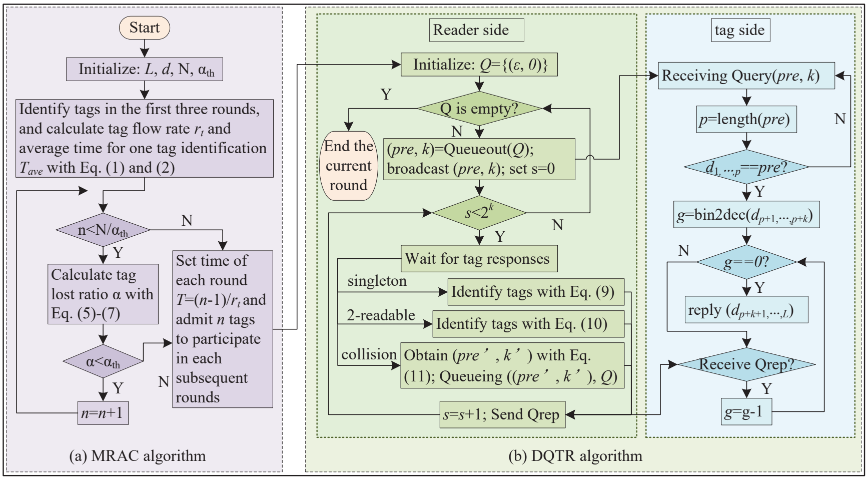

Start
Initialize: L, d, N, α_th
Identify tags in the first three rounds, and calculate tag flow rate r_t and average time for one tag identification T_ave with Eq. (1) and (2)
n<N/α_th
N
Y
Calculate tag lost ratio α with Eq. (5)-(7)
Set time of each round T=(n-1)/r_t and admit n tags to participate in each subsequent rounds
α<α_th
N
Y
n=n+1
(a) MRAC algorithm
Reader side
Initialize: Q={(ε, 0)}
Q is empty?
Y
N
End the current round
(pre, k)=Queueout(Q); broadcast (pre, k); set s=0
s<2^k
N
Y
Wait for tag responses
singleton
Identify tags with Eq. (9)
2-readable
Identify tags with Eq. (10)
collision
Obtain (pre', k') with Eq. (11); Queueing ((pre', k'), Q)
s=s+1; Send Qrep
tag side
Receiving Query(pre, k)
p=length(pre)
d_1,…,p==pre?
N
Y
g=bin2dec(d_p+1,…,p+k)
g==0?
N
Y
reply (d_p+k+1,…,L)
Receive Qrep?
Y
g=g-1
(b) DQTR algorithm

Figure 6. Flowchart of the proposed ACDQT algorithm: (**a**) the admission control phase with MRAC; (**b**) the identification phase in each round with DQTR.

An Example

To clearly show the DQTR algorithm, Figure 7 illustrates an example of the identification process for 10 tags, and the tag IDs are given in Table 4. In Figure 7, F_i refers to the *i*th frame, and the queue Q of each frame is also given in the right side.

At the beginning, the reader initializes queue $Q = \{(\varepsilon, 0)\}$. In the first frame F_1, it obtains parameters from Q and broadcasts $Query(\varepsilon, 0)$. Note that the initial frame consists of only one collision slot, since all tags will match with prefix ε. After receiving tags' responses, the decoded message is "*xxxxxxxxxx*". For the sake of simplicity, we use the first three constitutive colliding bits. Then, the reader sets $pre = \varepsilon$, $k = 3$, and pushes them into Q. In F_2, all tags will participate in this frame. After checking the first three bits of their ID, they obtain slot indices and reply in the corresponding slots. In this frame, Tag$_1$ and Tag$_2$ are identified in the two readable slots, i.e., the second slot, Tag$_6$ and Tag$_{10}$ are identified in two singleton slots, i.e., the fifth and seventh slots, respectively. The fourth and sixth slots are two collision slots with $k = 2$ and $k = 1$, respectively. At the end of F_2, Q becomes $\{(011, 2), (101, 1)\}$. The reader goes through the subsequent frames until Q is empty.

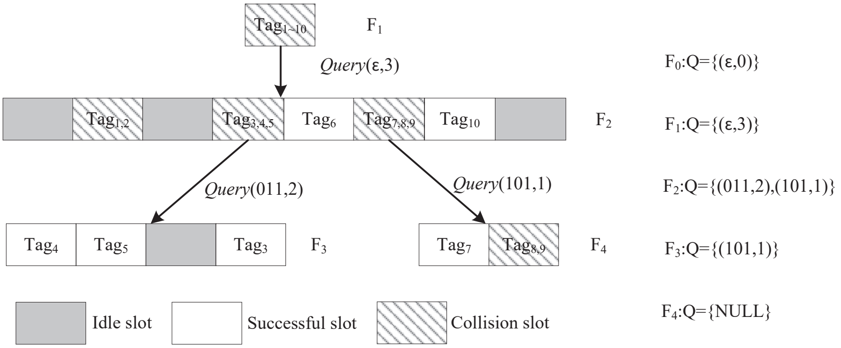


Figure 7. Example of DQTR recognition process.

Table 4. Tags' ID information.

Tag	ID	Tag	ID	Tag	ID	Tag	ID
Tag_1	0011000111	Tag_2	0011100111	Tag_3	0111101101	Tag_4	0110001010
Tag_5	0110100111	Tag_6	1000011010	Tag_7	1010100010	Tag_8	1011111010
Tag_9	1011111000	Tag_{10}	1101100111				

At the end of frame F_2, $Q = \{(011, 2), (101, 1)\}$, which includes two frame parameters. Next, the reader takes $(011, 2)$ from Q and broadcasts $Query(011, 2)$ to start the third frame F_3. There are four time slots in F_3, of which the first, second and fourth time slots have only one tag response, and the third time slot is an idle slot. The reader identifies Tag$_4$, Tag$_5$ and Tag$_3$ in these three singleton slots, separately. Then, it continues to take frame parameters $(101, 1)$ from Q. In frame F_4 , two slots are executed. The first slot has only one tag response, and the reader can directly identify Tag$_7$. The message reply in the second slot is "1110x0", so the reader recognizes Tag$_8$ and Tag$_9$ in this two-readable slot. At the end of F_4, Q becomes empty. The reader terminates this reading round.

The identification performance of DQTR is compared with two benchmark works, i.e., CT [4] and DPPS [7]. Table 5 lists the number of transmitted message bits on both the reader and tag sides as well as the total identification time. As can be observed, the proposed DQTR algorithm transmits the least number of message bits on both the reader and tag sides, and it also takes the least time to identify all tags.

Table 5. Compared with CT and DPPS.

	Message Transmitted by Reader (bit)	Message Transmitted by Each Tag (bit)	Total Identification Time (s)
CT	1028	191	0.0201
DPPS	585	152	0.0143
DQTR	**425**	**131**	**0.0124**

The bold values are the least cost in each column.

5. Performance Analysis

In mobile systems, ACDQT performs two key strategies, i.e., multi-round admission control (MRAC) and dynamic query tree recognition (DQTR), to accelerate the identification efficiency. In MRAC, the number of admitted tags is controlled to facilitate the identification of each round. Therefore, the overall system efficiency highly depends on the identification process in each round. In this section, we analyze the performance of DQTR in each round based on probability theory and classical tree analysis methods [33–35].

In DQTR, all tags will reply in the initial slot. As demonstrated in Figure 7, if there is more than one tag replying simultaneously, a collision slot occurs. The colliding tags will be split into small subsets according to the number of consecutive colliding bits after the maximum common prefix, i.e., they will attend a new frame in the next layer of the tree. Let $P_{bc}(i, k)$ be the probability that there are k consecutive colliding bits after the maximum common prefix when i tags reply in the slot. Then, the number of slots needed to identify n tags using DQTR in each round is given by

$$S(n) = 1 + \sum_{k=1}^{L-p} P_{bc}(n, k) \cdot S_k(n, k), \tag{12}$$

where L and p are the lengths of the tag ID and the maximum common prefix of colliding tags, respectively. $S_k(n, k)$ is the number of slots needed to identify n colliding tags when the number of consecutive collision bits in tag responses is k.

Assume that i tags reply in the same slot. There should be at least one colliding bit in the received message. In a specific bit position, if the corresponding bit of all response messages are the same, i.e., all zeroes or ones, this bit position is not colliding. Thus, the probability that a specific bit position is colliding can be expressed as

$$P_b = 1 - \frac{1}{2^i} \cdot 2 = 1 - \frac{1}{2^{(i-1)}}. \tag{13}$$

In a collision slot, there is at least one colliding bit. Thus, the probability of the first colliding bit in tag responses in a collision slot with i tags is $P_{bc}(i,1) = 1,\ i > 1$. If the number of consecutive colliding bits k is greater than one, that means the 2nd to kth bits are all colliding bits. Therefore, in a collision slot with i attending tags, the probability that k consecutive colliding bits exist after the maximum common prefix is obtained by

$$P_{bc}(i,k) = p_b^{k-1} \cdot (1 - p_b) = \left(1 - \frac{1}{2^{i-1}}\right)^{k-1} \cdot \frac{1}{2^{i-1}}, \quad k > 1. \tag{14}$$

Note that in a collision slot, there should be at least one colliding bit, i.e., the colliding bit after the maximum common prefix.

In a collision slot with k consecutive colliding bits after the maximum common prefix, the tags will be split into 2^k sets and will attend 2^k slots in the subsequent frame. Assume the event that a tag assigned to a specific slot follows the binomial distribution as most previous works [5–7,15]. The probability that i tags are assigned into one slot in a frame with 2^k slots is given by

$$P(i,2^k) = C_n^i \left(\frac{1}{2^k}\right)^i \left(1 - \frac{1}{2^k}\right)^{n-i}. \tag{15}$$

Since all collision slots will split in the same way, the number of slots in subsequent frames can be calculated with the following iterative function:

$$S_k(n,k) = 2^k \left\{ P(0,2^k) + P(1,2^k) + \sum_{i=2}^{n} P(i,2^k) \sum_{j=1}^{L-p'} P_{bc}(i,j) S_k(i,j) \right\} \tag{16}$$

where p' is the length of maximum common prefix of the colliding tags and it varies in different slots, and 2^k is the frame length of the stretched frame when the number of consecutive colliding bits is k. Note that $S_k(2,k) \leq 2$. Substituting (14), (15) and (16) to (12), the number of slots needed to identify n tags by DQTR in each round is obtained. Then, the slot efficiency is given by $n/S(n)$.

Since different types of slots will occupy various time intervals (for example, a collision slot takes much longer time than an idle slot), the slot efficiency cannot effectively evaluate the performance of a practical RFID system. So, we also consider the average identification time to recognize one tag as follows,

$$T_{ave} = \frac{S_{succ}(n)T_{succ} + S_{idle}(n)T_{idle} + S_{coll}(n)T_{coll}}{n}, \tag{17}$$

where $S_{succ}(n)$ is the number of singleton and two-readable slots, and $S_{idle}(n)$ and $S_{coll}(n)$ are the numbers of idle and collision slots, respectively. In a deterministic algorithm, all tags will be recognized. We have $S_{succ}(n) \leq n$. The values of S_{coll} and S_{idle} can also be calculated with similar analysis of $S(n)$.

As shown in Figure 7, the number of collision slots needed to identify n tags consists of the initial collision slot on top of the tree and the collision slots in subsequent frames in each layer of the tree. The second layer consists of only one frame, and its frame length depends on the number of consecutive colliding bits after the maximum common prefix in the initial slot. Participating tags in this slot are assigned to a stretched frame (i.e., tree branch) according to their slot indexes obtained from their IDs. Let $S_{coll}^{k}(n,k)$ be the number of collision slots needed to identify *n* colliding tags when the number of consecutive colliding bits after the maximum common prefix is *k*. The total number of collision slots is given by

$$S_{coll}(n) = 1 + \sum_{k=1}^{L-p} P_{bc}(n,k) S_{coll}^{k}(n,k), \tag{18}$$

In each frame, the attending tags are randomly assigned to each slot. If more than one tag is grouped into the same slot, these tags will repeat this process in a new frame in lower layers of the tree. Then, we can obtain

$$S_{coll}^{k}(n,k) = 2^{k} \sum_{i=2}^{n} P(i,2^{k}) \sum_{j=1}^{L-p'} P_{bc}(i,j) S_{coll}^{k}(i,j), \tag{19}$$

where 2^k is the number of slots in the frame. If two tags reply in the same slot, there should be a collision or a two-readable slot. If it is a two-readable slot, the two tags can be identified directly. Otherwise, they will be split into two subsets according to the position of the first colliding bit and be recognized in two singleton slots. Then, we have $S_{coll}^{k}(2,j) = 1$. Resolving (19) with an iterative method and substituting the results into (18), the number of collision slots is obtained.

