electronics

MDPI

Article

An Anonymous Mutual Authentication Scheme for RFID-Based Transportation System

Sai Ji [1,2], Shuai Liu [1], Chen Wang [1], Rongxin Qi [1] and Jian Shen [1,3,*]

[1] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 211800, China; jisai@nuist.edu.cn (S.J.); shuailiu2019@126.com (S.L.); wangchennuist@126.com (C.W.); q_qirongxin@126.com (R.Q.)
[2] School of Information Engineering, Suqian College, Suqian 223800, China
[3] Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 518000, China
* Correspondence: shenjian@nuist.edu.cn or s_shenjian@126.com

Received: 29 September 2020; Accepted: 7 December 2020; Published: 17 December 2020

Abstract: In traditional transportation, each driver usually relies on their experience to determine an appropriate route, which may shorten the driving time and transport cost. However, this may also lead to a waste of time in traffic jams or due to other problems. In recent years, by introducing Internet of Things technology into the transportation system, traffic condition data can be collected and analyzed in real-time, which makes it easier for drivers to choose appropriate routes. However, the transmitted data may be intercepted or falsified, especially in untrusted public communication channels. Some schemes have been proposed to protect personal data, while they are vulnerable to some known attacks. Therefore, we propose a mutual authentication scheme for session key agreement and information encryption before transmitting personal data. This scheme can correctly identify vehicles and information. The Burrows–Abadi–Needham logic proof and our security discussion demonstrate that this authentication scheme can resist the various known attacks, including de-synchronization, the replay attack and the reader lost attack, which is solved for the first time in this field. Compared with some typical schemes, the performance analysis shows that this new scheme realizes a balance between security and computing costs.

Keywords: anonymous; RFID; authentication; WSN; vehicle

1. Introduction

With wireless network and sensing technology applied to people's daily routine, various convenient and smart services for people have been developed. For example, by assembling or attaching sensors to household appliances, wearable devices and vehicles [1], the running statuses of items can easily be sensed and controlled without geographical limitations when a user utilizes a phone or tablet to send commands. In vehicle transportation management particularly, this technology plays a very meaningful role for drivers and administrators when they need reliable reports to acquire current vehicle and road conditions in real time and determine the proper traffic route. The occasional traffic event, such as a road accident or road maintenance, may affect some routines and the successive transportation service. Thus, different schemes have been designed to collect and share information about vehicles and roads. These are known as vehicular ad hoc networks (VANETs), which consist of vehicle-to-vehicle communication and vehicle-to-roadside-unit (RSU) infrastructure communication [2]. However, attackers may eavesdrop or falsify communicated messages that are unencrypted or transmitted to a receiver via an unprotected wireless channel. These attacks may result in personal data disclosure and unexpected errors or losses. In one particular scenario, an attacker tries to falsify transactor data for eluding barrier tolls, which may result in the loss of the administrator's

income. Such a security problem may reduce public interest in this technology and become an obstacle to developing wireless sensor networks for vehicles. Therefore, these security issues cannot be ignored and a practical protective mechanism is required.

Among many Internet of Things (IoT) sensing technologies, radio frequency identification (RFID) is an essential and low-cost technology. An RFID system can easily identify different tags in a range of one meter to tens of meters without close contact or sight restrictions, which is superior to an optical identification system [3]. In addition, tags have the advantage of computing and encrypting data securely. Due to these advantages, RFID technology has been applied to many areas, such as in telecare medicine information systems (TMIS) [4,5], geographical localization services [6], and supply-chain inventory management [7,8]. These RFID-based applications mainly contain three types of entities: tag, reader and server. RFID tags are usually placed on objects and store necessary confidential information about identification. The reader is an intermediary applied to communicate with tags and the server. The server collects much information about tags and readers' communications. There is a consensus that the local server must be trusted and will not leak any confidential data [9]. In an RFID system, a reader might connect to the server through a wired or wireless channel. The wired connection is considered secure, but the fixed line limits mobility. Thus, wireless portable readers have become popular in many mobile scenarios. Nevertheless, portable readers are easily lost or stolen when they are deployed on an unmanned site. Previous studies have seldom considered the problem of losing a reader. Thus, they have not considered precautionary methods to validate whether the reader works in the anticipated site. In such a case, a criminal may corrupt and imitate that reader to participate in communications with honest third parties, which leads to data leakage and loss. In addition, when certain tags' information is obtained by a given reader, these tags cannot be recognized by other readers. This is because the reader has to use the last session key, which has only been shared with each requested tag in the historic literature [4,6,9,10].

In VANETs, through employing sensors and communication units, vehicles can build temporary networks to transmit the latest conditions about traffic. Based on the received information, the transportation driver or administrator is able to adjust the traveling schedule in the case of traffic jams or accidents. In addition, these traffic conditions are useful for official roadside management (such as dispersing or limiting vehicle flow) and assistance (such as road repair). However, these traffic conditions are not reliable because the driver is not aware of incorrect or faked messages. In addition, the types of messages shared may cause concern about personal identity data and traveling trace leakage, which are adverse to developing VANETs. Thus, the personal data relating to a vehicle needs to be protected. There are some emergency vehicles, such as ambulances and fire engines, which usually use reserved lanes and transportation networks. To obtain enough traffic information, special vehicles need to access both the public and private VANETs. Because a fast-moving emergency vehicle does not have much time to obtain data, identity recognition should be efficient and lightweight [11].

Motivation of this paper: Considering all the aforementioned issues and the advantages of an RFID system, in our study we utilize this technology to protect a vehicle's privacy. In order to ensure that the shared traffic information is reliable, we propose an RFID-based scheme to verify traffic information from vehicles anonymously and resist the usual forms of attack.

Our contributions:

- **A new retrieval method is adopted by the server.** For solving the aforementioned privacy problem, we design a new retrieval method to assist the server in searching for the authenticated information, which initially allows multiple readers to identify different tags at the same time. Based on this retrieval method, we can predefine the scope of the tags that each reader recognizes, which is also a method to protect data privacy. That is to say, the reader is only permitted to recognize authorized vehicles.
- **An anonymous RFID authentication scheme is proposed for vehicles in a transportation system.** To resist attack after losing a reader, the authentication protocol innovatively confirms the legitimacy of a reader's identity . By requiring the reader to update its password periodically,

the server can ensure the running condition of the reader after verifying the updated response. Thus, the lost reader cannot be used to attack our protocol and may be nullified. Considering that the tag is limited, the proposed protocol adopts some lightweight operations. In experimental comparisons with related protocols, we prove that the proposed scheme consumes fewer computing and communication resources in relation to tags.

- **The new protocol is proven to be secure with the Burrows–Abadi–Needham (BAN) logic [12] proof method and security discussion.** Firstly, we employ a formal analysis tool BAN logic to demonstrate the security of key agreement and mutual authentication. Secondly, we discuss that the protocol achieves multiple safety goals, including reader lost resistance, anonymity un-traceability, mutual authentication, forward security, replay attack, and de-synchronization attack resistance. Thirdly, we compare the secure property of our protocol with some related protocols.

Organization: The remainder of this paper is organized as follows. Section 2 surveys some previous work. Section 3 introduces the system architecture and some security goals. In Section 4, we illustrate, in detail, our scheme which contains some initial assumptions, an anonymous authentication protocol, and a reader's password modification. Section 5 presents the formal analysis tool BAN logic and the careful security analysis for the new scheme. Section 6 presents the performance analysis and evaluation of the proposed scheme. Finally, some conclusions are provided in Section 7.

