

Article

Secure Cooperative Routing in Wireless Sensor Networks

Rida Batool ¹, Nargis Bibi ^{1,*} , Samah Alhazmi ^{2,*}  and Nazeer Muhammad ³ ¹ Department of Computer Science, Fatima Jinnah Women University, The Mall, Rawalpindi 44000, Pakistan² Computer Science Department, College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia³ School of Computing Sciences, Pak-Austria Fachhochschule Institute of Applied Sciences and Technology, Haripur 22621, Pakistan

* Correspondence: nargis@fjwu.edu.pk (N.B.); s.alhazmi@seu.edu.sa (S.A.)

Abstract: In wireless sensor networks (WSNs), sensor nodes are randomly distributed to transmit sensed data packets to the base station periodically. These sensor nodes, because of constrained battery power and storage space, cannot utilize conventional security measures. The widely held challenging issues for the network layer of WSNs are the packet-dropping attacks, mainly sinkhole and wormhole attacks, which focus on the routing pattern of the protocol. This thesis presents an improved version of the second level of the guard to the system, intrusion detection systems (IDSs), to limit the hostile impact of these attacks in a Low Energy Adaptive Clustering Hierarchy (LEACH) environment. The proposed system named multipath intrusion detection system (MIDS) integrates an IDS with ad hoc on-demand Multipath Distance Vector (AOMDV) protocol. The IDS agent uses the number of packets transmitted and received to calculate intrusion ratio (IR), which helps to mitigate sinkhole attacks and from AOMDV protocol round trip time (RTT) is computed by taking the difference between route request and route reply time to mitigate wormhole attack. MATLAB simulation results show that this cooperative model is an effective technique due to the higher packet delivery ratio (PDR), throughput, and detection accuracy. The proposed MIDS algorithm is proven to be more efficient when compared with an existing LEACH-based IDS system and MS-LEACH in terms of overall energy consumption, lifetime, and throughput of the network.

Keywords: wireless sensor networks (WSNs); intrusion detection systems (IDSs); low energy adaptive clustering hierarchy (LEACH); ad hoc on-demand multipath distance vector (AOMDV); sinkhole attacks; wormhole attacks



Citation: Batool, R.; Bibi, N.; Alhazmi, S.; Muhammad, N. Secure Cooperative Routing in Wireless Sensor Networks. *Appl. Sci.* **2024**, *14*, 5220. <https://doi.org/10.3390/app14125220>

Academic Editor: Alessandro Lo Schiavo

Received: 26 April 2024

Revised: 31 May 2024

Accepted: 13 June 2024

Published: 16 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Wireless sensor systems (WSNs) have encountered breathtaking development in recent years due to decreasing costs and a wide range of applications. In a WSN, a large number of sensor nodes are installed for gathering information from a monitored environment and transmitting it using the wireless medium to the base station [1]. Despite their advantages, WSNs face unique challenges such as limited storage, energy constraints, and high node density, which distinguish them from other wireless networks [2].

The security issues become more critical when the WSNs are deployed in a remote or threatening environment where sensors are vulnerable to failures [3,4]. This paper focuses on the security issues in the network layer, specifically on routing attacks that compromise data integrity, confidentiality, and network availability [5,6].

Generally, secure routing protocols are crucial for secure data transmission and network availability, as shown in Figure 1 [7]. The primary challenge in WSNs is the vulnerability of security protocols to various attacks, particularly sinkhole and wormhole attacks. These attacks can lead to serious consequences such as data tampering, unauthorized data access, and the disruption of network services [8,9].

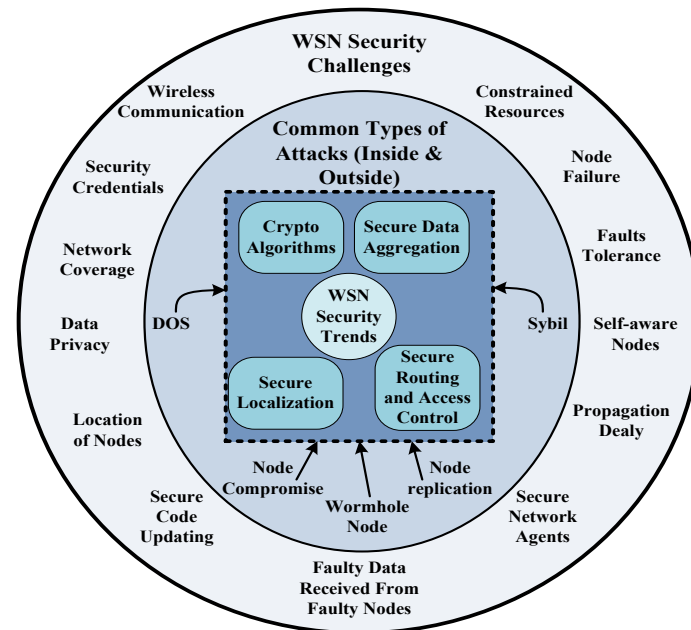


Figure 1. WSN security trends [7].

Previous studies have proposed various security mechanisms, but many suffer from high computational complexity and increased communication overhead [10]. Low-level security mechanisms, including cryptography, secure key encryption, and hash functions, provide protection but often need security primitives, for example, security keys. A key management system (KMS) is used for the creation and distribution of keys, consequently developing a protected key network [11,12]. The security protocols designed for sensor networks must take into account node failure and malicious activities as a feature of their basic functionality [13]. Complex or high-level security schemes, like intrusion detection systems (IDSs), offer enhanced protection by identifying and responding to malicious attacks within the network [14–17].