Next, as shown in Figure 7, idle slots will occur if no tags are assigned. Thus, the number of idle slots in the second layer, i.e., the frame stretched from the initial collision slot, is given by

$$S_{idle} = \sum_{k=1}^{L-p} P_{bc}(n,k) S_{idle}^{k}(n,k). \tag{20}$$

In each subsequent frame, the probability that an idle slot occurs is $P(0,2^k)$ and that of a collision slot is $P(i,2^k),\ i \geq 2$. Each collision slot will stretch a new branch (i.e., frame). Therefore, the number of idle slots generated in subsequent frames is given by

$$S_{idle}^{k}(n,k) = 2^{k} \left\{ P(0,2^{k}) + \sum_{i=2}^{n} P(i,2^{k}) \sum_{j=1}^{L-p'} P_{bc}(i,j) S_{idle}^{k}(i,j) \right\} \tag{21}$$

Since a collision slot with two tags will be identified as a two-readable slot or two singleton slots in the next layer, there should be no idle slots in sucha situation, that is, $S_{idle}^{k}(2,j) = 0$. Similarly, with iterative resolving, the number of idle slots is obtained. Substituting (18), (19) and (20) and (21) to (17), the average identification time is obtained.

6. Simulation Results

In this section, we first evaluate the performance of ACDQT in a single reading round and compare it with the three most related benchmark works, i.e., the collision window tree (CwT) [5], M-ary collision tree (MCT) [6] and dual prefix probing (DPPS) [7] algorithms. In the literature, CwT, MCT and DPPS are the most recent works that use bit tracking technology. In what follows, we also give the simulation results in conveyor belt systems. The throughput and tag lost ratio of ACDQT are evaluated and compared with the three most related benchmark works that solve the moving tag identification problem, i.e., efficient bit detecting (EBD) [15], dynamic collision tree (DCT) [29] and basic frame-slotted ALOHA (BFSA) [26]. The simulation is conducted based on the system model introduced in Section 3 where a single reader is mount above the conveyor belt. Tags are assumed equally spaced in the conveyor belt and move at a constant speed. Each tag has a 96-bit unique identifier, and the tag IDs are uniformly distributed. Moreover, similar to most works in the literature [29–32], we do not consider transmission errors and capture effect during the identification process since they have a similar impact on the comparable protocols. We use MATLAB R2019a to perform the simulation, and each simulation result is averaged from 100 tests. Table 6 lists the values of some parameters used in the simulation. Note that L_{cmd} is the length of the *Query* command, which varies in different algorithms.

Table 6. Parameters used in simulation.

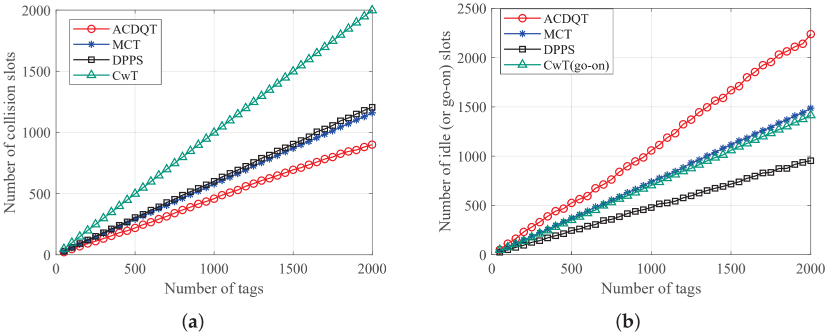
Parameter	Value	Parameter	Value
L	96 bits	Data rate D	160 kbps
$t_1,\ t_2$	25 us	t_3	12.5 us
t_Q	L_{cmd}/D	t_R	$4/D$

6.1. Single Round Identification

In this subsection, we simulate the identification process in a single round in a static situation. In the evaluation, we first give the numbers of collision and idle slots to identify all tags, respectively. Next, the number of message bits transmitted by the reader and tags are given separately. Then, the average identification time for one tag identification and time efficiency of the comparable algorithms are also exhibited.

6.1.1. Number of Slots

Firstly, Figure 8 gives the numbers of collision and idle slots needed to identify tags. It should be noted that in DPPS, each slot consists of two consecutive tag responses, which is actually one frame with two slots, and there is no *Qrep* command in the second slot. For a fair comparison, we consider this as two slots, and the state of each slot is related to the number of simultaneous tag responses. In CwT, the go-on slot takes such a very short time that they are compared with idle ones.



(**a**) (**b**)

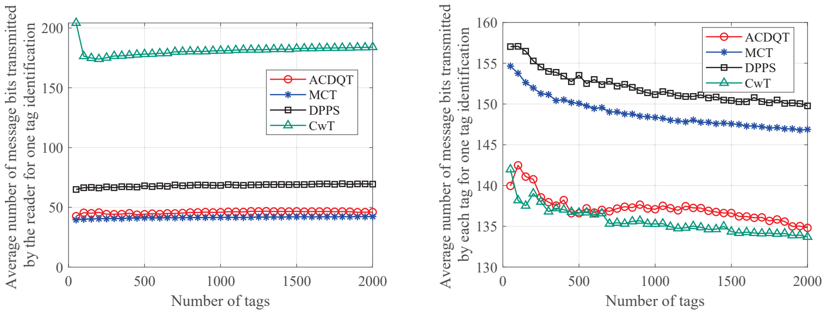
Figure 8. Number of slots needed to identify tags: (**a**) collision slots; (**b**) idle (or go-on) slots.

As can be observed from Figure 8a, the proposed ACDQT algorithm takes the least number of collision slots to identify tags, while DPPS and MCT take more collision slots than ACDQT. CwT takes the most number of collision slots. This is because DPPS only splits colliding tags into two or four subsets. MCT splits tags into a fixed number of subsets, whereas the proposed ACDQT algorithm splits colliding tags into various numbers of subsets which is based on the number of consecutive colliding bits. Dynamically splitting colliding tags into smaller subsets, the number of collision slots is significantly reduced. Moreover, one can also observe that CwT takes much more collision slots than comparable algorithms. The main reason is that CwT always splits colliding tags into two subsets based on the first colliding bit position. The splitting process is slow, especially when the number of colliding tags is large. Therefore, CwT takes much more collision slots than others, and the gap becomes larger with the increase of tag number.

Figure 8b illustrates the number of idle slots needed to identify tags. As shown, ACDQT takes more idle slots than other protocols. In MCT, DPPS and ACDQT, colliding tags are divided into more subsets according to the number of consecutive colliding bits. Each subset corresponds to a slot in the new frame. One can not sense the number of tags in each subset. So, there are some idle slots, and the number of idle slots increases with larger frame length. In CwT, there are no idle slots, but the number of go-on slots is large. Although ACDQT takes more idle slots than comparable algorithms, it takes the least number of collision slots. As known, a collision slot takes much more time than an idle (or go-on) slots. Therefore, ACDQT will take a shorter time to identify tags than comparable protocols.

6.1.2. Number of Transmitted Message Bits

In the comparable algorithms, the frame structure and messages transmitted in each slot are different. Only the number of collisions and idle slots are not enough to evaluate the overall performance of these algorithms. The communication overhead of the RFID tag identification protocol refers to the number of message bits sent and received by the reader and tags during the identification process. The reader side overhead refers to the total number of message bits sent by the reader, and the tag side overhead refers to the total number of message bits in tag replies to the reader. In the simulation, a tag uses a 96-bit ID, and the reader needs to send two necessary commands during the identification process, i.e., the Query and Qrep commands. Since the identification time highly depends on the number of transmitted message bits, we give the comparison results of these algorithms in Figure 9.



(**a**) (**b**)

Figure 9. Average number of message bits needed for one tag identification: (**a**) on the the reader side; (**b**) on the tag side.

The average number of command bits transmitted by the reader for one tag identification (i.e., communication overhead on the reader side) is shown in Figure 9a. It can be observed that ACDQT and MCT transmit smaller numbers of command bits on the reader side, and the communication overheads are stable at around 42 and 45 bits, respectively. This is because ACDQT and MCT both use a multi-branch tree structure. Compared with 180 bits of CwT and 68 bits of DPPS, communication overhead of ACDQT on the reader side is reduced by about 75% and 33.8%, respectively. This is because the proposed ACDQT protocol uses the number of consecutive collision bits to divide colliding tags into different groups in a new frame. In each frame, only one *Query* command and several *Qrep* commands are sent. This greatly saves the amount of command bits needed to send. Although the DPPS algorithm uses a *Query* command in each frame with two consecutive slots, the amount of command bits transmitted in each frame is small, but DPPS requires more frames to identify tags than ACDQT does. Thus, communication overhead on the reader side of DPPS is higher than that of ACDQT. In CwT, each slot comes with a *Query* command. With more slots, CwT transmits more command bits on the reader side than comparable algorithms.

Figure 9b illustrates the average number of message bits transmitted by the tag for one tag identification (i.e., communication overhead at each tag). As shown, a tag transmits fewer message bits in ACDQT and CwT than in the MCT and DPPS algorithms. This is because ACDQT takes the least number of collision slots. Thus, the response time for each tag is reduced accordingly. Secondly, a tag only needs to reply part of the ID information in each slot, which greatly reduces the number of message bits transmitted. Therefore, the communication overhead of each tag by implementing ACDQT is much lower than comparable algorithms. In CwT, a tag replies short messages in each slot. Therefore, although CwT takes more slots, the number of message bits transmitted by each tag is small.

6.1.3. Time Performance

Finally, Figure 10 demonstrates the average time needed to identify one tag and the time efficiency. It should be noted that time efficiency is defined as the ratio of the time cost of a singleton slot to the average time needed to identify one tag. As one can observe in Figure 10a, the proposed ACDQT takes about 1.2 ms to identify a tag on average, whereas, MCT, DPPS and CwT take about 1.25 ms, 1.43 ms and 1.95 ms for one tag identification, respectively. Compared with MCT, DPPS and CwT, the time gain of ACDQT is around 4.2%, 19.2% and 62.5%, respectively. It also demonstrates that although ACDQT takes more idle slots than other algorithms, the time saved by the smaller number of collision slots greatly improves the identification performance. Therefore, ACDQT takes much less time than the comparable algorithms. Moreover, in Figure 10b, one can also observe that the proposed ACDQT algorithm always has the highest time efficiency, which is about 50%.

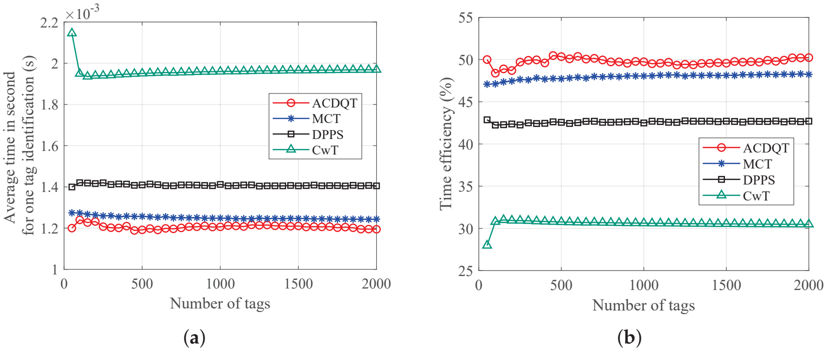


Figure 10. Time performance: (**a**) average time for one tag identification; (**b**) time efficiency.

To sum up, in single-round identification (i.e., a static situation), the proposed ACDQT algorithm is superior to comparable algorithms in terms of fewer number of collision slots, lower communication overhead and shorter identification delay.