2. Related Work

With various services growing in VANETs, many issues appear in VANET research. The cooperation in VANETs can share information to improve traffic instructions and entertainments. However, Fuad et al. [13] pointed out that misbehaving vehicles disrupted participant cooperativeness by sharing bogus information, where the misbehaving vehicle may cause a loss of people's lives and properties. An anonymous VANET is considered a privacy-preserving vehicle network. Lu et al. [14] stated that a mechanism based on pseudonymity is insufficient to thwart a tracking attack that may expose the vehicles' privacy. Lu et al. considered that location privacy needs further protection. Shrikant et al. [15] found that VANETs can improve traffic management and be susceptible to security attacks from malicious entities. With RFID deploying in many IoT applications, much attention is focused on the security and privacy-preserving scheme based-on RFID [16].

The transportation system integrates with RFID and other sensors to transport and dispatch manufacturing materials [17]. The system not only takes the bond to link vehicles and transportation but also brings some issues to them. For instance, the geographic position and identity mark are easily intercepted [18], for the reason that these data are transmitted for different services in a public network frequently. To protect personal privacy, Fan et al. [19] proposed a privacy-preserving scheme. However, there is a fatal error for synchronization when looping some steps. To design a proper scheme, we study the related RFID-based works. Pedro et al. [20] proposed an RFID-based system to handle the replay and forgery attack. Later, Liu et al. [21] pointed out that [20] is vulnerable under the imitative and de-synchronization attack [22], which causes the secret to be out of sync in different entities and may interrupt the running protocol. To avoid the de-synchronization attack, Tian et al. [23] presented a protocol to preserve the old and updated key values. Although the replay attack could be resisted in their security analysis, the adversary may still imitate the reader to fraud the tag.

Li et al. [24] considered it inadvisable in the previous works, such as [25], to declare each tag's identity before authenticating each entity in their protocols, which may leak its identity privacy to attackers. Thus, Li et al. proposed a novel authentication notion and three improved protocols based on the bilinear diffie hellman (BDH) problem under different security conditions. However, their protocols, which are designed for some special scenes, are not generic. Later, Chou [26] proposed a protocol based on elliptic curve cryptography (ECC) against usual attacks. However, Zhang et al. [27] pointed out the identity privacy exposure issue in [26] and presented an efficient protocol to overcome that issue. Abughazalah et al. [28] found that an adversary can distinguish a tag from different sessions in [9] and proposed an improved protocol. Xiao et al. [29] considered that the secure hypothesis in [28]

is infeasible and the privacy of tags is ignored. Then, Xiao et al. presented a supporting anonymity protocol to resist various attacks in a communication channel. Though these protocols can resist some known attacks, it is hard for the limited passive tags to execute relatively heavy computing operations according to the criterion in [30] and the demand in real-time applications. Thus, many lightweight RFID protocols are proposed and adopted in most RFID systems to deduce the cost of implementation.

Fan et al. [31] gave an RFID-based lightweight protocol for IoT. To reduce the time cost of retrieving and authenticating tags, they presented a cache mechanism to store the recent tag key in their reader. However, in fact, an adversary may attack this protocol after compromising the off-line reader's secrets. Later, Fan et al. [10] summed up the previous works and proposed a new lightweight protocol that has satisfied some necessary security properties. They illustrated a lightweight operation "$Cro(x, y)$" called "Cross". Actually, "$Cro(x, y)$" can be seen as a particular function composed of some XOR operations [32]. By analyzing the new protocol, we consider that anonymity and de-synchronization security have not be realized. To be specific, an adversary may obtain the tag's identity and interrupt the secret update through intercepting or modifying the communicating message. To deal with the above problems, we propose a new scheme.

3. Problem Statement

3.1. System Model

Figure 1 illustrates our authentication system architecture for vehicle transportation based on RFID. To protect the private data during the system communication, the new scheme has to mutually identify the system participants and achieve session key updates securely. The participants consist of three types that are the server, RSU/reader, and the recognized OBU/tag.

Server: The server undertakes the duty to initialize some necessary system parameter values for recognizing each participant. In addition, the server has the responsibility to provide enough computing ability and storage resources for reasonable access requests.

RSU/Reader: The RSU is a special reader, employed on the roadside and seen as the intermediate to obtain information from vehicles and the server. It is worth noting that there are two types of readers. One type connects to the server or the recognized vehicles with the insecure wireless channel. The other accesses the server through a wireline communication channel, which can be seen as a reliable connection. In general, we only discuss wireless access for the reader. Every reader has a unique and private password to prove the rightful identity, which is utilized to acquire the server's authorization before access to different information.

OBU/Tag: OBU consists of ample sensors (such as RFID tag, position, speed, acoustic sensor) and is assembled in the recognized vehicle. Here, the RFID tag is used as an identification license and session key calculation participant when a vehicle tries to enter VANETs. Only by passing through the reader's authentication can the vehicle attain shared messages from VANETs and send its traffic condition. Besides, the tag is able to distinguish the faked and rightful messages.

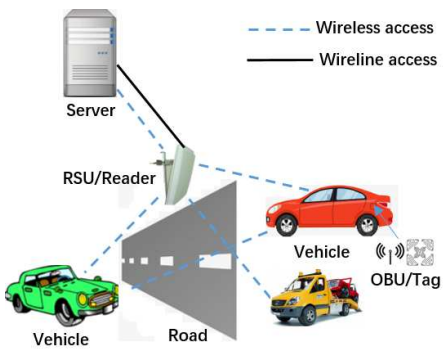

Figure 1. RFID-based architecture for transportation system.

3.2. Security Goals

According to the previous research works and Dolev–Yao model [33], an attacker may have the ability to control the wireless channel and launch some attacks that are intercepting, modifying, and even simulating a rightful participate to replay the transmitted messages at will. However, the traffic data is crucial, and an unexpected error may threaten personal property or even life. Thus, we designed this scheme to transmit traffic session data securely. To overcome those attacks, the following security goals are essential.

Anonymity Un-traceability: To protect the recognized vehicle's privacy, our scheme preserves the real identity and prevents attackers from distinguishing different session messages whether from the same recognized vehicle.

Mutual Authentication: Before providing the required information, the recognized vehicle or server has to verify the reader's reliability. The reader also authenticates the recognized vehicle or server to ensure the integrity and correctness of messages.

Forward Security: To ensure secure communication, the scheme updates the shared key in each new session. In addition, the utilized key previously cannot be deduced according to the current parameters.

Resist Replay Attack: Because the previous messages are valid and can be used to fraud the rightful participant. The scheme has to ensure each participant can recognize the replayed messages and resist this attack.

De-synchronization Attack Resistance: In most protocols, some secret parameters are periodically updated to resist the leakage of session secret values. However, an attacker may interrupt this operation. This attack leads to parameters that are out of sync in different participants and failure in a future session. Thereby, our scheme has to resist this attack.

Resist Reader Lost: After losing a reader, an attacker may utilize the reader to collect privacy information before it is nullified. To resist such an attack, precaution is indispensable.

4. The Scheme

We firstly describe some notations utilized in this scheme and their definitions, that are both shown in Table 1. Then, we illustrate, in detail, the new scheme in three subsections that are the initialization, authentication, and the reader's password updated phase.

Table 1. Symbols used in the scheme.