This section presents the related studies that proposed bi-level techniques for both sinkhole and wormhole attacks [18,19]. A leader-based sinkhole detection approach is proposed by [20]. It has an IDS agent with a counter that identifies the frequency visited by the agent. The counter value will be uploaded when an agent scatters the node. The counter value is refreshed if two agents are found with the same counter value. A swarm intelligence-based approach is proposed in [21] to identify sinkhole hubs in WSNs. Sinkhole detection involves a rule set and a node's ID. The value of energy is -1 if the ID of the routing parcel is smaller than that stored in the ruleset of the equated node; otherwise, the energy value is $+1$. To detect a sinkhole node, a technique based on hop count is proposed by [22]. Nodes in the network have their neighbor's record, including IDs and hop count. A hub node launches a sorting algorithm individually and computes the average number of hops. If the difference between the lowest and the average hop count is larger than the threshold, the particular hub is considered a sinkhole. WRHT, a hybrid technique for wormhole detection, is proposed by [4], which considers time delay probability per-hop (TDPH) and packet loss probability per-hop (PLPH). From the decisions of both the above probabilities, wormhole presence probabilities are calculated on the established route.

Ref. [23] proposed a key encryption technique that splits the network into areas and uses mobile agents (MAs) to preserve energy by keeping it safe from intruders. Visiting Center Local (VCL) partitioned the network into sectors. When the sectors are created, the base station generates a key and shares it among the sensor nodes of the same sectors for securing the network. The use of a key will make the first injection of malicious nodes ineffective. Ref. [24] proposed a weight hop-based packet scheduling scheme, namely the starvation mitigation algorithm (SMA), for networks using the AODV protocol. In this

algorithm, dynamic source routing (DSR) route discovery is done. Some of the previously proposed algorithms identify and isolate intruders based on neighbor-changing frequency and distance between nodes [25–27]. These protocols have heavy implementation and compromise the parameter of detection accuracy due to their high computational complexity.

Techniques using mobile cluster heads and leaders [20,23,28] to analyze the traffic and identify the attackers have a strong verification mechanism, but generally, the communication overhead increases in these types of mechanisms. This communication overhead increases latency and packet delivery ratio. Some multipath routing protocols are also observed [24,27,29–31]. These protocols show high detection accuracy and less resource consumption.

As they are multipath, they are cooperative and deal mostly with cooperative attacks like wormhole attacks. Several among them use the second level of the guard to the system, intrusion detection systems (IDSs) [21,32,33], in which the presence of threats alerts the system. Until now, the IDS mechanisms have low computational overhead, high energy efficiency, and high true positive rates but are unable to isolate attacks with different natures and discover multiple paths to mitigate link failure.

The primary objective of this research work is to develop a hybrid technique by integrating a multipath IDS (intrusion detection system) routing mechanism and a LEACH-based technique to effectively counter sinkhole and wormhole attacks, caused by a single node or multiple nodes, in an energy-efficient way, enhancing the lifetime of the network.

2. Materials and Methods

2.1. System Design and Problem Formulation

This research work innovatively merges AOMDV routing, which has the features of multipath routing, and LEACH protocol, capitalizing on their respective strengths to address routing attacks, such as sinkhole and wormhole attacks in WSNs. This integration offers a comprehensive solution that improves network resilience and adaptability, making a significant contribution to WSN performance and security. The security of the routing process is achieved through several key features such as cluster head (CH) selection and intrusion detection, multipath routing and round-trip time (RTT) monitoring, and non-cryptographic resource-efficient approach. By combining these techniques, the MIDS algorithm ensures secure, efficient, and reliable data routing in WSNs, effectively handling common routing attacks while maintaining high detection accuracy and resource efficiency.

In this research work, a wireless sensor network is deployed with “N = 200” sensor nodes. This network incorporates the criteria of first node die (FND), with the values of “0” and “1”. In this process of FND, if the value is 1, it means the algorithm will stop whenever there exists a dead node with an energy value less than the predefined threshold which is “0.01 J”. If the value is “0”, it will count the dead nodes in the further processing and the algorithm will not stop based on any dead node. The network is deployed on a simulation area of $100 \times 100 \text{ m}^2$. Anchor-based distance calculation is done by considering “4” anchor nodes.

The AODV protocol is used as an underlying protocol. The proposed version of the IDS mechanism is known as a multipath intrusion detection system (MIDS). As the name depicts, this MIDS also facilitates multipath routing in the case of main path failure using the AOMDV protocol along with minimizing the adverse effects of both attacks. The proposed multipath intrusion detection system (MIDS) assumes the following:

- The base station has the highest energy resource.
- The malicious nodes show energy levels higher than the normal sensor nodes.
- The network possesses the initial energy of 1 J.
- This algorithm does not require any clock synchronization.

2.2. Mathematical Model for MIDS Algorithm

To verify the effectiveness of the algorithm, a simple mathematical model is constructed. In this deployment, distance “D” between the estimated location of nodes in the coordinates system is calculated using the distance formula:

$$D = \sqrt{((x_2 - x_1) + (y_2 - y_1))^2} \quad (1)$$

The energy model used in the communication phase is adopted from [34]. To transmit “1” bit data packets to and from distance “d”, the energy used is calculated by using Equations (2) and (3), respectively.

$$E_{Tx}(l, d) = \begin{cases} (l e_{elec} + \varepsilon_{fs} \times d^2), & \text{if } d \leq d_{th} \\ (l e_{elec} + \varepsilon_{amp} \times d^4), & \text{if } d > d_{th} \end{cases} \quad (2)$$

$$E_{Rx}(l) = l \times e_{elec} \quad (3)$$

Here free space (d^2) and multipath fading (d^4) are engaged. The amplification factors are ε_{fs} and ε_{amp} for these two models, respectively. Signal processing energy consumption is denoted by “ e_{elec} ”.

Using FCM in the first round based on the nodes’ location and layer information, the network is divided into nodes which are grouped into different clusters. The main objective of the FCM is to minimize the objective function “O” given below in Equation (4).

$$O(\alpha, \beta) = \sum_{i=1}^n \sum_{k=1}^c (\alpha_{ij})_m = \|x_i - \beta_j\|^2 \quad (4)$$

where “ α_{ij} ” represents the membership of the node at “i” to the cluster center at the position “j” and the cluster center at the jth position is denoted by “ β_j ”.