6.2. Fast-Moving Tag Identification

To evaluate tag recognition performance in a conveyor belt system, we measured from two metrics: throughput and tag lost ratio. Throughput refers to the number of tags recognized per unit of time, and the tag lost ratio is the ratio of tags that are not recognized (lost tags) after they move out of the reader's reading range to the total number of tags passing through. The moving speed of the incoming tag flow of the system (termed tag flow rate) ranges from 0 to 800 tags/s, and the distances between tags are evenly distributed. The performance of ACDQT is compared with the three most related works dealing with moving tag situations, i.e., DCT [29], BFSA [26] and EBD [15]. Simulation results are illustrated in Figure 11.

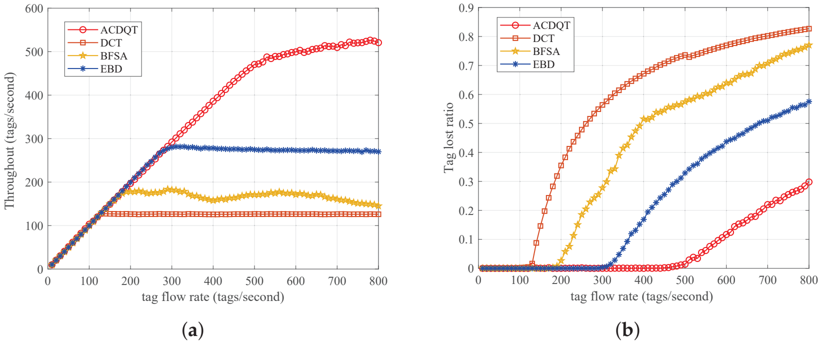


Figure 11. Identification performance for fast-moving tags: (**a**) throughput; (**b**) tag lost ratio.

As can be observed from Figure 11a, the proposed ACDQT algorithm achieves much higher throughput than comparable algorithms, and the highest throughput is about 510 tags/s. Compared with EBD, BFSA and DCT, the throughput is improved by 20%, 85% and 140%, respectively. When tag flow rate is greater than 510, the throughput of ACDQT basically tends to be stable. However, when tag flow rate of BFSA is greater than 160, the fluctuation of throughput is relatively large, and it changes around 150. Since DCT directly repeats the identification process for fast-moving tags, it is limited by the performance of the tree splitting process. When new tags enter the reader's reading range, they join the identification process immediately, which may collide with other participating tags. This greatly lowers the throughput in mobile systems. In EBD, newly arrived tags will participate in the identification process in the next round which relieves the collision situation. It also uses a new bit tracking strategy to accelerate the identification process in each round. Thus, its throughput is higher than DCT and BFSA but lower than ACDQT.

In Figure 11b, the tag lost ratio of ACDQT is 0 when tag flow moves slower than 470 tags/s, while in DCT, BFSA and EBD, the values are 120, 170 and 290, respectively. After these points, the tag lost ratio increases with the tag flow rate. This is because with the tag flow rate increasing, the reader does not have enough time to identify all tags in the current round before they move out of reading range. In this situation, some tags may leave unrecognized after they move out of the reader's reading range, resulting in a lost tag. With larger tag flow rate, the lost tag situation becomes worse. Nevertheless, the proposed ACDQT has much higher throughput and a lower tag lost ratio than comparable algorithms, which is more suitable to be implemented in fast-moving RFID systems. Finally, Table 7 lists the overall results of the comparable algorithms in single round and fast-moving situations. Note that the bold values refer to the best performance in each group, and the results are in accordance with these in Figures 8–10.

Table 7. Simulation results of the comparable algorithms in single round and fast-moving situations.

Single Round		**Number of Slots**		**Average Number of Message Bits**		**Time Performance**	
		Collision	**Idle**	**Reader Side**	**Tag Side**	**Average Time**	**Time Efficiency**
n = 500	ACDQT	**219.5**	525.1	44.3	**136.6**	**1.19 ms**	**50.4**%
	MCT	289.5	372.5	**41.2**	150.1	1.25 ms	47.7%
	DPPS	304.5	**245.1**	68	153.5	1.41 ms	42.6%
	CwT	498	351.1	178.1	136.7	1.95 ms	30.8%
n = 1500	ACDQT	**694.7**	1669.3	46.6	136.6	**1.21 ms**	**49.6**%
	MCT	870.4	1115.3	**42.1**	147.6	1.24 ms	48.1%
	DPPS	904.6	**716.8**	69.1	150.4	1.41 ms	42.7%
	CwT	1498	1059.1	182.8	**134.3**	1.97 ms	30.5%
fast moving		tag flow rate = 300		tag flow rate = 500		tag flow rate = 700	
		throughput	tag lost ratio	throughput	tag lost ratio	throughput	tag lost ratio
ACDQT		**291.99**	**0**	**470.54**	**0.01**	**509.68**	**0.22**
DCT		126.18	0.56	126.58	0.74	126.23	0.80
BFSA		181.89	0.28	170.93	0.57	160.55	0.71
EBD		279.85	0.01	274.71	0.33	271.58	0.51

The bold values are the best performance in each column.

7. Conclusions

In this paper, we established an identification model for mobile RFID systems and proposed an ACDQT algorithm for fast-moving tag identification. In ACDQT, a new multi-round admission control mechanism is designed to admit reasonable tags participating in each reading round. Next, a novel dynamic query tree strategy was developed to quickly identify tags in each round. Theoretical analysis was conducted to calculate the number of slots and average time needed to identify tags in a single round. We conducted numerous simulations to evaluate the identification performance in a single round and in multiple rounds in conveyor belt systems. The performance of ACDQT is also compared with the most related benchmark works. Simulation results demonstrate that ACDQT outperforms existing works in diverse situations. In our future work, we will consider using a machine learning method for tag flow estimation in the admission control process.

Author Contributions: Methodology, J.P. and N.Z.; conceptualization, L.Z. and L.L.; formal analysis, M.F.; validation, Q.H. and J.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (No. 61902182), the Natural Science Foundation of Jiangsu Province of China (No. BK20190409), the Aeronautical Science Foundation of China (No. 2016ZC52029), Qing Lan Project of Jiangsu Province of China, and China Postdoctoral Science Foundation (No. 2019TQ0153) and the Future Network Scientific Research Fund Project (FNSRFP-2021-ZD-4).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No public data link are privided in this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Elbasani, E.; Siriporn, P.; Choi, J.S. *A Survey on RFID in Industry 4.0*; part of EAI/springer innovations in communication and computing book series; Springer: Cham, Switzerland, 2019; pp. 1–16.
2. Landaluce, H.; Arjona, L.; Perallos, A.; Falcone, F.; Angulo, I.; Muralter, F. A review of IoT sensing applications and challenges using RFID and wireless sensor networks. *Sensors* **2020**, *20*, 2495. [CrossRef] [PubMed]
3. Klair, D.K.; Chin, K.-W.; Raad, R. A survey and tutorial of RFID anti-collision protocols. *IEEE Commun. Surv. Tutorials* **2010**, *12*, 400–421. [CrossRef]
4. Jia, X.; Feng, Q.; Ma, C. An efficient anti-collision protocol for RFID tag identification. *IEEE Commun. Lett.* **2010**, *14*, 1014–1016. [CrossRef]
5. Landaluce, H.; Perallos, A.; Onieva, E.; Arjona, L.; Bengtsson, L. An energy and identification time decreasing procedure for memoryless RFIDtag anti-collision protocols. *IEEE Trans. Wireless Commun.* **2016**, *15*, 4234–4247. [CrossRef]
6. Zhang, L.; Xiang, W.; Tang, X.; Li, Q.; Yan, Q. A Time- and Energy-Aware Collision Tree Protocol for Efficient Large-Scale RFID Tag Identification. *IEEE Trans. Ind. Informatics* **2018**, *14*, 2406–2417. [CrossRef]
7. Su, J.; Sheng, Z.; Wen, G.; Leung, V.C.M. A time efficient tag identification algorithm using dual prefix probe scheme (DPPS). *IEEE Signal Process. Lett.* **2016**, *23*, 386–389. [CrossRef]
8. Su, J.; Sheng, Z.; Liu, A.X.; Han, Y.; Chen, Y. A group-based binary splitting algorithm for UHF RFID anti-collision systems. *IEEE Trans. Commun.* **2020**, *68*, 998–1012. [CrossRef]
9. Roberti, M. Wal-Mart begins RFID rollout. *RFID J.* **2004**, 75–77. Available online: https://www.rfidjournal.com/wal-mart-begins-rfid-rollout (accessed on 30 April 2004).
10. Caccami, M.C.; Amendola, S.; Occhiuzzi, C. Method and system for reading RFID tags embedded into tires on conveyors. In Proceedings of the 2019 IEEE International Conference on RFID Technology and Applications (RFID-TA), Pisa, Italy, 25–27 September 2019; pp. 141–144.
11. Badriev, A.; Makarova, I.; Buyvol, P. The RFID system for accounting and control of truck tires with two-step identification: A case study. In Proceedings of the 2020 13th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, UK, 14–17 December 2020; pp. 100–104.
12. Vales-Alonso, J.; Bueno-Delgado, M.V.; Egea-Lopez, E.; Alcaraz-Epsin, J.J.; Garcia-Haro, J. Markovian Model for Computation of Tag Loss Ratio in Dynamic RFID Systems. In Proceedings of the 5th European Workshop on RFID Systems and Technologies, VDE, Bremen, Germany, 16–17 June 2009; pp. 1–8.
13. Gotfryd, M.; Pawlowicz, B. Modeling of a dynamic RFID system. In Proceedings of the 2013 IEEE Symposium on Computers and Communications (ISCC), Split, Croatia, 7–10 July 2013; pp. 747–752.
14. Liu, J.; Feng, Q. A blocking collision tracking tree algorithm in mobile RFID systems. In Proceedings of the 2017 Progress in Electromagnetics Research Symposium, St. Petersburg, Russia, 22–25 May 2017; pp. 22–25.
15. Zhang, L.; Xiang, W.; Tang, X. An efficient bit-detecting protocol for continuous tag recognition in mobile RFID systems. *IEEE Trans. Mob. Comput.* **2018**, *17*,503–516. [CrossRef]
16. EPCglobal. EPC^{TM} Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface Protocol for Communications at 860 MHz–960 MHz, Version 2.0.1 Ratified. 2015. Available online: http://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf (accessed on 1 April 2015).
17. Vales-Alonso, J.; Bueno-Delgado, V.; Egea-Lopez, E. Multi-frame maximum-likelihood tag estimation for RFID anticollision protocols. *IEEE Trans. Ind. Informatics* **2011**, *7*, 487–496. [CrossRef]
18. Myung, J.; Lee, W.; Shih, T.K. An Adaptive Memoryless Protocol for RFID Tag Collision Arbitration. *IEEE Trans. Multimed.* **2006**, *8*, 1096–1101. [CrossRef]
19. Myung, J.; Lee, W.; Srivastava, J.; Shih, T.K. Tag-Splitting: Adaptive Collision Arbitration Protocols for RFID Tag Identification. *IEEE Trans. Parallel Distrib. Syst.* **2007**, *18*, 763–775. [CrossRef]
20. Su, J.; Chen, Y.; Sheng, Z.; Huang, Z.; Liu, A.X. From M-ary query to bit query: A new strategy for efficient large-scale RFID identification. *IEEE Trans. Commun.* **2020**, *68*, 2381–2393. [CrossRef]
21. Liu, B.; Su, X. An anti-collision algorithm for RFID based on an array and encoding scheme. *Information* **2018**, *9*, 63. [CrossRef]
22. Hailemariam, Z.L.; Lai, Y.-C.; Jayadi, R.; Chen, Y.H. A knowledge-based query tree with shortcutting and couple-resolution for RFID tag identification. *Comput. Commun.* **2020**, *160*, 779–789. [CrossRef]
23. Saranga, V.; Devarapalli, M.R.; Radhakrishnan, S. A framework for fast RFID tag reading in static and mobile environments. *Comput. Netw.* **2008**, *52*, 1058–1073. [CrossRef]
24. Vales-Alonso, J.; Egea-Lopez, E.; Delgado, M.V.B. Analysis of tag lost ratio in dynamic RFID systems. *Int. J. Technol.* **2010**, *2*, 135–154.
25. Alcaraz, J.J.; Egea-Lopez, E.; Vales-Alonso, J.; Garcia-Haro, J. Dynamic system model for optimal configuration of mobile RFID systems. *Comput. Netw.* **2011**, *55*, 74–83. [CrossRef]
26. Alcaraz, J.J.; Vales-Alonso, J.; Garcia-Haro, J. RFID reader scheduling for reliable identification. *IEEE Trans. Autom. Sci. Eng.* **2013**, *10*, 816–827. [CrossRef]
27. Kang, L.; Qian, C.; Ni, L. RSAA: Reliable splitting aware ALOHA to capture passing tags. In Proceedings of the 2012 IEEE 9th International Conference on Mobile ad-hoc and Sensor Systems (MASS 2012), Las Vegas, NV, USA, 8–11 October 2012; pp. 38–46.