Symbol	Definition
id_R, id_T	A reader's identity, a tag's identity
R, T, S	A reader, a tag, a server
K_{RS}	Reader's next session key shared with a server
K_{TS}	Tag's next session key shared with a server
N_S	A number selected randomly by a server
N_R	A number selected randomly by a reader
N_T	A number selected randomly by a tag
$W(y)$	Calculate the number of non-zero bits in y
$LRot(x, y)$	The cyclic left shift $W(y)$ bits operation
$Rot(x, y)$	The cyclic right shift $W(y)$ bits operation
$H()$	A secure one-way hash function
$\oplus$	The exclusive or operation
$\|\|$	The concatenation operation

4.1. Initialization Phase

To recognize reasonable participants, the server S has to initialize some parameters for the system roles. Firstly, the server S establishes two registration parameter tables $RegT$ and $RegR$, shown in

Figure 2 before distributing identities and keys to all tags and readers. Then, the server S allocates a sole identity and key to every tag and reader via some secure channels, respectively.

$RegT$ includes some tuples (id_{Ti}, v_i) about the corresponding relation of each tag's identity and key. $RegR$ includes some information about each reader's identity id_{Ri} and the related long-term key C_i. Every reader has to calculate $C_{pw} = C \oplus H(id_R||pwd)$ to protect the long-term key C before storing it, where pwd is a pre-generated password for every reader and can be changed for the future. Additionally, the server S needs to encrypt this information with a private key before storing them in the database.

In addition, we define a new retrieval method by utilizing the relation between $RegT$ and $RegR$. From Figure 2, we can see an arrow from $RegR$'s content (C_1, id_{R1}) to (v_1, id_{T1}) in $RegT$, which indicates that the reader id_{R1} is only permitted to authenticate the tag id_{T1}. The arrow from content (C_2, id_{R2}) to (v_i, id_{Ti}) means that the reader id_{R2} is able to authenticate these tags from id_{T1} to id_{Ti}. Then, we can alter the reader's ability and the range of information retrieval by predefining the orientation of the arrow. Thus, this method assures that the privacy data are only accessed by the authorized users and distinguishes the security level for different vehicles.

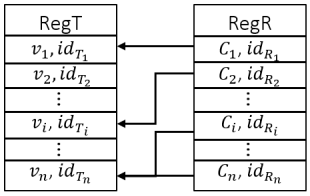

Figure 2. Two registration data tables.

4.2. Authentication Phase

Figure 3 illustrates this authentication phase that a reader identifies a tag in detail. This phase can be divided into seven steps, and the details of implementation are shown in every step.

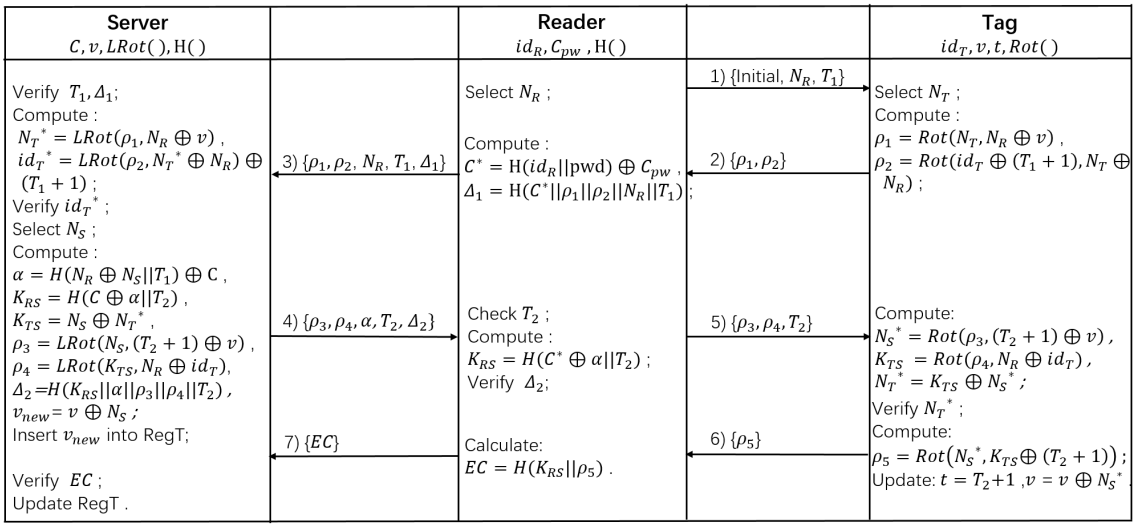

Figure 3. The authenticated phase.

(Step 1) The reader selects a random number N_R and sends the message $\{N_R, T_1, Initial\}$ to the tag, where T_1 is a timestamp and $Initial$ is a session beginning notification.

(Step 2) The tag first validates the freshness of T_1. If the timestamp T_1 is overdue, the tag terminates the protocol. Otherwise, the tag randomly selects a number N_T. Then, the tag computes $\rho_1 = Rot(N_T, N_R \oplus v)$, $\rho_2 = Rot(id_T \oplus (T_1 + 1), N_T \oplus N_R)$. Finally, the tag sends $\{\rho_1, \rho_2\}$ to the reader.

(Step 3) When getting the tag's response, the reader computes $C^* = H(id_R||pwd) \oplus C_{pw}$, $\Delta_1 = H(C^*||\rho_1||\rho_2||N_R||T_1)$, where C_{pw} and pwd are periodically updated values. Then, the reader sends the message $\{\rho_1, \rho_2, N_R, T_1, \Delta_1\}$ to the server.

(Step 4) After obtaining that message from the reader, the server first checks the freshness of the timestamp T_1 and the value of Δ_1 by computing ${\Delta_1}^* = H(C||\rho_1||\rho_2||N_R||T_1)$, where C is a local value in $RegR$. If the message does not reach the server within a predefined threshold or the value of Δ_1 is invalid, the server immediately terminates the current protocol. Otherwise, the server continues to compute ${N_T}^* = LRot(\rho_1, N_R \oplus v)$ and ${id_T}^* = LRot(\rho_2, {N_T}^* \oplus N_R) \oplus (T_1 + 1)$. Then, the server searches ${id_T}^*$ in its registration table $RegT$ in order to verify the tag's identity. When ${id_T}^*$ is found in $RegT$, the server randomly generates a number N_S and calculates $\alpha = H(N_R \oplus N_S||T_1) \oplus C$, $K_{RS} = H(C \oplus \alpha||T_2)$, $K_{TS} = {N_T}^* \oplus N_S$, $\rho_3 = LRot(N_S, (T_2 + 1) \oplus v)$, $\rho_4 = LRot(K_{TS}, N_R \oplus id_T)$, $\Delta_2 = H(K_{RS}||\alpha||\rho_3||\rho_4||T_2)$, $v_{new} = v \oplus N_S$. Finally, the server sends the message $\{\rho_3, \rho_4, \alpha, T_2, \Delta_2\}$ to the reader and inserts a new record $(v_{new}, {id_T}^*)$ into $RegT$.

(Step 5) Upon receiving a response message from the server, the reader first checks whether T_2 is fresh. If T_2 is fresh, the reader computes the session key $K_{RS} = H(C^* \oplus \alpha||T_2)$ which is shared with the server. Then, the reader verifies Δ_2 by using the received values and K_{RS} to calculate ${\Delta_2}^* = H(K_{RS}||\alpha||\rho_3||\rho_4||T_2)$. If the value ${\Delta_2}^*$ equals Δ_2, that session key K_{RS} is established, and the reader sends $\{\rho_3, \rho_4, T_2\}$ to the tag. Otherwise, the reader terminates the protocol.