The packets received R_i and packets transmitted T_i values of a CH(H_i) are processed by the IDS agent in the BS. The IDS agent has a ratio gauge which calculates the intrusion ratio (IR). The formula for the intrusion ratio is given below in Equation (5).

$$IR_i = R_i / T_i \quad (5)$$

where R_i are the packets received and T_i are the packets transmitted values of a CH(H_i). The RTT (round trip time) is calculated by using Equation (6).

$$RTT = t_{2_i} - t_1 \quad (6)$$

where t_1 is the route request time by the sender and t_{2_i} is the route reply time by the receiver.

2.3. Detection of Sinkhole and Wormhole Attack Using MIDS Algorithm

In the deployed LEACH-based network, CHs receive data from the sensor nodes which, for final processing, are transferred to the base station (BS). BS has an IDS agent which analyzes the information received by the BS. A simple mathematical model for the verification of the effectiveness of the algorithm is presented. The network comprises uniformly distributed four anchor nodes, strategically positioned at the perimeter of the simulation area and randomly deployed 196 non-anchor nodes (N_1, N_2). Clusters formed from fuzzy c-mean clustering are denoted by C_i . The H_i is the CH of a certain cluster C_i . The packets received R_i and packets transmitted T_i values of a CH(H_i) are processed by the IDS agent in the BS. The IDS agent has a ratio gauge which calculates the intrusion ratio (IR). From the value received from the IR, the IDS agent decides the malicious activity. IR can take any of the two values: infinity or any numeric value n:

$$IR_i = \{\text{infinity: } H_i \text{ is malicious ; } n: H_i \text{ is a normal node}\} \quad (7)$$

The underlying AOMDV protocol keeps a record of the routing table entries used by the sender node. It checks in the routing table whether a route is available or not for communication. If the route is found, it gives the information; otherwise, it broadcasts the RREQ parcel to its neighbors which then checks whether a route is available to the necessary goal or not. When the sender node transmits the RREQ, it will note the time t_1 . At whatever point the receiver gets the RREQ bundle, it sends the RREP parcel to the source along a similar way through which the RREQ parcel has shown up. Time t_{2_i} is noted for each route reply by the sender node.

Then, the sender node takes the RTT ($t_{3_i} = t_{2_i} - t_1$) value from each path and divides this value with the hop count of each respective route. The obtained value is termed as ts_i . The average RTT is calculated with the help of this value ts_i . Now, the calculated value is the threshold (tht) RTT. From the comparison of tht and ts_i , it is found that if ts_i is very minimal, also the hop count of the certain path is 2, then the route is detected as a wormhole link and is jammed for further communication. The sender node detects the first neighbor as malicious and sends a dummy request to it and the receiver receives this dummy request through its first neighbor and detects this node as malicious. In this way, both nodes are eliminated, and routing table entries are updated throughout the network.

2.4. Simulation Parameters

Simulations for the proposed MIDS are simulated using MATLAB R2023b. A WSN is built through deploying “200” sensor nodes in the “ $100 \times 100 \text{ m}^2$ ” simulation area. BS is placed at the center of the WSN which is reflected as the optimal placement for the efficient use of energy. Out of “200” sensor nodes, “4” nodes are positioned as anchor nodes for effective localization, and the rest “196” are non-anchor sensor nodes. Initially, the network has the energy of “1 J”. Some parameters that are used during the simulation process of the proposed MIDS algorithm with their values are shown in Table 1 and Figure 2.

Table 1. Simulation parameters and values.

Parameters	Values
Simulation Area	$100 \times 100 \text{ m}^2$
Sensor Nodes	200
Initial Energy (I_e)	1 J
Simulation Time	306.0459 s
Termination Threshold ($E_{TH} = 0.02$)	$\text{mean}(I_e) < N \times ETH \text{ J}$
Termination Threshold (For First Node Die)	0.01 J
ϵ_{fs}	10 pJ/bit/m ²
ϵ_{amp}	0.0013 pJ/bit/m ⁴
Length of Data	5000 bits
e_r, e_t	50 nJ
d_o	87.7 m
Anchor Nodes	4
Non-anchor Nodes	196

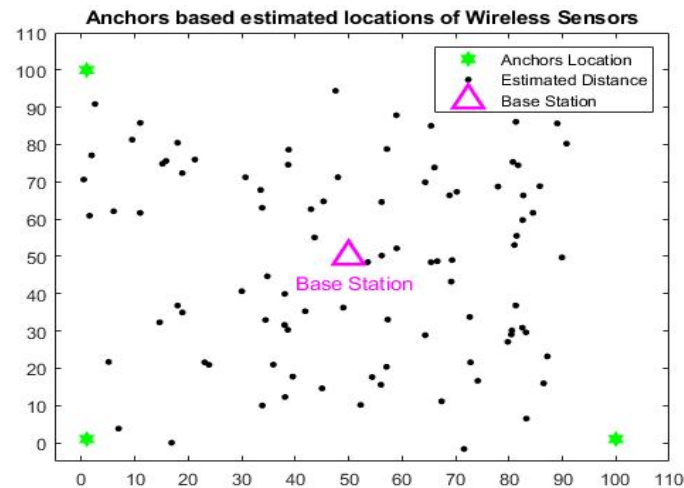


Figure 2. Anchor-based location estimation.

3. Results

Simulation Results

The MIDS algorithm performed fuzzy c-mean (FCM) clustering which assigned cluster centers a membership function based on which they can be the part of more than one cluster. Here, the CHs are assumed as hops. The CH of each cluster receives data from its members and then looks for the shortest path for data transmission to the BS. The path which has the shortest number of hops (CHs) from a specific CH to the BS is considered as the optimal path for that particular CH.

The deployed sensor network has “16” clusters. According to the above-mentioned Figure 3, consider the CH (20) whose cluster members send their sensed data towards it. The IR value computed for the CH (20). Suppose the packet received value “ R_i ” of CH (20) is “80”, similarly the packets transmitted value “ T_i ” is “0”. The IR value is calculated as “ $IR = 80/0 = \infty$ ”; hence, CH (20) is a sinkhole node as indicated in Figure 4 below, and it drops all the packets.