28. Zhu, W.; Cao, J.; Chan, H.C.B.; Liu, X.; Raychoudhury, V. Mobile RFID with a high identification rate. *IEEE Trans. Comput.* **2014**, *63*, 1778–1792. [CrossRef]
29. Jia, X.; Bolic, M.; Feng, Y.; Gu, Y. An efficient dynamic anti-collision protocol for mobile RFID tags identification. *IEEE Commun. Lett.* **2019**, *23*, 620–623. [CrossRef]
30. Yu, J.; Chen, L. From static to dynamic tag population estimation: An extended kalman filter perspective. In *Tag Counting and Monitoring in Large-Scale RFID Systems*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 43–75.
31. Lin, Q.; Yang, L.; Duan, C.; Liu, Y. Revisiting reading rate with mobility: Rate-adaptive reading of COTS RFID systems. *IEEE Trans. Mob. Comput.* **2019**, *18*, 1631–1646. [CrossRef]
32. Chen, Y.; Feng, Q. A Collision Avoidance Identification Algorithm for Mobile RFID Device. *IEEE Trans. Consum. Electron.* **2019**, *65*, 493–501.
33. Hush, D.; Wood, C. Analysis of tree algorithms for RFID arbitration. In Proceedings of the 1998 IEEE International Symposium on Information Theory, Cambridge, MA, USA , 16–21 August 1998; pp. 107–117.
34. Kaplan, M.A.; Golko, E. Analytic properties of multiple access trees. *IEEE Trans. Inf. Theory* **1985**, *31*, 255–263. [CrossRef]
35. Feller, W. *An Introduction to Probability Theory and Its Applications*, 3rd ed.; John Wiley: Hoboken, NJ, USA, 1968; Volume 1.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

applied sciences

Article

A Filter-Based and Parallel Unknown Tag Identification Protocol in Open RFID Systems

Xia Wang [1,2,*], Xianghong Tian [1], Shoubao Su [1], Ruijun Gu [1], Caiping Hu [1], Haiqiang Liu [1] and Jia Liu [2]

[1] The School of Computer Engineering, Jinling Institute of Technology, Nanjing 211100, China
[2] The State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China
* Correspondence: wangxia@jit.edu.cn

Abstract: Unknown tag identification plays a pivotal role in radio frequency identification (RFID) systems, but it has not been fully investigated. This paper proposes a filter-based and parallel unknown tag identification protocol (FPUI) for open RFID systems. The FPUI adopts an RSQF-based fingerprint filter to reconcile the collision slots and discriminate the known tags from unknown tags. Meanwhile, it collects the IDs of unknown tags in parallel. FPUI achieves high performance through the following three steps: (1) adopting the RSQF-based filter to build an indicator vector, thus improving the space efficiency; (2) building a fingerprint filter to discriminate known tags from unknown tags, thus reducing the false positive rate; (3) employing a parallel identification scheme to collect the IDs of unknown tags, thus improving identification efficiency. The identification time of our protocol was minimized by conducting a theoretical analysis of the relevant parameters. Furthermore, the performance of our protocol was evaluated by conducting a wide range of simulation experiments. The theoretical analysis and simulation results indicated that our protocol significantly outperformed the current advanced protocols.

Keywords: RFID system; unknown tag identification; RSQF-based fingerprint filter; parallel identification

Citation: Wang, X.; Tian, X.; Su, S.; Gu, R.; Hu, C.; Liu, H.; Liu, J. A Filter-Based and Parallel Unknown Tag Identification Protocol in Open RFID Systems. *Appl. Sci.* **2022**, *12*, 11349. https://doi.org/10.3390/app122211349

Academic Editor: Christos Bouras

Received: 6 October 2022
Accepted: 6 November 2022
Published: 8 November 2022

1. Introduction

Radio frequency identification (RFID) has a variety of applications in the Internet of Things, such as supply chain management [1–5], warehouse inventory [6–10], object monitoring and tracking [11–15], and posture recognition and localization [16–20]. In this broad range of RFID-enabled applications, unknown tag identification is crucial for collecting tag IDs from unexpected tags. For example, when a group of tagged objects is moved into a supermarket or warehouse such as Walmart, the manager needs to store these new tag IDs in the back-end database server for subsequent business operations such as daily inventory. In another example of a shopping mall, the customers often misplace frozen food with candy, causing the food to rot, or misplace oil near a lighter, causing great danger. The objective of unknown tag identification is to quickly identify newly added or misplaced tags from a large number of known tags. Considering a large-scale RFID system with millions of known tags whose IDs have already been stored in the back-end database previously, these known tags will participate in the identification of unknown tags, thus making it difficult to identify the unknown tags rapidly.

The existing unknown tag identification protocols are divided into two categories: probabilistic protocols [21–23] and deterministic protocols [24–28]. The probabilistic protocols can perform unknown tag detection quickly with an expected accuracy. The state-of-the-art probabilistic protocol is the *collision seeking detection* (CSD) protocol [23], which finds a collision seed to make many known tags collide in the last N slots with a frame size of f, thus saving the detection time and ensuring the desired detection accuracy. The deterministic protocol can correctly identify all unknown tags in a batch. Reference [25] proposed a series of protocols to improve identification performance. The *basic unknown tag identification protocol* (BUIP) separates known tags from unknown tags and deactivates them; the *single-pairing unknown tag identification protocol* (SUIP) adopts a slot pairing method, and the *multi-pairing unknown tag identification protocol* (MUIP) adopts multiple reselection methods to resolve the problem of known tag collisions. Meanwhile, the *filtering-based unknown tag identification protocol* (FUTI) and the *interactive filtering-based unknown tag identification protocol* (IFUTI) were investigated in [27] to separate unknown tags from known tags and assign a status code to each singleton slot, thus reducing known–unknown collisions and identifying unknown tags at the bit level. Although the existing protocols can identify unknown tags, they do not have enough time efficiency and space efficiency in open RFID systems.

This paper investigates the problem of unknown tag identification in open RFID systems and proposes a deterministic unknown tag identification protocol called the filter-based and parallel unknown tag identification (FPUI) protocol. Considering the drawbacks of the existing protocols, the proposed protocol formulates a solution that satisfies the requirements of efficiency and accuracy by: (1) taking less time and space to achieve unknown tag identification; (2) accurately collecting the information of unknown tags. To achieve these goals, the FPUI consists of two phases: the separation phase and the collection phase. In the first phase, the FPUI adopts an RSQF-based filter [29] to calculate the hash value for each known tag by $H(\cdot)$ and divides the hash value into two parts: *quotient* and *remainder*. The *remainders* of tags with an identical *quotient* are placed in consecutive slots from small to large, and this sequence of slots is called a *run*. Meanwhile, the fingerprint filter assigns different fingerprints to multiple known tags in the same *run* to reconcile the collision slots and separate the known tags from unknown tags. In the second phase, the FPUI collects the IDs of multiple tags by using a CDMA-based parallel identification method.

The main contributions of this paper are summarized as follows:

(1) A complete and robust solution to unknown tag identification in open RFID systems is provided.

(2) An RSQF-based fingerprint filter is utilized to solve the problem of slot collisions and separate the known tags from unknown tags, thus improving slot utilization and reducing the false positive rate.

(3) A parallel identification method is adopted to collect the IDs of multiple unknown tags with high efficiency.

(4) The performance of the proposed protocol is formally analyzed. The impact of various parameters on the identification time of our protocol is investigated, and the parameters are optimized to obtain the shortest identification time.

(5) Theoretical analysis and extensive simulations are conducted. The results indicate that our protocol performs better and has a lower false positive rate than the existing advanced protocols.

The rest of the paper is organized as follows. Section 2 introduces the related work. Section 3 formulates our problem. Section 4 proposes an efficient and complete unknown tag identification protocol called FPUI and theoretically analyzes its performance. Section 6 evaluates our protocol. Section 7 summarizes this paper.

2. Related Work

Many recent studies on RFID technology focus on functional applications, including information collection [30,31], cardinality estimation [32,33], tag grouping [34,35], searching a wanted tag set [36,37], and missing tag identification [38,39]. Unknown tag identification, as a research branch, is practically important because it helps identify the unknown tags that are misplaced or moved in the reader's interrogation area. To solve this problem, two categories of protocols have been designed: the probabilistic protocol [21–23] and the deterministic protocol [24–28].

The probabilistic protocol can identify unknown tags rapidly with an expected accuracy. Liu et al. designed an unknown tag detection scheme for detecting unknown tags with an expected confidence level [21]. Gong et al. proposed the *white paper* (WP) protocol [22], which constructs a composite message data structure consisting of all useful informative data from some independent detection synopses. This structure helps improve the unknown tag detection efficiency and decrease the failure probability. Although these probabilistic protocols can judge unknown tags in a fast way, they cannot identify the information of all unknown tags' IDs. Compared with the probabilistic protocol for unknown tag identification, the deterministic protocol can collect all information of unknown tags' IDs. For example, Sheng et al. firstly formulated the problem of unknown tag identification and presented an unknown tag identification protocol called *continuous scanning* (CU), which can collect a specified fraction of intact unknown tags [24]. However, CU only achieves incomplete unknown tag identification caused by randomized algorithms. Liu et al. proposed the BUIP, SUIP, and MUIP protocols [25], which adopt indicator vectors to distinguish known tags from unknown tags and deactivate the known tags. Although they can identify the intact unknown tag set with higher efficiency, more time is needed. Liu et al. proposed the FUTI and IFUTI protocols [27], which investigate the interactive filters to accelerate the process of unknown tag identification. Xie et al. proposed the unknown tag identification protocol based on a coded filtering vector [26], which utilizes the coded filtering vector technique to separate unknown tags from known tags and assign each singleton slot a status code to reduce known–unknown collisions, thus improving the identification performance. Zhu et al. proposed the *physical-layer unknown tag identification* (PUTI) protocol [28], which identifies the unknown tags by aggregating physical layer signals. Although these deterministic protocols can identify unknown tags, they are time-consuming and suffer from a high false positive rate.

This paper proposes a filter-based and parallel unknown tag identification protocol called FPUI. The FPUI thoroughly separates known tags from unknown tags and deactivates all known tags by adopting an RSQF-based fingerprint filter, thus improving the slot utilization and the accuracy of the protocol. Meanwhile, the FPUI adopts a parallel identification method to collect multiple unknown tag IDs in parallel, thus increasing the efficiency of the protocol.

3. System Model

3.1. Assumption and Problem

This paper considered an open RFID system consisting of one reader, N known tags, M unknown tags, and some missing tags. All these tags were within the interrogating range of this reader. The IDs of all known tags (including missing tags) were already stored in the back-end database of the server, but all IDs and M unknown tags were unavailable in the server. The known tag set is denoted as $\mathbb{K}$, i.e., $\mathbb{K} = \{t_1, t_2, \ldots, t_i, \ldots, t_N\}$, and the unknown tag set is denoted as $\mathbb{U}$, i.e., $\mathbb{U} = \{t_{u_1}, t_{u_2}, \ldots, t_{u_i}, \ldots, t_{u_M}\}$. The intersection of sets $\mathbb{K}$ and $\mathbb{U}$ is null, i.e., $\mathbb{K} \cap \mathbb{U} = \emptyset$. Each tag has a unique ID, and all tags are equipped with the identical hash generator $H(\cdot)$. The missing tag set is a part of the known tag set $\mathbb{K}$. Figure 1 presents an overview of an open RFID system with unknown tags and missing tags. There are a large number of known tags and numerous unknown tags in the interrogation of the reader. Table 1 shows the notations used in this paper. The objective of our protocol is to collect the information of the intact IDs of all unknown tags from the total tag set $\mathbb{K} \cup \mathbb{U}$ and eliminate the influence of false positives.