(Step 6) After receiving the reader's response message, the tag computes ${N_S}^* = Rot(\rho_3, (T_2 + 1) \oplus v)$, $K_{TS} = Rot(\rho_4, N_R \oplus id_T)$, and ${N_T}^* = K_{TS} \oplus {N_S}^*$ in order. If ${N_T}^*$ does not equal N_T generated by itself, the tag ends this phase. Otherwise, the tag considers that the server and reader are reliable and the session key K_{TS} has been shared with the server. Then, the tag updates $t = T_2 + 1$ and $v = v \oplus {N_S}^*$, which manifests in a new session key being established. After the update, the tag sends a message $\rho_5 = Rot({N_S}^*, K_{TS} \oplus (T_2 + 1))$ to the reader.

(Step 7) The reader calculates the cipher $EC = H(K_{RS}||\rho_5)$ and sends it to the server. When the server obtains EC, it can verify EC by calculating $EC^* = H(K_{RS}||Rot({N_S}^*, K_{TS} \oplus (T_2 + 1)))$ with K_{RS} and K_{TS}. If there exists an equation relationship "$EC = EC^*$", it indicates that the server has shared a session key with the reader and tag severally. In this case, the server has to delete old tuples $(v_i \neq v_{new}, {id_T}^*)$ and update $RegT$.

4.3. Password Updated Phase

Due to the reader being installed in an unmanned site, it is inconvenient to check the running condition. We propose a periodically updated password strategy to avoid the failure or loss of a reader. To be specific, the server sends updated order and the encrypted nonce $E_C(N_S)$ to a certain reader. After confirming the updated command, the reader preserves the new password pwd^{new} and ${C_{pw}}^{new}$, where $pwd^{new} = H(pwd||N_S)$, ${C_{pw}}^{new} = C_{pw} \oplus H(id_R||pwd) \oplus H(id_R||pwd^{new})$. Then, the reader returns $E_{C \oplus N_S}(C||T_i)$ to the server, where T_i is a timestamp. After passing through the authentication of the server, we consider the reader working normally.

It is easy to see that the authentication structure of a reader R is a single factor mechanism. We can extend a single-factor authentication into two-factor authentication by adding an extra XOR operation into C_{pw} to resist password leakage, e.g., we have another factor named pos, which is a position code [34] transformed into the same bit length of C_{pw}, and we can calculate $C_{pw} = C_{pw} \oplus C \oplus pos$ to hide the secret information C. In that case, as long as one factor has not been corrupted, the reader's secret is still secure [35,36]. To resist the leakage of secret keys, a leakage-resilient mechanism [37,38] can be introduced into our scheme. However, the resilient key's leakage is beyond this paper, we do not expand the work in this paper.

5. Security Analysis

We firstly employ the logic "Burrows–Abadi–Needham (BAN) [12]" proof tool to demonstrate that our scheme is correct and secure. Further, we discuss the security goals of our authentication protocol in detail. Finally, we present the properties of our protocol in comparison with some typical protocols.

5.1. Security Proof

BAN logic is an intuitive and efficient proof tool. We can employ this logic to idealize and model the authentication phase, which forms assumptions and goals. By utilizing some logical belief rules to prove the security goals, we can judge the correctness and mutual authentication security in our scheme.

5.1.1. Notations

Before exploiting the BAN logic, we briefly introduce the following notations utilized in this proof.

- $P \mid\equiv X$: P believes that a statement X is authentic.
- $P \mid\sim X$: P sent the statement X before.
- $P \lhd X$: P once received that statement X.
- $P \mid\Rightarrow X$: P has jurisdiction over that statement or a notation X.
- $\#(X)$: The statement or notation X that has never been sent is fresh.
- $\{X\}_k$: This statement is obtained by using a secret key k to encrypt X or combining X with a secret value k.
- $P \overset{Y}{\rightleftharpoons} Q$: P only shares the same secret value Y with Q and the others that P or Q believes.
- $P \overset{k}{\leftrightarrow} Q$: There is a secret key k only known by P and Q.

5.1.2. Rules

To deduce and prove some secure goals, we need to employ the following BAN rules. From the following rules, we can obtain a corollary below when these hypotheses above the horizontal line are satisfied.

R_{u1} (Message-meaning rule): $\frac{P|\equiv P\overset{Y}{\rightleftharpoons}Q, P\lhd\{X\}_Y}{P|\equiv Q|\sim X}$ and $\frac{P|\equiv P\overset{k}{\leftrightarrow}Q, P\lhd\{X\}_k}{P|\equiv Q|\sim X}$;

R_{u2} (Jurisdiction rule): $\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$;

R_{u3} (Freshness-conjuncatenation rule): $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$;

R_{u4} (Nonce-verification rule): $\frac{P|\equiv\#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$;

R_{u5} (Belief rule): $\frac{P|\equiv(X,Y)}{P|\equiv X}$ and $\frac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X}$.

5.1.3. Descriptions

According to these messages exchanged in our scheme and the proof procedure of BAN logic, we extract essential parameters and form the idealized description of the authentication phase. Descriptions are shown as follows.

The exchanged messages:

M_{e1}:$T \rightarrow R$ $\{\rho_1, \rho_2\}$

M_{e2}:$R \rightarrow S$ $\{\rho_1, \rho_2, N_R, T_1, \Delta_1\}$

M_{e3}:$S \rightarrow R$ $\{\rho_3, \rho_4, \alpha, T_2, \Delta_2\}$

M_{e4}:$R \rightarrow T$ $\{\rho_3, \rho_4, T_2\}$

M_{e5}:$T \rightarrow R$ $\{\rho_5\}$

M_{e6}:$R \rightarrow S$ $\{EC\}$

The idealized descriptions:

M_{e1}: $T \rightarrow R$ $\{T \overset{N_T}{\rightleftharpoons} S, N_R, T_1, id_T\}_{T\overset{v}{\leftrightarrow}S}$;

M_{e2}: $R \rightarrow S$ $\{\rho_1, \rho_2, N_R, T_1\}_{R\overset{C}{\leftrightarrow}S}$;

M_{e3}: $S \rightarrow R$ $\{R \overset{K_{RS}}{\leftrightarrow} S, \alpha, \rho_3, \rho_4, T_2\}_{R \overset{C}{\leftrightarrow} S}$;
M_{e4}: $R \rightarrow T$ $\{T \overset{K_{TS}}{\leftrightarrow} S, T \overset{N_S}{\rightleftharpoons} S, T_2, N_R, T \overset{N_T}{\rightleftharpoons} S, id_T\}_{T \overset{v}{\leftrightarrow} S}$;
M_{e5}: $T \rightarrow R$ $\{T \overset{K_{TS}}{\leftrightarrow} S, T_2\}_{T \overset{N_S}{\rightleftharpoons} S}$;
M_{e6}: $R \rightarrow S$ $\{R \overset{K_{RS}}{\leftrightarrow} S, \rho_5\}_{T \overset{N_S}{\rightleftharpoons} S}$.

5.1.4. Assumptions

According to the next procedure of BAN logic, we analyze our authentication protocol and present some initial assumptions for the proof phase.