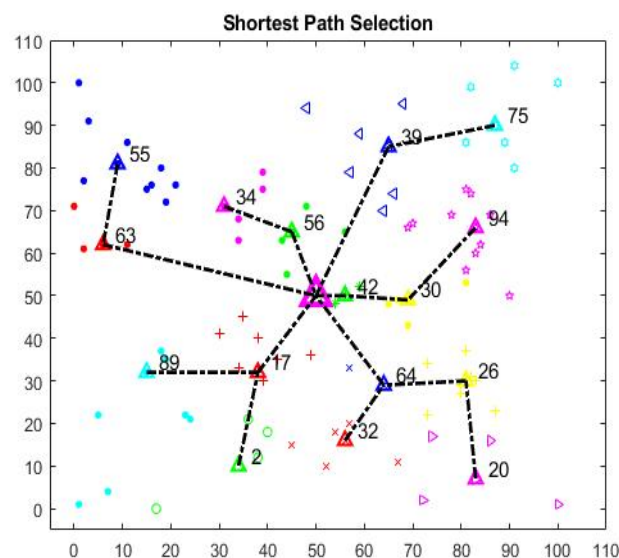


Figure 3. FCM and optimal path selection. Each color shows distinct cluster. Triangle in each cluster is cluster head (CH). Purple triangle in the center is base station.

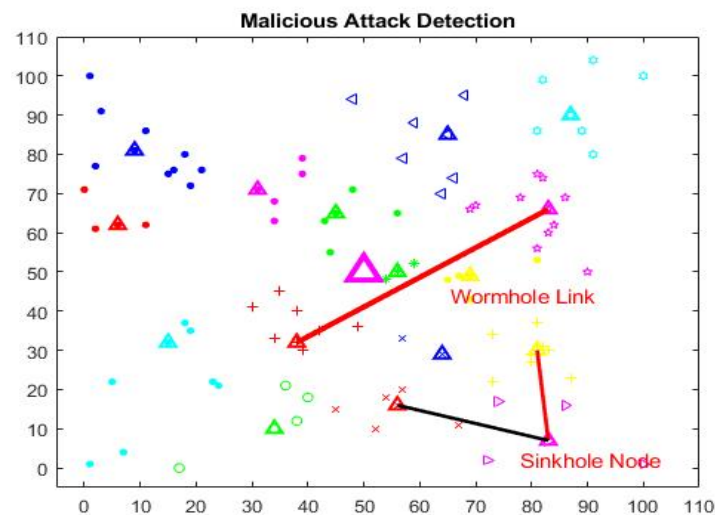


Figure 4. Sinkhole/wormhole detection. Each color shows distinct cluster. Triangle in each cluster is cluster head (CH). purple triangle in the center is base station.

The second case is for wormhole attack detection. In this case, consider that the cluster members of CH (89) delivered sensed data towards it. CH (89) after receiving data from cluster members intends to transmit it to the base station, so it broadcasts a route request and notes the time, let $t_1 = 5$ s, when the RREQ is sent. It receives more than one route replies from the BS, which means that three routes are available to the destination, i.e., $i = 3$. For each route reply RREP, the sender node noted the time. Assume that it receives three replies through CH (94), CH (34), and CH (64), and the time of RREP is $t_{2_1} = 7$ s, $t_{2_2} = 8$ s, and $t_{2_3} = 9$ s, respectively. Then, the RTT for each route is calculated. $T_{3_1} = 7 - 5 = 2$, $t_{3_2} = 8 - 5 = 3$, and $t_{3_3} = 9 - 5 = 4$. Now, the threshold RTT is calculated using the previous values divided by the number of hop counts between the sender (CH (94)) and the receivers (CH (94), CH (34), and CH (64)). The hop count for the first two routes is two and the third route is one. The value of threshold RTT came out to be, $ts_1 = 1$, $ts_2 = 1.5$, and $ts_3 = 4$. Now, take the average of ts_i and the calculated value is $tht = 2.16$. Now, compare the values ts_i with tht . For the first route, $ts_1 = 1 < 2.16$ and the hop count is two. For the second route, the hop count value is two but the $ts_2 = 1.5$ is not less than the tht value.

4. Discussion

4.1. Performance Evaluation Parameters

This section describes the performance evaluation of the proposed MIDS algorithm in terms of the following:

- The number of alive nodes.
- Packet delivery ratio.
- Latency.
- Network throughput.
- Consumed energy during the communication phase.

For the third route, both conditions are false; $ts_3 = 4$ is not less than the tht and the hop count is one. Hence, the first route is fulfilling the criteria for a malicious node. So, CH (89) detects the first neighbor CH (17) as a wormhole and sends a dummy RREQ to it on the first route; the receiver will receive that dummy request from the CH (94) on the same route so the receiver will detect the CH (94) as the wormhole node. Both these nodes will be isolated, and an alarm will be generated for the other nodes to update their routing entries eliminating these nodes. So, basically, CH (17) and CH (94) were forming a tunnel and accessing the sensitive information of the network.

4.1.1. Number of Alive Nodes

The size of the network is 200 nodes. Figure 5 shows the quantity of alive nodes with the section of rounds that has appeared. Alive node's recurrence is straightforwardly relative to the estimation of energy. As the energy diminishes, the quantity of alive nodes decreases. Hence, the system's lifetime diminishes.