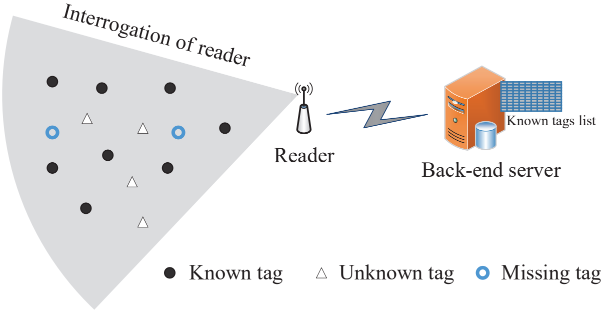


Figure 1. The system model of unknown tag identification.

Table 1. Notations.

Symbols	Descriptions
$\mathbb{K}$	A known tag set
$\mathbb{U}$	An unknown tag set
N	The number of known tags
M	The number of unknown tags
l_{fp}	The size of the fingerprint
F_R	A real frame in the collection phase
V_C	An address code vector
l_s	The size of the address code vector
m	The size of the address code
n	The number of missing tags
$H(\cdot)$	A hash function with a uniform random distribution

3.2. Communication Slots

The physical-layer RFID communication between the reader and the tags was based on slotted ALOHA. The reader starts a slotted frame, on the basis of which each tag randomly maps itself to one of the slots by a hash function. Thus, there are three categories of slots: (1) empty slot: selected by no tags; (2) singleton slot: selected by just one tag; (3) collision slot: selected by more than one tag. In this paper, singleton slots and collision slots are also called non-empty slots. By constructing the frame and handling the statuses of slots, the reader can accumulate the functional information of the expected tags for the practical application of RFID systems.

To distinguish an empty slot from non-empty slots, the tag needs to transmit only 1 bit of information, which needs t_s time in a slot. Meanwhile, it takes t_l time in a slot to transmit 10 bits of information for distinguishing the three types of slots. The time for transmitting one tag ID (96 bits) from the tag to the reader is denoted by t_{tag}. Generally, $t_{tag} > t_l > t_s$.

4. Filter-Based and Parallel Unknown Tag Identification Protocol

In this section, the filter-based and parallel unknown tag identification (FPUI) protocol is proposed, which can identify all unknown tags within the interrogation area efficiently and completely.

4.1. Basic Idea

Most of the existing unknown tag identification protocols are based on a slotted hash, and they have two drawbacks: large time consumption and low accuracy. Firstly, the existing protocols have lower slot utilization due to slot collisions. In this case, they need multiple rounds to deactivate all known tags, which is time-consuming. Secondly, a false positive occurs when an unknown tag and a known tag pick the same slot, resulting in this unknown tag being deactivated.

The idea of the FPUI is to identify unknown tags as quickly and precisely as possible by the following three design principles:

(1) *Improving slot utilization*: In the slotted-ALOHA-based protocol, multiple tags may choose a slot to respond to the reader, causing slot collisions and reducing slot utilization. This protocol modifies the RSQF filter to reconcile the collision slots to single slots, thus increasing the number of useful slots.

(2) *Eliminating false positives*: In real open RFID systems, unknown tags may select the same slot as known tags, which causes these unknown tags to be regarded as known tags and deactivated, i.e., a false positive problem. The key to tackling the problem is separating known tags from unknown tags thoroughly. In this paper, a unique fingerprint is provided for each known tag in a *run* to distinguish known tags from unknown tags, thus eliminating false positives.

(3) *Increasing the identification efficiency*: Traditional tag identification protocols adopt ALOHA-based or tree-based methods to collect the tag ID information serially, so the process is time-consuming. This paper proposes a parallel tag ID collection scheme to concurrently identify multiple unknown tags, thus increasing the identification efficiency.

To achieve the above goals, the FPUI identifies unknown tags in two phases: the separation phase and the collection phase. In the first phase, an RSQF-based fingerprint filter is built to separate known tags from unknown tags. In the second phase, the IDs of unknown tags are concurrently collected by assigning a series of orthogonal address codes to multiple singleton unknown tags, which is similar to CDMA technology.

4.2. Separation Phase

In this phase, the reader first builds an RSQF-based filter to increase the number of useful slots. Then, the reader constructs a fingerprint filter to separate known tags from unknown tags. The process of the separation phase is described in detail below.

4.2.1. Building an RSQF-Based Filter

The reader first calculates the hash value for each known tag by $H(id, r_1)$, where id is the tag's ID and r_1 is a random seed. The RSQF filter divides $H(id, r_1)$ into two parts: the first q-bit part is called *quotient*, denoted by $h_0(id)$, and the second r-bit part is called *remainder*, denoted by $h_1(id)$. In this paper, the original RSQF filter was modified to make it adapt to our problem. The modified RSQF-based filter maintains a vector $occupieds$ to determine whether a slot is occupied or not. A position j is occupied and is set to "1" when there is at least one tag t_i whose $h_0(id_i) = j$. The number of "1s" in the $occupied$ vector up to position j is counted as s_j, and the total number of "1s" in the $occupieds$ vector is counted as s. Furthermore, the RSQF-based filter maintains a vector Q in which there are N slots. Each slot with a size of r bits can store a *remainder*. The *remainders* of tags with an identical *quotient* are placed in consecutive slots from small to large. In this paper, this sequence of slots is called a *run*, and the number of tags in a *run* is called the *runsize*. When a tag t_i is inserted, the RSQF-based filter tries to store its *remainder* $h_1(id_i)$ in the *home slot* $Q[s_{h_0(id_i)}]$. Here, the linear probing scheme was adopted to store the *remainders* in the same *run*. As will be described below, the RSQF-based filter seeks out an unoccupied slot to save $h_1(id_i)$ when its *home slot* is already occupied.

A slot storing a *remainder* is called "used", and a slot storing no *remainder* is called "unused". Since the RSQF-based filter uses the linear probing scheme to store *remainders*, a slot may also be "used" even when its corresponding position in the $occupieds$ vector is not occupied. The RSQF-based filter always attempts to store the *remainders* in their *home slots* and only drifts a *remainder* when its *home slot* is occupied by another *remainder*. As shown in Figure 2, the RSQF-based filter maintains three vectors to determine whether a slot is "used" or not and the actual slot in which each *remainder* is stored. Specifically, the *occupieds* bit vector with a size of 2^q is used to indicate the *home slot* of each tag, the *runends* bit vector with a size of N is used to indicate the number of tags having the same *home slot*, and the *remainders* vector (namely Q array) is used to indicate the actual slot of each tag.

For the convenience of expression, two operations are defined for the RSQF-based filter: $SELECT(\cdot)$ and $RANK(\cdot)$. For a given bit vector D, $SELECT(D, i)$ returns the index of the ith 1 in D, and $RANK(D, i)$ returns the number of 1s preceding the ith position in D, i.e., $RANK(D, i) = \Sigma_{j=0}^{i-1} D[j]$. The two operations help seek out the *run* of any *quotient* $h_0(id)$. If $occupieds[h_0(id)] = 0$, there is no such *run*; otherwise, $RANK(occupieds, h_0(id))$ is applied to calculate the number s_j of slots $j \leq h_0(id)$, i.e., the number of *runs* preceding the slot $h_0(id)$, and then, $SELECT(runends, s_j + 1)$ is applied to calculate the end position of the s_jth *run*. As shown in Figure 2, the slot of tag t_i is in the $\{\lambda_i\}$th *run*, where $\lambda_i = s_{h_0(id_i)} = RANK(occupieds, h_0(id_i))$. The end slot of this *run* is $e_{\lambda_i} = SELECT(runends, \lambda_i + 1)$, and the beginning slot of this *run* is $b_{\lambda_i} = SELECT(runends, \lambda_i) + 1$ (we set $SELECT(runends, 0)$ to be -1). Thus, the size of this *run* can be obtained by $runsize_{\lambda_i} = e_{\lambda_i} - b_{\lambda_i} + 1$. The actual slot index of tag t_i falls between b_{λ_i} and e_{λ_i}. The tag t_i checks the jth position in the *remainders* vector ($b_{\lambda_i} \leq j \leq e_{\lambda_i}$). When $remainders[j] > h_1(id_i)$ and $remainders[j-1] \leq h_1(id_i)$, t_i is inserted $h_1(id_i)$ into the jth position.

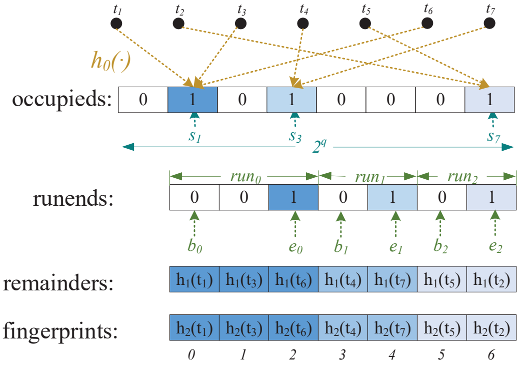


Figure 2. A simple RSQF-based fingerprint filter.

4.2.2. Building Fingerprint Filter

Although the RSQF-based filter can assign a slot to each known tag, it cannot solve the slot collision problem when multiple tags have the same *quotient* and *remainder*. Furthermore, it cannot separate known tags from unknown tags with the same *quotient* and *remainder* in open RFID systems. Therefore, this paper added a *fingerprints* vector to solve the above two problems. The reader generates a unique l_{fp}-bit fingerprint via a hash function $h_2(id, r_2)$ for every tag in the same *run*, where r_2 is another random seed. The reader inserts the fingerprint of each tag into the corresponding position of the *fingerprints* vector according to the *remainders* vector, as shown in Figure 2.

The reader broadcasts a request with parameters $\langle occupieds, runends, fingerprints, r_1, r_2 \rangle$ to all tags. After receiving the request, the tag t_i firstly calculates its occupieds index by $h_0(id_i)$ and obtains its *run* index λ_i. Then, it obtains the beginning position b_{λ_i} and the end position e_{λ_i} in the *fingerprints* vector. Subsequently, it calculates its fingerprint FP_i by $h_2(id_i, r_2)$ and checks $fingerprints[j]$ ($b_{\lambda_i} \leq j \leq e_{\lambda_i}$). If $FP_i = fingerprints[j]$, this tag regards itself as a known tag and deactivates itself. The flowchart of separation phase is shown in Figure 3. After this phase, all known tags are deactivated without participating in the collection phase.

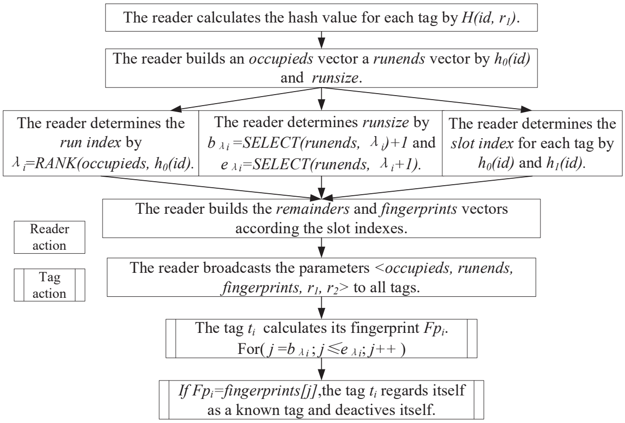

The reader calculates the hash value for each tag by H(id, r1).
The reader builds an occupieds vector a runends vector by h0(id) and runsize.
The reader determines the run index by λi=RANK(occupieds, h0(id).
The reader determines runsize by bλi =SELECT(runends, λi)+1 and eλi=SELECT(runends, λi+1).
The reader determines the slot index for each tag by h0(id) and h1(id).
The reader builds the remainders and fingerprints vectors according the slot indexes.
Reader action
Tag action
The reader broadcasts the parameters <occupieds, runends, fingerprints, r1, r2> to all tags.
The tag ti calculates its fingerprint Fpi. For(j =bλi ; j ≤eλi; j++)
If Fpi=fingerprints[j],the tag ti regards itself as a known tag and deactives itself.