A_{s1}: $T \mid\equiv \#(N_T)$;
A_{s2}: $R \mid\equiv \#(N_R), R \mid\equiv \#(T_1)$;
A_{s3}: $S \mid\equiv \#(N_S), S \mid\equiv \#(T_1), S \mid\equiv \#(T_2)$;
A_{s4}: $T \mid\equiv T \overset{v}{\leftrightarrow} S, S \mid\equiv T \overset{v}{\leftrightarrow} S$;
A_{s5}: $R \mid\equiv R \overset{C}{\leftrightarrow} S, S \mid\equiv R \overset{C}{\leftrightarrow} S$;
A_{s6}: $T \mid\equiv T \overset{N_T}{\rightleftharpoons} S, S \mid\equiv T \overset{N_S}{\rightleftharpoons} S$;
A_{s7}: $S \mid\equiv R \mid\Rightarrow \{\rho_1, \rho_2, N_R, T_1\}$;
A_{s8}: $T \mid\equiv R \mid\Rightarrow \{T \overset{K_{TS}}{\leftrightarrow} S, T \overset{N_S}{\rightleftharpoons} S, T_2, N_R, T \overset{N_T}{\rightleftharpoons} S, id_T\}$;
A_{s9}: $R \mid\equiv S \mid\Rightarrow \{R \overset{K_{RS}}{\leftrightarrow} S\}$;
A_{s10}: $S \mid\equiv R \mid\Rightarrow \{R \overset{K_{RS}}{\leftrightarrow} S, \rho_5\}$.

5.1.5. Goals

According to the logic analytic program, it is a necessary step to prove that the protocol achieves the following specific goals before believing the correctness and session security of the proposed scheme.

G_{o1}: $S \mid\equiv T \overset{N_T}{\rightleftharpoons} S$; G_{o2}: $T \mid\equiv T \overset{N_S}{\rightleftharpoons} S$;
G_{o3}: $T \mid\equiv T \overset{K_{TS}}{\leftrightarrow} S$; G_{o4}: $R \mid\equiv R \overset{K_{RS}}{\leftrightarrow} S$;
G_{o5}: $S \mid\equiv T \overset{K_{TS}}{\leftrightarrow} S$; G_{o6}: $S \mid\equiv R \overset{K_{RS}}{\leftrightarrow} S$.

5.1.6. Proof

The following statements are the detailed process to prove these goals $G_{o1}, G_{o2}, G_{o3}, G_{o4}, G_{o5}, G_{o6}$.

(1) : From message M_{e1}, we get, $R \lhd \{T \overset{N_T}{\rightleftharpoons} S, N_R, T_1, id_T\}_{T \overset{v}{\leftrightarrow} S}$.
(2) : From message M_{e2}, we get, $S \lhd \{\rho_1, \rho_2, N_R, T_1\}_{R \overset{C}{\leftrightarrow} S}$.
(3) : From message M_{e3}, we get, $R \lhd \{R \overset{K_{RS}}{\leftrightarrow} S, \alpha, \rho_3, \rho_4, T_2\}_{R \overset{C}{\leftrightarrow} S}$.
(4) : From message M_{e4}, we get, $T \lhd \{T \overset{K_{TS}}{\leftrightarrow} S, T \overset{N_S}{\rightleftharpoons} S, T_2, N_R, T \overset{N_T}{\rightleftharpoons} S, id_T\}_{T \overset{v}{\leftrightarrow} S}$.
(5) : From message M_{e5}, we get, $R \lhd \{T \overset{K_{TS}}{\leftrightarrow} S, T_2\}_{T \overset{N_S}{\rightleftharpoons} S}$.
(6) : From message M_{e6}, we get, $S \lhd \{R \overset{K_{RS}}{\leftrightarrow} S, \rho_5\}_{T \overset{N_S}{\rightleftharpoons} S}$.
(7) : According to R_{u1}, A_{s5} and (2), we deduce, $S \mid\equiv R \mid\sim \{\rho_1, \rho_2, N_R, T_1\}$.
(8) : According to R_{u3}, R_{u4}, A_{s3} and (7), we deduce, $S \mid\equiv R \mid\equiv \{\rho_1, \rho_2, N_R, T_1\}$.
(9) : According to R_{u2}, R_{u5} , A_{s7} and (8), we deduce, $S \mid\equiv \{T \overset{N_T}{\rightleftharpoons} S, N_R, T_1\}$.
From R_{u5} and (9), we prove the goal, $G_{o1} : S \mid\equiv T \overset{N_T}{\rightleftharpoons} S$.
(10) : According to R_{u1}, A_{s4} and (4), we deduce, $T \mid\equiv R \mid\sim \{T \overset{K_{TS}}{\leftrightarrow} S, T \overset{N_S}{\rightleftharpoons} S, T_2, N_R, T \overset{N_T}{\rightleftharpoons} S, id_T\}$.

(11) : According to A_{s1}, R_{u3}, R_{u4} and (10), we deduce, $T \mid\equiv R \mid\equiv \{T \overset{K_{TS}}{\leftrightarrow} S, T \overset{N_S}{\rightleftharpoons} S, T_2, N_R, T \overset{N_T}{\rightleftharpoons} S, id_T\}$.

(12) : According to R_{u2}, A_{s8} and (11), we deduce, $T \mid\equiv \{T \overset{K_{TS}}{\leftrightarrow} S, T \overset{N_S}{\rightleftharpoons} S, T_2, N_R, T \overset{N_T}{\rightleftharpoons} S, id_T\}$.

From R_{u5} and (12), we obtain the goal, $G_{o2} : T \mid\equiv T \overset{N_S}{\rightleftharpoons} S$ and $G_{o3} : T \mid\equiv T \overset{K_{TS}}{\leftrightarrow} S$.

(13) : According to R_{u1}, A_{s5} and (3), we deduce, $R \mid\equiv S \mid\sim \{R \overset{K_{RS}}{\leftrightarrow} S, \alpha, \rho_3, \rho_4, T_2\}$.

(14) : According to R_{u3}, R_{u4}, A_{s2} and (13), we deduce, $R \mid\equiv S \mid\equiv \{R \overset{K_{RS}}{\leftrightarrow} S, \alpha, \rho_3, \rho_4, T_2\}$.

(15) : According to R_{u2}, R_{u5} , A_{s9} and (14), we deduce, $R \mid\equiv R \overset{K_{RS}}{\leftrightarrow} S$. That is to say we prove G_{o4}.

(16) : According to R_{u1}, A_{s6} and (6), we deduce, $S \mid\equiv R \mid\sim \{R \overset{K_{RS}}{\leftrightarrow} S, \rho_5\}$.

(17) : According to R_{u3}, R_{u4}, A_{s2} and (16), we deduce, $S \mid\equiv R \mid\equiv \{R \overset{K_{RS}}{\leftrightarrow} S, \rho_5\}$.

(18) : According to R_{u2}, R_{u5} , A_{s10} and (17), we deduce, $S \mid\equiv \{R \overset{K_{RS}}{\leftrightarrow} S, \rho_5\}_{T \overset{N_S}{\rightleftharpoons} S}$.

From R_{u5} and (18), we can prove the goal, $G_{o5} : S \mid\equiv T \overset{K_{TS}}{\leftrightarrow} S$ and $G_{o6} : S \mid\equiv R \overset{K_{RS}}{\leftrightarrow} S$.

After these goals are proved, it means that the mutual authentication security has been achieved and the session is secure.

5.2. Security Discussion

To make out our scheme, it is necessary to discuss some security and functionality goals detailedly. The following analysis illustrates all the realized goals.