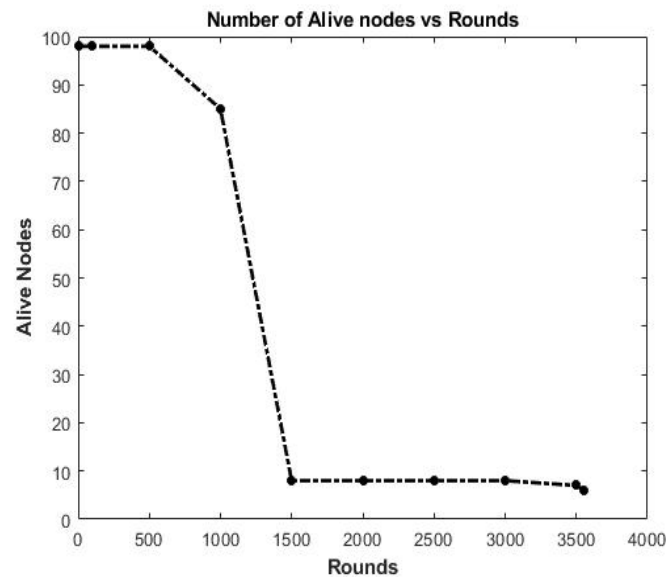


Figure 5. Alive nodes of the network vs. rounds.

In this calculation, up to the 500th round, none of the nodes completely lost its energy and had an energy level higher than the threshold energy “0.01” and consequently stayed alive after that as the round increment nodes started depleting energy even after the proposed MIDS algorithm productively finished its 3500th rounds.

4.1.2. Packet Delivery Ratio (PDR)

In the proposed MIDS algorithm, PDR is anticipated based on the data packets produced and packets got according to the record of each node. It has a quantitative relationship between the data packets produced by the source node and those received at the destination node.

In Figure 6 PDR is plotted on the “X-pivot” and rounds are plotted on the “Y-pivot”. Toward the beginning when the sensors are completely dynamic and in their most elevated energy structure, PDR is higher up to the 500th round. After that, as the energy utilization begins expanding, the nodes turn out to be dead which slows the procedure of packet conveyance. Be that as it may, it does not fully disappear up to the 35,000th round. At the point when the all-out energy of the network dips under the edge esteem, the PDR becomes “0”.

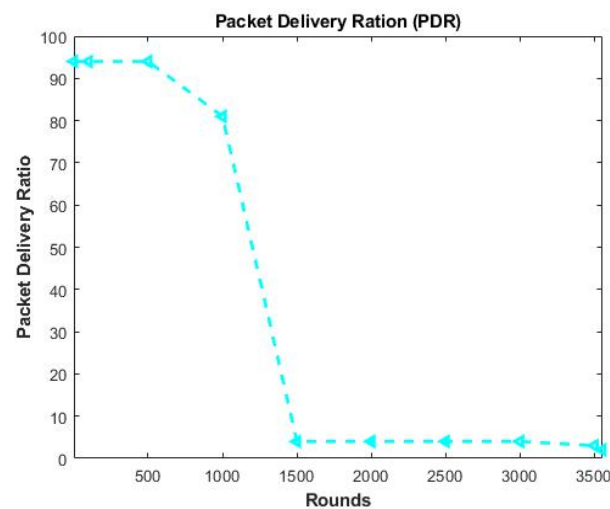


Figure 6. Packet delivery ratio with rounds.

4.1.3. Latency

Latency is a deferral of time between the source and the destination of the physical change in the framework being analyzed, or it delineates the time length between the response and simulation. In this research to avoid energy loss.

Figure 7 represents that latency is higher at the beginning of the algorithm as the number of nodes participating is higher, as it is an expression of how much time MIDS takes for a packet to reach its destination after being sent. When the network size is larger till the 10th round, the latency value is almost “5 ms” but it suddenly drops till the 1000th round to “0 ms”. Though the network size does not decrease much, the MIDS algorithm decreases latency value comparatively by the efficient usage of routes.

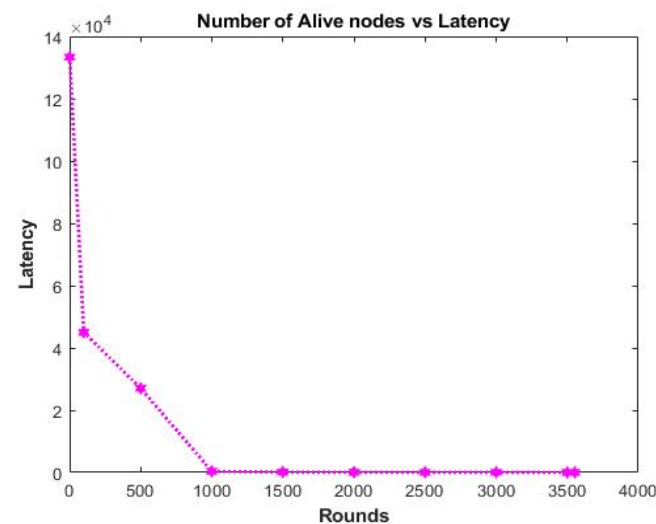


Figure 7. Latency with rounds.

4.1.4. Throughput

Throughput characterizes the quantity of data handled within the given time or transmitted from one location to another. To examine the overall throughput of the algorithm, it is also compared with the size of the network as shown in Figure 8. The number of nodes participating in the activity at the launch of algorithm throughput is lower due to communication overhead. More number of packets start reaching their destination as the size of the network decreases with the passage of rounds.

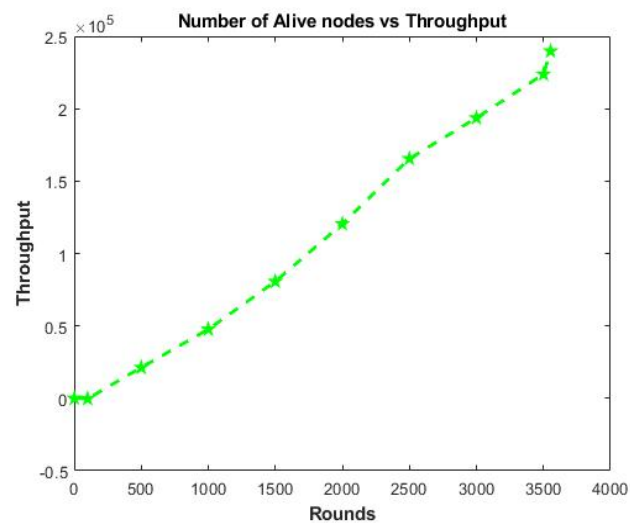


Figure 8. Throughput with rounds.