Figure 3. The flowchart of separation phase.

4.3. Collection Phase

In this phase, our objective was to efficiently collect the IDs from all unknown tags. To save the collection time, the IDs were collected concurrently from multiple singleton unknown tags through a CDMA-based method, and each tag needs to determine its address code before transmitting its ID to the reader. The accomplishment of this goal involves four stages.

4.3.1. Building Real Frame

The real frame is constructed based on the responses of all unknown tags. In particular, the reader broadcasts a request with the parameter $\langle f, r_3 \rangle$ to issue the frame, where f is the size of the real frame and r_3 is a random seed. In this frame, each active unknown tag t_{u_i} randomly picks a slot by the hash function $H(id_{u_i}, r_3)\ mod\ f$ and sends a 1-bit response to the reader in this slot. The reader listens to the channel and records the status of each slot, i.e., empty and collision are recorded as "0" and singleton is recorded as "1". Then, the reader obtains the real frame that reflects the actual responses from the unknown tags, and the frame is denoted by F_R. F_R is also referred to as the indicator vector, and its length is f.

$$F_R[i] = \begin{cases} 0, & \text{the ith slot is an empty/collision slot,} \\ 1, & \text{the ith slot is a singleton slot.} \end{cases}$$

For example, as shown in Figure 4, there are 10 unknown tags $\{t_{u_1}, t_{u_2}, \ldots, tu_{10}\}$ and $f = 10$. The tags $\{t_{u_1}, t_{u_3}, t_{u_4}, t_{u_6}, t_{u_8}\}$ are mapped to the 1st, 3nd, 6th, 5th, and 10th singleton slots, respectively, and other tags are mapped to collision slots. Therefore, the real frame (also called the indicator vector) is denoted as "1010110001".

4.3.2. Building Address Code Vector

The reader generates a series of orthogonal address codes and builds the address code vector V_C with a length of l_s, where l_s is the number of "1s" in F_R. Here, the *Walsh* sequence is employed to provide address codes. The *Walsh* sequence of order m can provide m different orthogonal address codes, and each address code is m bits long, which guarantees that m singleton unknown tags can respond in parallel. Every m singleton slot belongs to a $loop$. The address codes of all tags are different and orthogonal within a $loop$. Therefore, V_C can be expressed as $\{ac_1, ac_2, \ldots, ac_m, ac_1, ac_2, \ldots ac_m, \ldots\}$, where ac_i is the address code of the tag t_{u_i}.

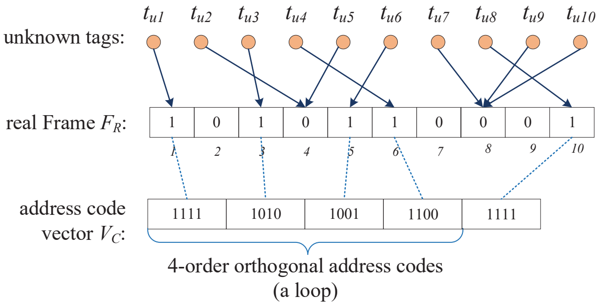

t_{u1} t_{u2} t_{u3} t_{u4} t_{u5} t_{u6} t_{u7} t_{u8} t_{u9} t_{u10}
unknown tags:
real Frame F_R:
1 0 1 0 1 1 0 0 0 1
1 2 3 4 5 6 7 8 9 10
address code vector V_C:
1111 1010 1001 1100 1111
4-order orthogonal address codes (a loop)

Figure 4. Building real frame and address code vector in the collection phase.

Taking Figure 4 as an example, the reader generates four orthogonal address codes and builds the address code vector V_C $\{1111, 1010, 1001, 1100, 1111\}$.

4.3.3. Assigning Address Code

The reader broadcasts the request with parameters $\langle F_R, V_C \rangle$ to all tags. Upon receiving the request, each singleton tag obtains its address code. Specifically, if the tag t_{u_i} is mapped to the jth slot and $F_R[j] = 1$, the address code of the tag is $V_C[\mu_i]$, where μ_i is the number of "1s" preceding the jth element in F_R. As shown in Figure 4, after receiving F_R and V_C, each tag checks its index and obtains its address code. For example, the indexes of $\{t_{u_1}, t_{u_3}, t_{u_4}, t_{u_6}, t_{u_8}\}$ are $\{1, 2, 4, 3, 5\}$, and the corresponding address codes are "1111", "1010", "1100", "1001", and "1111", respectively. So far, each singleton tag has an address code, which is different and orthogonal to the address codes of other singleton tags in its $loop$.

4.3.4. Collecting IDs in Parallel

The reader broadcasts the request to issue the frame. Every m unknown tag sends its ID to the reader in the same slot. For an arbitrary unknown tag t_{ui}, it adopts the following encoding scheme in place of *FM0* and *Miller*.: (i) The tag transmits the true code of $V_C[\mu_i]$ in the $\lceil \frac{\mu_i}{m} \rceil$th slot if a bit of its ID is "1".

(ii) The tag transmits the ones' complement code of $V_C[\mu_i]$ in the $\lceil \frac{\mu_i}{m} \rceil$th slot if a bit of its ID is "0".

Following the above rules, the number of real slots in the frame is $\lceil \frac{l_s}{m} \rceil$. Considering the address code "1010" of t_{ui}, the tag traverses each binary bit of its ID. In the ID, each "0" bit in the ID is encoded by "0101", and each "1" bit is encoded by "1010"; they are transmitted in the $\lceil \frac{\mu_i}{m} \rceil$th slot. Upon receiving the overlapping information, the reader isolates each ID of the tag by calculating normalized inner products of each m code and the address code of this tag. If the normalized inner product is "1", the bit received from this tag is "1"; if the normalized inner product is "-1", the bit received from this tag is "0"; otherwise, this tag did not send information.

Take Figure 5 for example. The tags $\{t_{u_1}, t_{u_3}, t_{u_4}, t_{u_6}\}$ concurrently transmit their IDs in the 1^{st} slot. The first two bits in the IDs of $\{t_{u_1}, t_{u_3}, t_{u_4}, t_{u_6}\}$ are $\{10, 11, 10, 00\}$. According to the rules (i) and (ii), the bits "1" and "0" are encoded by the true code and the one' -complement code of each tag's address code, respectively. Using "-1" to represent "0" and "+1" to represent "1", t_{u_1} transmits $\{(+1, +1, +1, +1), (-1, -1, -1, -1)\}$, t_{u_3} transmits $\{(+1, -1, +1, -1), (+1, -1, +1, -1)\}$, t_{u_4} transmits $\{(+1, +1, -1, -1), (-1, -1, +1, +1)\}$, and t_{u_6} transmits $\{(-1, +1, +1, -1), (-1, +1, +1, -1)\}$ in the first slot. Therefore, the reader receives the final overlapping information $\{(+2, +2, +2, -2), (-2, -2, +2, -2)\}$. The normalized inner product of the overlapping code and the address code determine whether a tag has sent data and what data to be sent. For example, the normalized inner product of $(+2, +2, +2, -2)$ and $(+1, +1, +1, +1)$ is "1", which indicates that the first bit t_{u_1} sent is "1"; the normalized inner product of $(-2, -2, +2, -2)$ and $(+1, +1, +1, +1)$ is

"-1", which indicates that the second bit t_{u_1} sent is "0". Consequently, the reader knows that the first two bits of t_{u_1}'s ID are "10". Similarly, the reader can obtain the IDs of the other three tags.

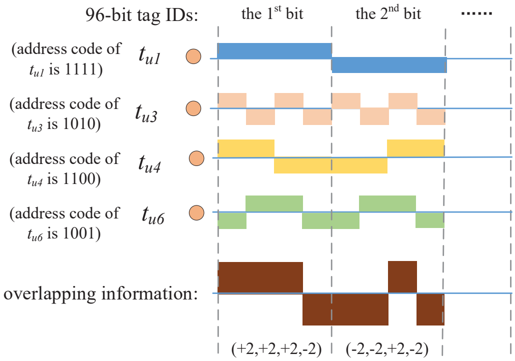

96-bit tag IDs:
the 1st bit
the 2nd bit
......
(address code of t_{u1} is 1111)
t_{u1}
(address code of t_{u3} is 1010)
t_{u3}
(address code of t_{u4} is 1100)
t_{u4}
(address code of t_{u6} is 1001)
t_{u6}
overlapping information:
(+2,+2,+2,-2)
(-2,-2,+2,-2)

Figure 5. Collecting IDs in parallel.

If $F_R[i] = 0$, the unknown tags picking this slot will participate in the next round. Then, the collection phase will be executed for several rounds until the reader cannot detect replies from unknown tags in the channel.

5. Performance Analysis

5.1. Fingerprint Size

First, the influence of fingerprint size l_{fp} is discussed. In our filter, each tag has a unique fingerprint in its *run*. To achieve a higher separation accuracy, different hash functions can be chosen for each *run* by transmitting multiple random seeds to tags. For saving the communication overhead, the fingerprint size was set to $\lceil log_2 runsize \rceil$ for each *run*. To simplify the calculation, l_{fp} is defined as the average fingerprint size, and it is discussed below. The probability p_u of a slot not being occupied in the *occupieds* vector is:

$$p_u = (1 - \frac{1}{2^q})^N = e^{-\rho_1}, \tag{1}$$

where ρ_1 is $\frac{N}{2^q}$. The number n_o of occupied slots in the *occupieds* vector is:

$$n_o = 2^q(1 - e^{-\rho_1}). \tag{2}$$

Therefore, the average *runsize* can be calculated as:

$$runsize_{average} = \frac{N}{n_o} = \frac{N}{2^q(1 - e^{-\rho_1})} = \frac{\rho_1}{(1 - e^{-\rho_1})}. \tag{3}$$

The average fingerprint is:

$$l_{fp} = \lceil log_2 runsize_{average} \rceil = \lceil log_2 \frac{\rho_1}{(1 - e^{-\rho_1})} \rceil. \tag{4}$$

5.2. Address Code Size

Next, the influence of the address code size m on the execution time is discussed. The CDMA-based scheme has high noise resistance and application adaptability. This paper chose the *Walsh* codes as the address codes of unknown tags, which can provide perfect orthogonal codes for concurrently identifying multiple unknown tags. However, the quality of communication may decrease when the address code size is large. Therefore, the *Walsh* codes with an order of 4∼64 were adopted to guarantee the communication quality, which indicates that $4 \leq m \leq 64$.

According to the characteristics of the *CDMA* code, there are $\frac{m}{2}$ sub-carrier cycles per symbol after modulation, so the data rate is $2BLF/m$, which indicates that the data rate is in an inverse proportion to m. That is, the performance of the protocol will decrease as m increases. Letting t_{tag} be the time for transmitting a 96-bit ID from the tag to the reader based on the *FM0* code, we have $t'_{tag} = \frac{mt_{tag}}{2}$. In our protocol, $m = 4$.