Anonymity Un-Traceability (AU): Anonymity is a critical security goal. Without the protection of identity privacy, attackers can find out a certain vehicle or reader by eavesdropping the wireless signals and collecting more information to analyze the vehicle's or reader's behaviors. Then, attackers may simulate a right participant to fraud a certain reader or vehicle. To prevent such a tracking attack, both the tag's and reader's anonymity are considered in our scheme. Note that the reader's identity is only used in the local, and the unique secret C^* cannot be inferred from the value Δ_1 due to the advantage of the one-way hash function $H()$ and the random number N_R, which is different in every session. So, it is hard for the adversary to distinguish and trace a certain reader. For the tag, its identity id_T is never disclosed and cannot be retrieved from the transmitted ρ_2 without knowing N_T, which is a secret value hidden in ρ_1 and changed in each session. Additionally, attackers cannot retrieve N_T from ρ_1 without knowing the tag's secret v, which is shared with the server. Thus, tag anonymity is also realized.

Mutual Authentication (MA): In the open environment, there are some attackers to impersonate real participants to cheat other legitimate participants and filch secret information. Thus, it is necessary to confirm the protocol participators' identity before establishing the session key or executing some operations. In this protocol, the server has to authenticate the tag and reader, respectively. Upon receiving the message $\{\rho_1, \rho_2, N_R, T_1, \Delta_1\}$ from the reader, the server searches a value C to calculate ${\Delta_1}^i$, where i is the reader's number. If there is an equation ${\Delta_1}^i = \Delta_1$, it indicates that the reader's identity is legitimate. Then, the server retrieves ${N_T}^*$ from ρ_1 with the shared secret v and obtains the tag's identity ${id_T}^*$ from ρ_2. When the tuple $(v, {id_T}^*)$ can be matched in $RegT$, which includes tag identity and the related key, this means that the server authenticates a tag successfully. Meanwhile, the reader can verify Δ_2 to confirm the server's reliability, and the tag can calculate and compare ${N_T}^*$ with the local N_T to authenticate the server. Therefore, this protocol satisfies the need for mutual authentication.

Forward Security (FS): Even if an adversary illegally gets access to partial or intact secret information that is related to the current session key, she/he is unable to speculate the previous session key, which is named as forward security. In this protocol, the session keys $K_{RS} = H(C^* \oplus \alpha || T_2)$ and $K_{TS} = {N_S}^* \oplus {N_T}^*$ contain different random numbers and timestamps. It is noted that the session key is changed in each new communication and these random numbers are only used in the current session. Thus, it is hard for an adversary to guess the previous keys according to current or past information.

Resist Replay Attack (RA): Attackers may resend some messages to fraud the real authenticator when they collect sufficient communication messages. To deal with the replay attack, we adopt two mechanisms that are timestamps $\{T_1, T_2\}$ and random nonces $\{N_T, N_R, N_S\}$. Assuming an adversary replays the message $\{\rho_1, \rho_2, N_R, T_1, \Delta_1\}$ to the server, it may fail to pass authentication due to the overdue timestamp or random nonces. Even if the replayed message reaches the server within the valid period and the adversary gets a response message, the adversary is still unable to compute the shared session key $K_{RS} = H(C^* \oplus \alpha || T_2)$ and the confirmation message EC. Because the adversary has to know the reader's secret value C to compute the K_{RS} and EC. However the adversary can not obtain that value C without the reader's password pwd and C_{pw}. In addition, the adversary is also unable to impersonate a tag and infer the tag's session key $K_{TS} = {N_S}^* \oplus {N_T}^*$ from ρ_4 without knowing secret id_T and v.

De-Synchronization Attack Resistance (DA): When some participants update some secrets, a kind attack that an adversary blocks one part of a session's update is named de-synchronization, which may cause the later authentication failure. In our protocol, if an adversary intercepts $\{\rho_3, \rho_4, T_2\}$, the tag may not update v. So, the server inserts updated content $(v_{new}, {id_T}^*)$ into $RegT$ before getting synchronization acknowledgement EC, to prevent such an attack. To be specific, when the server fails to verify ${id_T}^*$ with the new content $(v, {id_T}^*)$ in the next authentication session, it can try the old content $(v, {id_T}^*)$ to verify ${id_T}^*$. After a successful verification, the server deletes the invalid content $(v, {id_T}^*)$ to maintain the consistency of v.

Resist Reader Lost (RL): If a reader is stolen, an adversary may utilize it to trick the server and filch some secret information. By hiding the essential value C^* in $C_{pw} = C^* \oplus H(id_R || pwd)$ with identity id_R and password pwd, it is hard for the adversary to guess the right value. Because we do not arrange a mechanism to verify C^* in the reader, the adversary has to speculate the lost reader's password on-line. Only if the latest password and the protocol is executed honestly, may the adversary pass through the server's authentication and get its response. However, the number of failed attempts is limited by the server, which is a method to avoid such an on-line password dictionary attack. Besides, the server periodically sends updated orders to a certain reader. If the server does not receive the updated response in time, the lost reader may be nullified or removed from rightful $RegT$.

5.3. Property Comparison

This section selects some typical schemes [9,10,28,29] properties in comparison with our authentication phase (AP). Table 2 shows the comparison vividly, where "✓" indicates this property is satisfied, while the symbol "×" means this property is unfulfilled.

From Table 2, we can see that MA and DA are both achieved in [9,28,29] and AP. However, [29] only satisfies partial MA between the tag and reader. Compared to other schemes, the server and reader cannot be authenticated by each other. The authors in [9,28,29] fail to satisfy the FS and RA properties simultaneously. However, FS and RA are vital for authentication key agreement protocol to establish some secure session keys. When these properties are absent, the attacker may illegally speculate some secret information from previous messages by deducing the old session key with some corrupted keys. Though [29] simultaneously achieves the MA and RA properties, it is still unable to protect personal privacy. Because the tag keys are all preserved in the server, and MA between the reader and server is absent, an honest server is unable to confirm the validity of a reader. After corrupting the reader successfully, an adversary may imitate a rightful reader and steal the tag's privacy data, which may not be detected.

We also find that MA, FS, and RA are achieved in the lightweight protocol [10] except for AU, DA, and RL. Though [10] deems that the property AU and DA are satisfied, it fails to preserve the identity of the tag and update session key. Due to a design defeat, an adversary can extract a tag's identity and even current key from the authentication message by a simple exclusive or operation. Besides, an adversary may utilize a lost reader to pass validation and collect private information before declaring it invalid when the feature RL is absent. Compared with the aforesaid protocols,

our authentication protocol (AP) can guarantee AU, MA, FS security and prevent RA, DA, RL attack. That is our secure property advantage.

Table 2. Property comparison.

	[9]	[10]	[28]	[29]	AP
AU	×	×	×	✓	✓
MA	✓	✓	✓	✓	✓
FS	✓	✓	×	×	✓
RA	×	✓	✓	✓	✓
DA	✓	×	✓	✓	✓
RL	×	×	×	×	✓

6. Performance Analysis And Evaluation

We first compare our authentication phase (AP) with some typical schemes [9,10,28,29] in the aspect of computation, storage, and communication cost. Then, we conduct a simulated performance evaluation for the new scheme.