4.1.5. Consumed Energy during Communication Phase

The proposed MIDS system loses a particular estimation of energy for every correspondence round. Figure 9 shows when the correspondence started, till the 1000th round, the remaining energy line dropped straightly up to 20 J. Then, until the 1500th round, there occurred a 10 J decrease in energy. After that, the energy value line stood almost steady in the coming rounds till the end limit came.

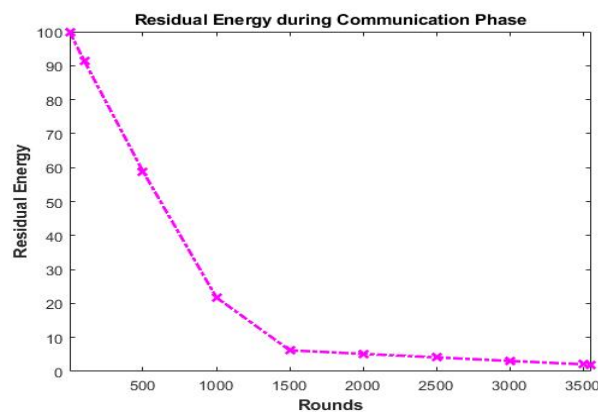


Figure 9. Residual energy during communication phase.

4.2. Comparative Analysis

For performance comparison of the proposed MIDS, an existing LEACH-based IDS is chosen. Another technique is that MS-LEACH is chosen for comparative analysis. The LEACH-based IDS mechanism adapts a physical division-wise clustering approach and detects forwarding attacks. MS-LEACH adapts a key-based cryptographic approach. Both these techniques outperform their ancestor techniques in terms of overall

- Network energy consumption.
- Network throughput.
- Network lifetime.

The proposed MIDS is also compared with the chosen techniques based on these three parameters. The decision to keep energy consumption, network lifetime, and throughput aligns with the similar simulation parameters used by the LEACH-based IDS and MS-LEACH techniques for comparison. By maintaining consistent parameters, we ensure a fair and accurate evaluation of performance across different algorithms. This approach

allows us to directly compare metrics such as energy consumption, network lifetime, and throughput without introducing variability that could arise from changing the number of sensor nodes. It provides a controlled environment to validate the effectiveness and efficiency of the MIDS algorithm relative to the established techniques. The detail of the results is given below.

4.2.1. Network Energy Consumption

For MS-LEACH, when the nodes are less, almost 30% the energy consumption is around 95%. With the increase in the number of nodes, the energy consumption process increases and comes closer to the extreme value which is 100%, as shown in Figure 5. The blue dotted line is a reference paper technique which is the LEACH-based IDS mechanism, and the extreme energy consumption value for this is also 100%. The proposed MIDS has 43% less energy consumption with a change in the size of the network.

The efficient use of energy by the BS makes the proposed algorithm use less energy. The fuzzy c-mean clustering algorithm decides the best possible nodes as CHs which also helps in the minimal use of power by the sensor nodes. Also, the AOMDV mechanism helps in minimal energy consumption by selecting the optimal and secure path for packet transmission.

The MIDS algorithm keeps track of each node, and as soon as it finds an adversary, it generates an alarm and isolates that node. This quick response mechanism helps in the minimal loss of energy by the attacker nodes. In Figure 10, at the start, the energy consumption of MIDS is as low as 35%, but with the increase in the size of the network it starts increasing but the extreme value for this algorithm is not more than 55%.

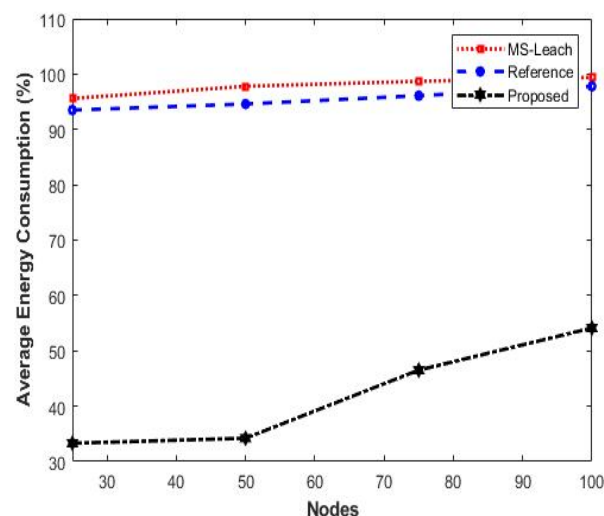


Figure 10. Average energy consumption.

4.2.2. Throughput of the Network

Average network throughput is a significant metric in this comparison as our MIDS algorithms deal with the packet-dropping attacks. Figure 11 shows the comparison of all three techniques based on average network throughput. MS-LEACH has the worst average network throughput among all. The cryptographic key management process takes a very large amount of time process and causes high communication overhead on both the sender and receiver side. The attacker recognition process is slower in cryptographic key management mechanisms. Hence, the packet delivery ratio is much less in these mechanisms.

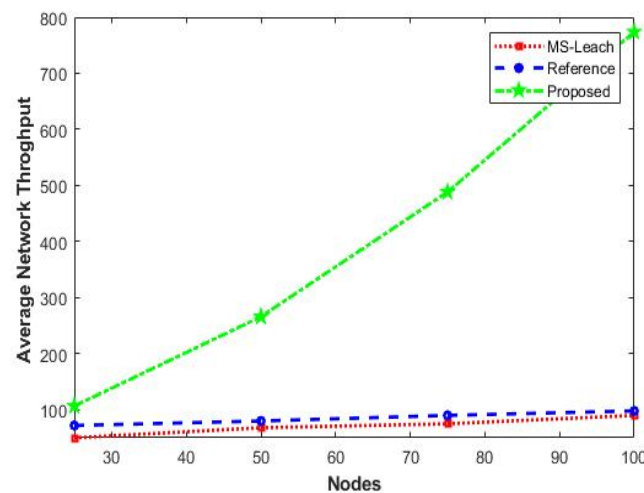


Figure 11. Throughput of the network.