5.3. Time Efficiency

In this section, the time efficiency of the FPUI protocol is analyzed. The execution time comprises two parts: the separation time and the collection time. The total execution time is given as:

$$T_t = T_{sep} + T_{col}, \tag{5}$$

where T_{sep} is the separation time and T_{col} is the collection time. The separation time T_{sep} is represented as:

$$\begin{aligned} T_{sep} &= \frac{2^q + N\times(l_{fp}+1)}{96} \times t_{id} \\ &= (2^q + (l_{fp}+1)N)\frac{t_{id}}{96}, \end{aligned} \tag{6}$$

where t_{id} is the time for transmitting 96-bit information from the reader to the tags, q is the size of *quotient*, N is the number of known tags, and l_{fp} is the average length of the fingerprint. The number η of bits per tag is defined as:

$$\begin{aligned} \eta &= \frac{2^q}{N} + (l_{fp}+1) \\ &= \frac{1}{\rho_1} + \lceil log_2 \frac{\rho_1}{(1-e^{-\rho_1})} \rceil + 1. \end{aligned} \tag{7}$$

η is minimized to obtain the optimal space efficiency. Then, the optimal parameter ρ_1 for minimizing η is investigated. The derivative of η can be given as follows:

$$\frac{\partial \eta}{\partial \rho_1} = -\frac{1}{\rho_1^2} + \frac{1}{\rho_1 ln2} - \frac{e^{-\rho_1}}{(1-e^{-\rho_1})ln2}. \tag{8}$$

By setting the derivatives in Equation (8) to 0, the lowest space efficiency is obtained when ρ_1 is 1.3. Then, the reader takes 1.93 bits to deactivate one known tag and the average fingerprint $l_{fp} = 2$. Figure 6a shows the changes of unit execution time δ with respect to ρ. Therefore, the minimum separation time is:

$$T_{sep}^{min} = \frac{1.93t_{id}}{96}N\text{ms} = 0.02Nt_{id}\text{ms}. \tag{9}$$

Then, the collection time T_{col} is discussed. Considering the ith round of *unknown tag IDs' collection*, the collection time, denoted by T_{col}^i, is expressed as follows:

$$T_{col}^i = M_i \times t_s + \frac{f_i + l_s^i \times m}{96} \times t_{id} + \lceil \frac{l_s^i}{m} \rceil \times t'_{tag}, \tag{10}$$

where M_i, f_i, and l_s^i are the number of participating unknown tags, the frame size, and the number of singleton slots in the ith round, respectively; t_s is the time for the tag transmitting 1 bit of information to the reader; t'_{tag} is the time for transmitting a 96-bit ID from the tag to the reader. Note that t_{id} and t_s were based on the traditional *FM0* code, and t'_{tag} was based on the *CDMA* code. The probability of mapping one unknown tag to a singleton slot in this round is denoted as P_s^i, which is given as follows:

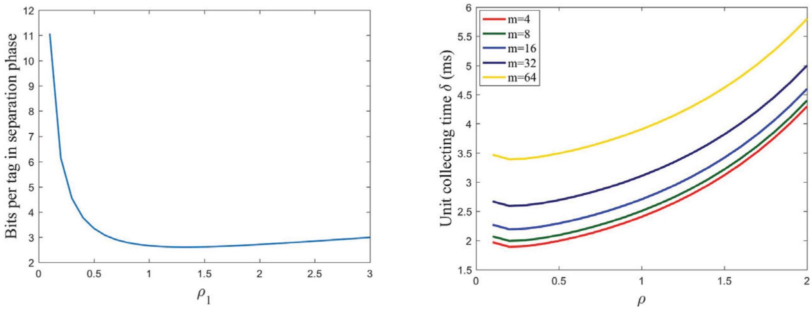
$$\begin{aligned} P_s^i &= M_i \times \frac{1}{f_i} \times (1 - \frac{1}{f_i})^{M_i - 1} \\ &= \rho e^{-\rho}, \end{aligned} \tag{11}$$

where $\rho = \frac{M_i}{f_i}$. Therefore, $l_s^i = f_i \times \rho e^{-\rho}$. This paper defines the unit collection time δ as the ratio of the collection time to the number of identified tags in the ith round. Therefore, we have:

$$\begin{aligned} \delta &= \frac{M_i \times t_s + \frac{f_i + f_i \rho e^{-\rho} m}{96} \times t_{id} + \lceil \frac{f_i \times \rho e^{-\rho}}{m} \rceil \times t'_{tag}}{f_i \rho e^{-\rho}} \\ &\approx e^{\rho} t_s + (\frac{e^{\rho}}{\rho} + m)\frac{t_{id}}{96} + \frac{t'_{tag}}{m}. \end{aligned} \tag{12}$$

Here, δ needs to be minimized to achieve the shortest collection time. Next, the optimal parameter ρ is found to minimize δ. The derivative of δ is calculated as follows:

$$\frac{\partial \delta}{\partial \rho} = e^{\rho} t_s + \frac{e^{\rho}(\rho - 1)}{\rho^2} \frac{t_{id}}{96}. \tag{13}$$



(**a**) (**b**)

Figure 6. The Optimal parameter settings for the separation time and collection time. (**a**) The unit space usage η with respect to ρ_1. (**b**) The unit collection time δ with respect to ρ.

Based on the Philips I-Code system [20] and the *CDMA* code, we have $t_{id} = 2.4$ ms, $t_{tag} = 2.3$ ms, $t_l = 0.8$ ms, and $t_s = 0.4$ ms. By setting the derivative in Equation (13) to 0, the minimum unit collection time is obtained when ρ is 0.22. That is, the minimum execution time is taken to collect the IDs of all unknown tags when $f = 4.5M$. Figure 6b shows the changes of unit execution time δ with respect to ρ. As a result, the optimal collection time T_{col}^{op} can be given as follows:

$$\begin{aligned} T_{col}^{op} &= (0.51 + 0.03m + \frac{t'_{tag}}{m})M(\text{ms}) \\ &= (0.51 + 0.03m + \frac{t_{tag}}{2})M(\text{ms}) \\ &= (1.66 + 0.03m)M(\text{ms}). \end{aligned} \tag{14}$$

Substituting $t_{id} = 2.4$ ms into (9), the optimal separation time can be given as follows:

$$T_{sep}^{min} = 0.02Nt_{id}\text{ms} = 0.048N\text{ms}. \tag{15}$$

By substituting (14) and (15) into (5), the total execution time is $1.66M + 0.03mM + 0.048N$ ms.

5.4. Discussion on False Positive Rate

As shown in [29], the original RSQF filter takes $\frac{2.125+log_2 1/\zeta}{\alpha}$ bits to count one element, where α is the load factor and ζ is the false positive rate. When the false positive rate is smaller than 1/64, the RSQF filter has better space efficiency than other classic filters, including the Bloom filter, the Cuckoo filter, and the original QF filter. The RSQF filter maintains a load factor of up to 0.95, and our filter has the same load factor as the original RSQF filter. Meanwhile, in the RSQF filter, multiple tags in a *run* may have the same *remainder*; in our filter, due to the tags in a *run* having different fingerprints, our filter has a better false positive rate than the original RSQF filter.

6. Evaluation

This section evaluates the performance of our protocol and the existing CU [24], BUIP and MUIP [25], and FUTI and IFUTI protocols [27]. Also, the execution time of our protocol is compared with that of state-of-the-art unknown identification protocols.

6.1. Simulation Setting

Our protocol was implemented in Matlab and run on a ThinkPad X1 Carbon desktop computer equipped with an Intel 2.40 GHz CPU. In the simulations, there was a 302 μs interval between each pair of consecutive communications from the tag to the reader and from the reader to the tags. The transmission rates in different directions were not symmetric depending on specific physical implementations and practical environments. According to the specification of the Philips I-Code system [20] and the *CDMA* code, we have $t_{id} = 2.4$ ms, $t_{tag} = 2.3$ ms, $t_l = 0.8$ ms, $t_s = 0.4$ ms, and $t'_{tag} = 1.15m$ ms. Our simulations were executed 100 times in Matlab, and the results were averaged.

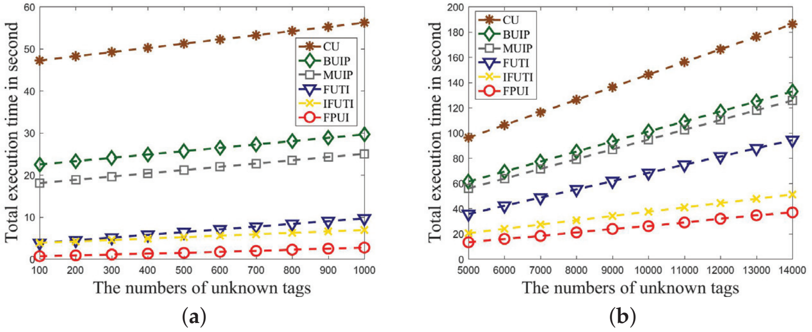
6.2. Total Execution Time

In this section, the total execution time of our protocol is analyzed and the proposed FPUI protocol is compared with some state-of-the-art protocols, including CU, BUIP and MUIP, and FUTI and IFUTI. In different applications, the number of unknown tags also varies. Therefore, in the following simulation experiments, the number N of known tags was fixed to 10,000 and the number M of unknown tags was changed in different applications. To thoroughly evaluate the performance of our protocol, two sets of simulations were conducted under two application scenarios: the scenario of low-density unknown tags and the scenario of high-density unknown tags. Furthermore, a set of simulations was conducted to evaluate the impact of the size m of the address code on the execution time.

Low-density unknown tags scenario: In this scenario, a simulation was conducted for an RFID system under low-density unknown tags. Here, the number M of unknown tags varied from 100 to 1000 with a step of 100. As shown in Figure 7a, the simulation results demonstrated that our FPUI protocol outperformed the advanced protocols in [25,27]. Specifically, the took takes 5.6 s and MUIP 18.8 s to identify 200 unknown tags, respectively. By contrast, our proposed PFUI protocol just took 0.86 s to identify 200 unknown tags, showing 84.6% and 95.4% less execution time than the IFUTI and MUIP protocols, respectively.

High-density unknown tags scenario: In this scenario, a simulation was conducted for an RFID system under high-density unknown tags. Here, the number M of unknown tags varied from 5000 to 14,000 with a step of 1000. As shown in Figure 7b, the simulation results demonstrated that our FPUI protocol also performed better than the existing protocols in [25,27]. Concretely, the IFUTI protocol took 42.7 s and the MUIP protocol 107.9 s to identify 12,000 unknown tags, respectively. By contrast, our proposed FPUI protocol only took 31.9 to identify 12,000 unknown tags, showing 25.3% and 70.4% less execution time than the IFUTI and MUIP protocols, respectively.

The simulation results in Table 2 also show that our FPUI protocol was more efficient under the RFID scenario with low-density unknown tags and high-density unknown tags.



(**a**) (**b**)

Figure 7. Evaluating the execution time of different unknown identification protocols, where the number N of known tags is fixed to 10,000. (**a**) Low density of unknown tags. (**b**) High density of unknown tags.

Table 2. Total execution time of the protocols, where N is fixed to 10,000.

Alg. Name	CU	BUIP	MUIP	FUTI	IFUTI	FUTI
$M = 100$	46.3	22.7	17.6	4.2	3.9	0.71
$M = 500$	50.2	25.7	21.4	6.4	4.9	1.4
$M = 1000$	55.7	29.3	24.6	9.3	6.8	2.8
$M = 5000$	95.2	61.8	55.9	35.7	21.2	13.3
M = 10,000	152.7	106.3	98.7	72.8	39.5	28.2

6.3. Impact of Address Code Variation

In this group of simulation experiments, the execution time of our protocol in an RFID system with different m values was evaluated. The size m of the address code was varied from 4 to 64 with a step of 2x. Meanwhile, The number M of unknown tags was changed from 1000 to 10,000 to observe the impact of m on the total execution time. As seen in Figure 8, the simulation results demonstrated that our FPUI protocol achieved the best performance when $m = 4$. This is because, as m increased, the data rate decreased and the reader needed to transmit more information to the tags for their address codes. This analysis was consistent with that presented in Section 5.2.

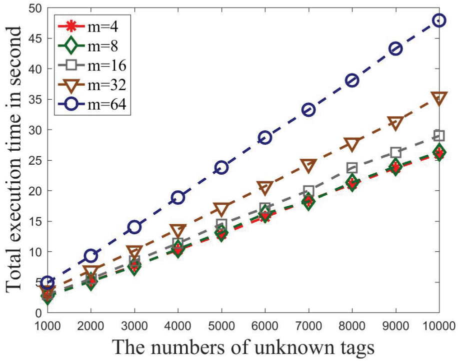


Figure 8. The execution time with respect to m.

6.4. Impact of Missing Tags

Since our protocol assigns a unique fingerprint to each known tag, all known tags can be deactivated to remove false positives. Then, a set of simulations was conducted to evaluate the impact of the number n of missing tags on the deactivating accuracy. As shown in Figure 9, our protocol always deactivated all known tags regardless of the number n of missing tags, which indicates that our protocol can achieve better performance in real open RFID systems than other existing works.

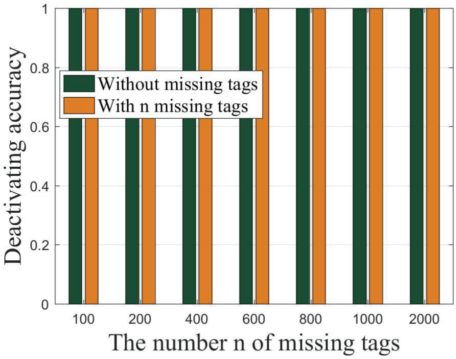


Figure 9. The deactivating accuracy with respect to n.