6.1. Performance Analysis

Computing complexity analysis: In Table 3, it shows the time of different operations or functions that are utilized in each participant. "T_H" represents the time to execute a secure one-way function. "T_N" is the time to generate a number randomly. "$T_{E/D}$" is the symmetric encryption or decryption time. "T_{Cro}" is the time of a cross mixing operation which is defined in the paper [10]. Because the computing complexity of "H" is further higher than other functions, it is more significant for us to focus on the amount of "T_H". From Table 3, it is apparent that [9,28,29] may consume more time and energy resources than AP, for the reason that more "H" and other operations have to be executed in comparison to AP. However, in fact, we know the tags' power is limited relative to their readers. It is inefficient and unwise for the tag to execute many complex computations, especially in some scenarios of timeliness. We also pay attention to the number of operations in the tag. Therefore, some lightweight operations are adopted in the tag of AP. From Table 3, it appears that [10] and AP are both efficient when some lightweight operations are utilized in their tags. However, [10] has to handle more operations on their readers than AP. In AP, the computation cost of its reader is five times H and an N for the message authentication, which is less than [9,28,29]. Thus, AP is lightweight and efficient.

Table 3. Computation comparison.

Protocol	Tag	Reader	Server
[9]	$T_N + 4T_H$	$T_{E/D} + T_N + 6T_H$	$T_{E/D} + 3T_H$
[10]	$T_N + 3T_{Cro}$	$T_N + 6T_{Cro} + T_{Rot}$	$T_N + 6T_{Cro} + 2T_{Rot}$
[28]	$T_N + 5T_H$	$T_{E/D} + T_N + 5T_H$	$T_{E/D} + 2T_H$
[29]	$T_N + 6T_H$	$T_N + 7T_H$	$3T_H$
AP	$T_N + 5T_{Rot}$	$T_N + 5T_H$	$T_N + 5T_{Rot} + 5T_H$

Storage complexity analysis: In Table 4, the symbol ι is the average length of these notations utilized in our scheme and the compared schemes. Additionally, the length of these notations is considered as same. We compare the storage cost of different schemes on the tag and reader, respectively, where that cost is the static storage space occupied in the reader or tag. In AP, the secret values id_T, v and the timestamp T of the last session are preserved in the tag, and the reader preserves id_R, C_{PW} in its storage space. Therefore, the storage cost on the tag is 3ι, and that on the reader is 2ι. Similarly, in the compared schemes, the tag or reader also has to preserve its identity and some secret values for future authentication and next key agreement. Table 4 displays the storage comparison. The storage cost of AP is almost no different from the compared schemes. We can find that the tag's

storage cost is 3ι in [9,29] and AP, which is slightly greater than that in [28,29]. That is because [9,29] and AP need an extra value to achieve de-synchronization or replay attack resistance except storing the tag's identity and keyword. Indeed, therefore, their schemes reach that resistance.

Table 4. Storage comparison.

Protocol	Tag	Reader
[9]	3ι	2ι
[10]	2ι	2ι
[28]	2ι	ι
[29]	3ι	2ι
AP	3ι	2ι

Communication cost analysis: In Table 5, we present the amount of communication data between two pairs of the participant. In AP, the tag sends three values ρ_1, ρ_2, ρ_5 to the reader, and receives a nonce N_R, two timestamps T_1, T_2, two values ρ_3, ρ_4 during a whole authentication process. Therefore, the communication cost for a pair of tag and reader is "8ι $(3\iota + 5\iota)$". According to these transmitted messages between the reader and the server, we can deduce that the communication cost is "14ι $(8\iota + 6\iota)$", where the length of the hashed message is 2ι, such as Δ_1, Δ_2, EC. Then, by counting the amount of communication data in [9,10,28,29], we form Table 5. From this communication comparison, we notice that the total communication amount of AP is greater than [28,29] and lower than [9,10]. That is because AP simultaneously adopts the method of nonce and timestamp to resist replay attack. Additionally, some operations or functions with double-length output, such as $Cro(x, y)$, are utilized in [9,10], which leads to the communication cost of AP increasing. However, in fact, the amount of communication data on AP's tag is 3ι, which is superior to that in [9,10,28,29]. That is to say, AP is suitable to apply in the limited tag.

Table 5. Communication comparison.

Protocol	Tag-Reader	Reader-Server	Total
[9]	10ι $(5\iota + 5\iota)$	14ι $(8\iota + 6\iota)$	24ι
[10]	11ι $(6\iota + 5\iota)$	13ι $(7\iota + 6\iota)$	24ι
[28]	8ι $(5\iota + 3\iota)$	9ι $(6\iota + 3\iota)$	17ι
[29]	8ι $(5\iota + 3\iota)$	12ι $(9\iota + 3\iota)$	20ι
AP	8ι $(3\iota + 5\iota)$	14ι $(8\iota + 6\iota)$	22ι

6.2. Performance Evaluation

To get the accurate performance evaluation, we utilize C programming language to simulate our scheme on a personal computer with the Win8.1 operation system, an Intel(R) Core(TM) i5-5200U CPU @ 2.19GHz, 8G RAM, and a Visual C++ 6.0 testbed.

Figure 4 presents the time cost of executing the new scheme and compared schemes. The horizontal axis indicates the number of recognized tags. The vertical axis indicates the total computation time cost of processing authentication and key agreement phase for each scheme. From the figure, we can see that the consumed time appears to have linear growth as the number of recognized tags increases. The time cost of [9,10] is larger than other schemes for the reason of heavy computation and communication. The consumed time of AP is obviously less than [9,10,28,29]. When the number of recognized tags is 60 and 80, this excellent performance is the most intuitive. Therefore, our scheme is efficient and suitable for the vehicle identification scene.

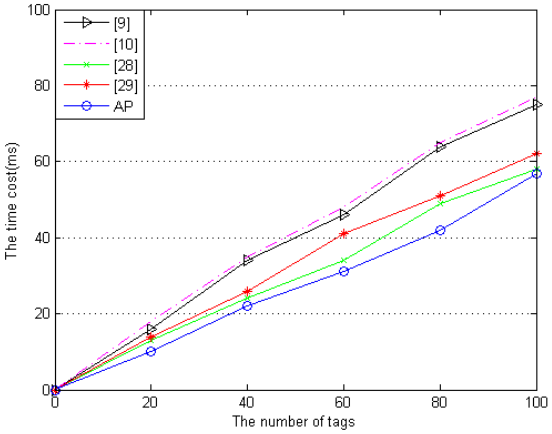

Figure 4. Time cost comparison of these schemes.

7. Conclusions and Future Work

In this paper, we survey some privacy issues of VANETs and discuss the previous work. Then, we put forward an anonymous RFID authentication scheme for VANETs. This scheme can resist different attacks and establish session keys securely. In this scheme, we also exhibit a new retrieval method that permits multiple readers to access different tags in the same authentication scope. Additionally, security analysis proves that secure goals are fulfilled. Finally, the performance comparison shows that our protocol is efficient and suitable for the limited tags. However, there is a limitation that must be discussed in the next work. The limitation is that the proposed retrieval method has to be implemented on a trusted server or third party. Otherwise, an adversary may collude with a semi-trusted party to confirm and steal private information through some corrupted readers. Though our scheme can resist the lost reader attack, the values stored in the lost reader are still a threat before the lost reader is nullified. So, in future work, we have to design a mechanism to avoid the collusion attack and value leakage under a semi-trusted server.

Author Contributions: Conceptualization, formal analysis, methodology, writing—original draft, S.L.; supervision, S.J., C.W., R.Q. and J.S.; writing—review & editing, C.W., J.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China under Grants No. U1836115, No. 61672295, No. 61922045, No. 61672290, No. 61877034, the Natural Science Foundation of Jiangsu Province under Grant No. BK20181408, the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004, the 2020 Research Innovation Program for Postgraduates of Jiangsu Province under No. KYCX20-0936, KYCX20-0972, the CICAEET fund, and the PAPD fund.