The reference technique deals with only one packet-dropping attack. Also, it lacks a secure CH selection technique which makes it more vulnerable to attacks. Hence, when more prone to packet-dropping attacks the average throughput of the network decreases.

The throughput of the network increases by 65% when the MIDS algorithm is used. The MIDS algorithm has a strong mechanism of CH selection, after that the malicious nodes are efficiently detected and isolated, which increases the packet delivery ratio of the algorithm. A strong IDS mechanism makes it quicker in detecting and preventing malicious nodes. Multipath routing mechanism helps in optimal path selection towards the destination which reduces the time for packet transmission, and in the case of the failure of a link, the alternative path is ready which also makes it more time efficient.

4.2.3. Lifetime of the Network

The comparison of MS-LEACH, LEACH-based IDS mechanism, and the proposed MIDS algorithm for network lifetime is shown in Figure 12. The reference paper has 2% more network lifetime than the MS-LEACH but the performance is not effective. The CH selection process in this algorithm is done randomly where the chances of the attacker node selected as CH are higher. The MS-LEACH algorithm has the worst performance out of all. Due to the cryptographic key mechanism, the nodes have a very high communication overhead which leads to the earlier death of the nodes. The proposed MIDS algorithm has almost 62% more life span than the other two techniques. The MIDS algorithm uses an efficient way of CH selection which makes the network secure and long-lasting. MIDS algorithms, through less energy drain, make the sensor nodes alive for a longer time which extends the network lifetime.

From comparative analysis, it is depicted that the proposed MIDS algorithm has 43% less energy consumption than the other two techniques due to the resourceful selection of the CH mechanism and the launching energy consumption model at each level during the communication phase. After CH selection, the intrusion detection agent actively responds to the attacker node which also avoids energy loss by the attacker. This less energy drain makes the nodes alive which increases the processing rounds and hence the overall lifetime of the network by 62%. Similarly, the average network throughput is increased by 65% through proficiently combating the packet drop attacks as shown in Table 2.

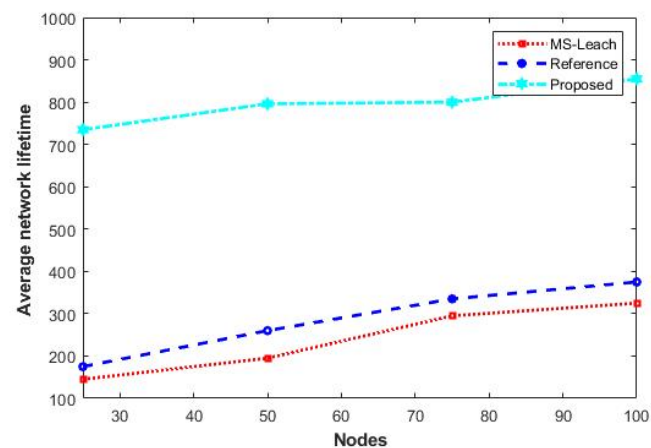


Figure 12. Lifetime of the network.

Table 2. Comparative analysis of results.

Sr #	Technique	Energy Consumption	Lifetime	Throughput
1	MIDS (Proposed)	43% less	62% High	65% High
2	LEACH (Reference)	Medium	Medium	Medium
3	MS LEACH	High	Low	Low

5. Conclusions

In this work, a lightweight non-cryptographic intrusion detection routing protocol is proposed which is named Multipath Intrusion Detection Protocol (MIDS). This MIDS mechanism combats the two main routing attacks of the network layer, which are sinkhole attack and wormhole attack, resourcefully and with less communication overhead. In this work, various existing studies are examined which attempt to deal with sinkhole and wormhole attacks in WSNs.

The comparative analysis of the cooperative MIDS algorithm is done with an existing IDS mechanism and MS-LEACH in relation to overall network energy consumption, lifetime, and throughput. The simulation results show that the overall performance of an IDS mechanism increases when combined with a multipath routing algorithm.

MIDS provides comprehensive security coverage, ensuring robust protection against diverse threats. MIDS is designed to operate within LEACH-based networks, but its flexibility allows for adaptation to various WSN architectures and protocols, enhancing its applicability across different deployment scenarios. It has real-time detection capabilities that enable prompt response to malicious nodes, enhancing network integrity and reliability. Potential application scenarios for MIDS can be environmental monitoring, Industrial IoT (IIoT), smart agriculture, healthcare monitoring, and smart cities.

In the future, the algorithm can be improved to enhance security at a multilayer level by mitigating attacks at other layers. Another scope of research is the optimization of memory size used at each level, i.e., sensor nodes, cluster heads, and base stations, in an IDS mechanism.

Author Contributions: Conceptualization, R.B. and N.B.; methodology, R.B. and N.B.; software, R.B.; validation, R.B., N.B. and S.A.; formal analysis, R.B., N.B., S.A. and N.M.; investigation, R.B., N.B., S.A. and N.M.; resources, R.B.; data curation, R.B.; writing—original draft preparation, R.B., N.B., S.A. and N.M.; writing—review and editing, R.B., N.B., S.A. and N.M.; visualization, R.B., N.B., S.A. and N.M.; supervision, N.B. and S.A.; project administration, N.B. and S.A.; funding acquisition, N.B. and S.A. 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: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Acknowledgments: The authors would like to thank Fatima Jinnah Women University, Saudi Electronic University, and Pak-Austria Fachhochschule Institute of Applied Sciences and Technology.