7. Conclusions

This paper investigated the problem of unknown tag identification in open RFID systems and proposed a filter-based parallel unknown tag identification protocol (FPUI), which can address the unknown tag identification problem completely and efficiently. FPUI first separates known tags from unknown tags by constructing an RSQF-based fingerprint filter, deactivating all known tags and eliminating false positives. Then, it effectively identifies unknown tags by using a CDMA-based parallel identification scheme. A theoretical analysis was conducted to optimize the parameters for minimizing the total execution time. Meanwhile, many simulation experiments were carried out to evaluate the performance of the proposed protocol. The simulation results indicated that the proposed protocol comparatively outperformed the existing advanced protocols.

Author Contributions: Investigation, H.L. and J.L.; Methodology, R.G. and C.H.; Project administration, X.T., S.S. and J.L.; Writing—original draft, X.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was financially supported by the National Natural Science Foundation of China (Nos. 61702257, 61272418), the Open Foundation of State Key Laboratory for Novel Software Technology for Nanjing University (No. KFKT2021B15), the Jinling Institute of Technology High Level Talents Research Foundation (No. jit-b-202118), and the Major Project of Natural Science Foundation of the Jiangsu Higher Education Institutions of China (No. 18KJA520003, 21KJA120001).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Liu, X.; Yin, J.; Zhang, S.; Xiao, B.; Ou, B. Time-Efficient Target Tags Information Collection in Large-Scale RFID Systems. *IEEE Trans. Mob. Comput.* **2020**, *20*, 2891–2905. [CrossRef]
2. Gaukler, G.M. Item-Level RFID in a Retail Supply Chain with Stock-Out-Based Substitution. *IEEE Trans. Ind. Inform.* **2011**, *7*, 362–370. [CrossRef]
3. Choi, T.M. Coordination and Risk Analysis of VMI Supply Chains with RFID Technology. *IEEE Trans. Ind. Inform.* **2011**, *7*, 497–504. [CrossRef]
4. Xiao, Q.; Zhang, Y.; Chen, S.; Chen, M.; Liu, J. Estimating Cardinality of Arbitrary Expression of Multiple Tag Sets in a Distributed RFID System. *IEEE/ACM Trans. Netw.* **2019**, *27*, 748–762. [CrossRef]
5. Yu, J.; Zhang, P.; Chen, L.; Liu, J.; Zhang, R.; Wang, K.; An, J. Stabilizing Frame Slotted Aloha Based IoT Systems: A Geometric Ergodicity Perspective. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 714–725. [CrossRef]
6. Fyhn, K.; Jacobsen, R.M.; Popovski, P.; Larsen, T. Fast Capture-Recapture Approach for Mitigating the Problem of Missing RFID Tags. *IEEE Trans. Mob. Comput.* **2012**, *11*, 518–528. [CrossRef]
7. Simon, M.; Divsalar, D. Some interesting observations for certain line codes with application to RFID. *IEEE Trans. Commun.* **2006**, *54*, 583–586. [CrossRef]
8. Yang, L.; Lin, Q.; Duan, C.; An, Z. Analog On-Tag Hashing: Towards Selective Reading as Hash Primitives in Gen2 RFID Systems. In Proceedings of the ACM MobiCom, Snowbird, UT, USA, 16–20 October 2017; pp. 301–314.
9. Yu, J.; Liu, J.; Zhang, R.; Chen, L.; Gong, W.; Zhang, S. Multi-Seed Group Labeling in RFID Systems. *IEEE Trans. Mob. Comput.* **2020**, *19*, 2850–2862. [CrossRef]
10. Shahzad, M.; Liu, A.X. Probabilistic Optimal Tree Hopping for RFID Identification. *IEEE/ACM Trans. Netw.* **2015**, *23*, 796–809. [CrossRef]
11. Ding, H.; Qian, C.; Han, J.; Xiao, J.; Zhang, X.; Wang, G.; Xi, W.; Zhao, J. Close-proximity Detection for Hand Approaching using Backscatter Communication. *IEEE Trans. Mob. Comput.* **2019**, *18*, 2285–2297. [CrossRef]
12. Shangguan, L.; Zhouy, Z.; Zheng, X.; Yang, L.; Liu, Y.; Han, J. ShopMiner: Mining Customer Shopping Behavior in Physical Clothing Stores with COTS RFID Devices. In Proceedings of the ACM SenSys, Seoul, Korea, 1–4 November 2015; pp. 113–126.
13. Choi, J.; Lee, I.; Du, D.Z.; Lee, W. FTTP: A Fast Tree Traversal Protocol for Efficient Tag Identification in RFID Networks. *IEEE Commun. Lett.* **2010**, *14*, 713–715. [CrossRef]
14. Shi, X.; Cai, H.; Wang, M.; Wang, G.; Huang, B.; Xie, J.; Qian, C. TagAttention: Mobile Object Tracing with Zero Appearance Knowledge by Vision-RFID Fusion. *IEEE/ACM Trans. Netw.* **2021**, *29*, 890–903. [CrossRef]
15. Motroni, A.; Buffi, A.; Nepa, P.; Tellini, B. Sensor-Fusion and Tracking Method for Indoor Vehicles with Low-Density UHF-RFID Tags. *IEEE Trans. Instrum. Meas.* **2020**, *70*, 1–14. [CrossRef]
16. Yang, L.; Chen, Y.; Li, X.Y.; Xiao, C.; Li, M.; Liu, Y. Tagoram: Real-Time tracking of mobile RFID tags to high precision using COTS devices. In Proceedings of the ACM MobiCom, Maui, HI, USA, 7–11 September 2014; pp. 237–248.
17. Benes, F.; Stasa, P.; Svub, J.; Alfian, G.; Kang, Y.-S.; Rhee, J.-T. Investigation of UHF Signal Strength Propagation at Warehouse Management Applications Based on Drones and RFID Technology Utilization. *Appl. Sci.* **2022**, *12*, 1277. [CrossRef]
18. Liu, J.; Chen, X.; Chen, S.; Liu, X.; Wang, Y.; Chen, L. TagSheet: Sleeping Posture Recognition with Unobtrusive Passive Tag Matrix. In Proceedings of the IEEE INFOCOM, Paris, France, 29 April–2 May 2019; pp. 874–882.
19. Stefaniak, P.; Jachnik, B.; Koperska, W.; Skoczylas, A. Localization of LHD Machines in Underground Conditions Using IMU Sensors and DTW Algorithm. *Appl. Sci.* **2021**, *11*, 6751. [CrossRef]
20. Liu, J.; Chen, S.; Chen, M.; Xiao, Q.; Chen, L. Pose Sensing with a Single RFID Tag. *IEEE/ACM Trans. Netw.* **2020**, *28*, 2023–2036. [CrossRef]
21. Liu, X.; Qi, H.; Li, K.; Stojmenovic, I.; Liu, A.X.; Shen, Y.; Qu, W.; Xue, W. Sampling Bloom Filter-Based Detection of Unknown RFID Tags. *IEEE Trans. Commun.* **2015**, *63*, 1432–1442. [CrossRef]
22. Gong, W.; Liu, J.; Yang, Z. Efficient Unknown Tag Detection in Large-Scale RFID Systems with Unreliable Channels. *IEEE/ACM Trans. Netw.* **2017**, *25*, 2528–2539. [CrossRef]
23. Liu, X.; Chen, S.; Liu, J.; Qu, W.; Xiao, F. Fast and Accurate Detection of Unknown Tags for RFID Systems? Hash Collisions are Desirable. *IEEE/ACM Trans. Netw.* **2020**, *28*, 126–139. [CrossRef]
24. Sheng, B.; Li, Q.; Mao, W. Efficient continuous scanning in RFID systems. In Proceedings of the IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
25. Liu, X.; Xiao, B.; Zhang, S.; Bu, K. Unknown Tag Identification in Large RFID Systems: An Efficient and Complete Solution. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 1775–1788. [CrossRef]
26. Xie, X.; Li, K.; Liu, X. An Unknown Tag Identification Protocol Based on Coded Filtering Vector in Large Scale RFID Systems. In Proceedings of the IEEE ICCCN, Shanghai, China, 4–7 August 2014; pp. 1–9.
27. Liu, X.; Li, K.; Min, G.; Lin, K.; Xiao, B.; Shen, Y.; Qu, W. Efficient Unknown Tag Identification Protocols in Large-Scale RFID Systems. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 3145–3155. [CrossRef]
28. Zhu, F.; Xiao, B.; Liu, J.; Chen, L. Efficient Physical-Layer Unknown Tag Identification in Large-scale RFID Systems. *IEEE Trans. Commun.* **2017**, *65*, 283–295. [CrossRef]
29. Pandey, P.; Bender, M.A.; Johnson, R.; Patro, R. A General-Purpose Counting Filter: Making Every Bit Count. In Proceedings of the ACM SIGMOD 2017, Chicago, IL, USA, 14–19 May 2017; pp. 775–787.

30. Buffi, A.; Michel, A.; Nepa, P.; Tellini, B. RSSI Measurements for RFID Tag Classification in Smart Storage Systems. *IEEE Trans. Instrum. Meas.* **2018**, *67*, 894–904. [CrossRef]
31. Liu, J.; Chen, S.; Xiao, Q.; Chen, M.; Xiao, B.; Chen, L. Efficient Information Sampling in Multi-Category RFID Systems. *IEEE/ACM Trans. Netw.* **2019**, *27*, 159–172. [CrossRef]
32. Arjona, L.; Landaluce, H.; Perallos, A.; Onieva, E. Scalable RFID Tag Estimator with Enhanced Accuracy and Low Estimation Time. *IEEE Signal Process. Lett.* **2017**, *24*, 982–986. [CrossRef]
33. Liu, X.; Li, K.; Liu, A.X.; Guo, S.; Shahzad, M.; Wang, A.L.; Wu, J. Multi-Category RFID Estimation. *IEEE/ACM Trans. Netw.* **2017**, *25*, 264–277. [CrossRef]
34. Liu, J.; Chen, M.; Xiao, B.; IEEE, F.Z.; Chen, S.; Chen, L. Efficient RFID Grouping Protocols. *IEEE/ACM Trans. Netw.* **2016**, *24*, 3177–3190. [CrossRef]
35. Wang, X.; Liu, J.; Wang, Y.; Chen, X.; Chen, L. Efficient Tag Grouping via Collision Reconciliation and Data Compression. *IEEE Trans. Mob. Comput.* **2020**, *20*, 1817–1831. [CrossRef]
36. Vizziello, A.; Savazzi, P. Efficient RFID Tag Identification Exploiting Hybrid UHF-UWB Tags and Compressive Sensing. *IEEE Sens. J.* **2016**, *16*, 4932–4939. [CrossRef]
37. Chen, M.; Luo, W.; Mo, Z.; Chen, S.; Fang, Y. An Efficient Tag Search Protocol in Large-Scale RFID Systems with Noisy Channel. *IEEE/ACM Trans. Netw.* **2016**, *24*, 703–716. [CrossRef]
38. Wang, X.; Liu, J.; Wang, Y.; Chen, X.; Chen, L. Efficient missing tag identification in blocker-enabled RFID systems. *Comput. Netw.* **2019**, *164*, 106894. [CrossRef]
39. Su, J.; Sheng, Z.; Liu, A.X.; Fu, Z.; Huang, C. An efficient missing tag identification approach in RFID collisions. *IEEE Trans. Mob. Comput.* **2021**. [CrossRef]

MDPI AG
Grosspeteranlage 5
4052 Basel
Switzerland
Tel.: +41 61 683 77 34

Applied Sciences Editorial Office
E-mail: applsci@mdpi.com
www.mdpi.com/journal/applsci

Disclaimer/Publisher's Note: The title and front matter of this reprint are at the discretion of the Guest Editor. The publisher is not responsible for their content or any associated concerns. The statements, opinions and data contained in all individual articles are solely those of the individual Editor and contributors and not of MDPI. MDPI disclaims responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

MDPI

Academic Open
Access Publishing

mdpi.com

ISBN 978-3-7258-2312-3