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

References

1. Chen, D.; Zhang, N.; Qin, Z.; Mao, X.; Qin, Z.; Shen, X.; Li, X. S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol. *IEEE Internet Things J.* **2017**, *4*, 88–100. [CrossRef]
2. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
3. Tan, C.C.; Sheng, B.; Li, Q. Secure and Serverless RFID Authentication and Search Protocols. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 1400–1407. [CrossRef]
4. Zhou, Z.; Wang, P.; Li, Z. A quadratic residue-based RFID authentication protocol with enhanced security for TMIS. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 3603–3615. [CrossRef]
5. Fatty, M.S.; Ruhul, A. A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS. *Inf. Sci.* **2020**, *527*, 382–393.

6. Prosanta, G.; Amin, R.; Hafizul, S.; Neeraj, K.; Vinod, K.B. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Gener. Comput. Syst.* **2018**, *83*, 629–637.
7. Boursianis, A.; Samaras, T.; Polycarpou, A.; Sahalos, J. A UHF RFID reader antenna for searching tagged items. In Proceedings of the 2014 IEEE RFID Technology and Applications Conference (RFID-TA), Tampere, Finland, 8–9 September 2014; pp. 193–198.
8. Guo, Z.; Ngai, E.; Yang, C.; Liang, X. An RFID-based intelligent decision support system architecture for production monitoring and scheduling in a distributed manufacturing environment. *Int. J. Prod. Econ.* **2015**, *159*, 16–28. [CrossRef]
9. Xie, W.; Xie, L.; Zhang, C.; Zhang, Q.; Tang, C. Cloud-based RFID authentication. In Proceedings of the 2013 IEEE International Conference on RFID (RFID), Penang, Malaysia, 30 April–2 May 2013; pp. 168–175.
10. Fan, K.; Jiang, W.; Li, H.; Yang, Y. Lightweight RFID Protocol for Medical Privacy Protection in IoT. *IEEE Trans. Ind. Inform.* **2018**, *14*, 1656–1665. [CrossRef]
11. Sharma, S.; Kaul, A. VANETs Cloud: Architecture, Applications, Challenges, and Issues. *Arch. Comput. Meth. Eng.* **2020**, 1–22. [CrossRef]
12. Burrows, M.; Abadi, M.; Needham, R. A Logic of Authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]
13. Fuad, A.G.; Anazida, Z.; Mohd, A.M.; Murad, A.R.; Faisal, S. Detecting Bogus Information Attack in Vehicular Ad Hoc Network: A Context-Aware Approach. *Procedia Comput. Sci.* **2019**, *163*, 180–189.
14. Lu, Z.; Qu, G.; Liu, Z. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. *IEEE Trans. Intell. Transp. Syst.* **2019**, *70*, 760–776. [CrossRef]
15. Tangade, S.; Manvi, S.S.; Pascal, L. Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5232–5243. [CrossRef]
16. Manik, L.D.; Pardeep, K.; Andrew, M. Secure and Privacy-Preserving RFID Authentication Scheme for Internet of Things Applications. *Wirel. Pers. Commun.* **2020**, *110*, 339–353.
17. Ding, K.; Jiang, P.; Su, S. RFID-enabled social manufacturing system for inter-enterprise monitoring and dispatching of integrated production and transportation tasks. *Robot. Comput. Integr. Manuf.* **2018**, *49*, 120–133. [CrossRef]
18. Jiang, Q.; Ni, J.; Ma, J.; Yang, L.; Shen, X. Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing. *IEEE Netw.* **2018**, *32*, 28–35. [CrossRef]
19. Fan, K.; Jiang, W.; Luo, Q.; Li, H.; Yang, Y. Cloud-based RFID mutual authentication scheme for efficient privacy preserving in IoV. *J. Frankl. Inst.* **2019**. [CrossRef]
20. Pedro, P.L.; Agustin, O.; Mitrokotsa, A.; Lubbe, J. A comprehensive RFID solution to enhance inpatient medication safety. *Int. J. Med. Inform.* **2011**, *80*, 13–24.
21. Liu, H.; Ning, H.; Zhang, Y.; He, D.; Xiong, Q.; Yang, L.T. Grouping-proofs-based authentication protocol for distributed RFID systems. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *24*, 1321–1330. [CrossRef]
22. Sun, H.M.; Ting, W.C.; Wang, K.H. On the security of Chien's ultralightweight RFID authentication protocol. *IEEE Trans. Dependable Secur. Comput.* **2009**, *8*, 315–317. [CrossRef]
23. Tian, Y.; Chen, G.L.; Li, J.H. A New Ultralightweight RFID Authentication Protocol with Permutation. *IEEE Commun. Lett.* **2012**, *16*, 702–705. [CrossRef]
24. Li, N.; Mu, Y.; Susilo, W.; Guo, F.; Varadharajan, V. Privacy-preserving authorized RFID authentication protocols. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues*; Springer: Cham, Switzerland, 2015; pp. 108–122.
25. Song, B.; Mitchell, C.J. RFID authentication protocol for low-cost tags. In Proceedings of the First ACM Conference on Wireless Network Security, Alexandria, VA, USA, 31 March–2 April 2008; pp. 140–147.
26. Chou, J.S. An efficient mutual authentication RFID scheme based on elliptic curve cryptography. *J. Supercomput.* **2014**, *70*, 75–94. [CrossRef]
27. Zhang, Z.; Qi, Q. An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *J. Med. Syst.* **2014**, *38*, 47–54. [CrossRef] [PubMed]
28. Abughazalah, S.; Markantonakis, K.; Mayes, K. Secure improved cloud-based RFID authentication protocol. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*; Springer: Cham, Switzerland, 2014; pp. 147–164.

29. Xiao, H.; Alshehri, A.A.; Christianson, B. A cloud-based RFID authentication protocol with insecure communication channels. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 332–339.
30. Chien, H.Y.; Chen, C.H. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Comput. Stand. Interfaces* **2007**, *29*, 254–259. [CrossRef]
31. Fan, K.; Gong, Y.; Liang, C.; Li, H.; Yang, Y. Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. *Secur. Commun. Netw.* **2016**, *9*, 3095–3104. [CrossRef]
32. Aghili, S.F.; Mala, H.; Kaliyar, P.; Conti, M. SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. *Future Gener. Comput. Syst.* **2019**, *101*, 621–634. [CrossRef]
33. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
34. Kuseler, T.; Lami, I.A. Using geographical location as an authentication factor to enhance mCommerce applications on smartphones. *Int. J. Comput. Sci. Secur. (IJCSS)* **2012**, *6*, 277–287.
35. Odelu, V.; Das, A.K.; Goswami, A. A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1953–1966. [CrossRef]
36. Wang, D.; Wang, P. Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 708–722. [CrossRef]
37. Zhang, J.; Zhang, F.T.; Huang, X.; Liu, X. Leakage-Resilient Authenticated Key Exchange for Edge Artificial Intelligence. *IEEE Trans. Dependable Secur. Comput.* **2020**. [CrossRef]
38. Dziembowski, S.; Faust, S. Leakage-Resilient Cryptography from the Inner-Product Extractor. In *Advances in Cryptology—ASIACRYPT 2011*; Lee, D.H., Wang, X., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 702–721.