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

References

1. Gupta, C.; Singh, L.; Tiwari, R. Wormhole attack detection techniques in ad-hoc network: A systematic review. *Open Comput. Sci.* **2022**, *12*, 260–288. [\[CrossRef\]](#)
2. Srinivasan, V. Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET. *Ing. Syst. d'Inf.* **2021**, *26*, 549–557. [\[CrossRef\]](#)
3. Annie, M.; Terence, J.S. A Survey on Various Detection Techniques of Sinkhole Attacks in WSN. In Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, Chennai, India, 6–8 April 2017.
4. Tahboush, M.; Agoyi, M. A hybrid wormhole attack detection in mobile ad-hoc network (MANET). *IEEE Access* **2021**, *9*, 11872–11883. [\[CrossRef\]](#)
5. Jahangeer, A.; Bazai, S.U.; Aslam, S.; Marjan, S.; Anas, M.; Hashemi, S.H. A review on the security of IoT networks: From network layer's perspective. *IEEE Access* **2023**, *11*, 71073–71087. [\[CrossRef\]](#)
6. Godala, S.; Vaddella, R.P.V. A study on intrusion detection system in wireless sensor networks. *Int. J. Commun. Netw. Inf. Secur.* **2020**, *12*, 127–141. [\[CrossRef\]](#)
7. Riad, A.M.; El-Minir, H.K.; El-Hoseny, M. Secure routing in wireless sensor networks: A state of the art. *Int. J. Comput. Appl.* **2013**, *67*, 7–12.
8. Moundounga, A.R.A.; Satori, H.; Boutazart, Y.; Abderrahim, E. Malicious attack detection based on continuous Hidden Markov Models in Wireless sensor networks. *Microprocess. Microsyst.* **2023**, *101*, 104888. [\[CrossRef\]](#)
9. Karthikeyan, B.; Malik, K.A.; Babbu, D.B.; Nithya, K.; Ibrahim, S.J.A.; Chakravarthy, N.K. Survey of Cooperative Routing Algorithms in Wireless Sensor Networks. *Ann. Rom. Soc. Cell Biol.* **2021**, *53*, 16–20.
10. Subbiah, S.; Anbananthen, K.S.M.; Thangaraj, S.; Kannan, S.; Chelliah, D. Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm. *J. Commun. Netw.* **2022**, *24*, 264–273. [\[CrossRef\]](#)
11. Umarani, C.; Kannan, S. Intrusion Detection System Using Hybrid Tissue Growing Algorithm for Wireless Sensor Network. *Peer-to-Peer Netw. Appl.* **2019**, *13*, 752–761. [\[CrossRef\]](#)
12. Raghav, R.S.; Thirugnansambandam, K.; Anguraj, D.K. Beeware Routing Scheme for Detecting Network Layer Attacks in Wireless Sensor Networks. *Wirel. Pers. Commun.* **2020**, *112*, 2439–2459. [\[CrossRef\]](#)
13. Safa, O.; Kantarci, B.; Mouftah, H.T. On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. *IEEE Netw. Lett.* **2019**, *1*, 68–71.
14. Gulati, K.; Boddu, R.S.K.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G. A review paper on wireless sensor network techniques in Internet of Things (IoT). *Mater. Today Proc.* **2022**, *51*, 161–165. [\[CrossRef\]](#)
15. Boubiche, D.E.; Athmani, S.; Boubiche, S.; Toral-Cruz, H. Cybersecurity issues in wireless sensor networks: Current challenges and solutions. *Wirel. Pers. Commun.* **2021**, *117*, 177–213. [\[CrossRef\]](#)
16. Rehman, A.; Rehman, S.; Raheem, S. Sinkhole Attacks in Wireless Sensor Networks: A Survey. *Wirel. Pers. Commun.* **2019**, *106*, 2291–2313. [\[CrossRef\]](#)
17. Keerthika, M.; Shanmugapriya, D. Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. *Glob. Transit. Proc.* **2021**, *2*, 362–367. [\[CrossRef\]](#)
18. Nourildean, S.W.; Hassib, M.D.; Mohammed, Y.A. Internet of things based wireless sensor network: A review. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *27*, 246–261. [\[CrossRef\]](#)
19. Uzougbo, O.I.; Ajibade, S.S.; Taiwo, F. An overview of wireless sensor network security attacks: Mode of operation, severity and mitigation techniques. *arXiv* **2020**, arXiv:2011.06779.
20. Aparnaa, M.; Dhanush Krishna, S.; Amaran, S.; Maheswari, S.; Soundarya, R. An Enhanced Scheme of Excluding Compromised Nodes in Wireless Sensor Networks. *J. Phys.* **2019**, *1362*, 012007. [\[CrossRef\]](#)
21. Al-Nasser, A.; Almesaeed, R.; Al-Junaid, H. A comprehensive survey on routing and security in mobile wireless sensor networks. *Int. J. Electron. Telecommun.* **2021**, *67*, 483–496. [\[CrossRef\]](#)
22. Shanmugaraja, P.; Bhardwaj, M.; Mehbodniya, A.; Vali, S.; Reddy, P.C.S. An Efficient Clustered M-path Sinkhole Attack Detection (MSAD) Algorithm for Wireless Sensor Networks. *Adhoc Sens. Wirel. Netw.* **2023**, *55*, 1–16.
23. Nwankwo, K.E.; Abdulhamid, S.I.M.; Ojeniyi, J.A.; Misra, S.; Oluranti, J.; Ahuja, R. A Panacea to soft computing approach for Sinkhole attack classification in a wireless sensor networks environment. In Proceedings of the Futuristic Trends in Network and Communication Technologies: Third International Conference, FTNCT, Taganrog, Russia, 14–16 October 2020; pp. 78–87.

24. Babaeer, H.A.; Al-Ahmadi, S.A. Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking. *IEEE Access* **2020**, *8*, 92098–92109. [[CrossRef](#)]
25. Hanif, M.; Ashraf, H.; Jalil, Z.; Jhanjhi, N.Z.; Humayun, M.; Saeed, S.; Almuhaideb, A.M. AI-based wormhole attack detection techniques in wireless sensor networks. *Electronics* **2022**, *11*, 2324. [[CrossRef](#)]
26. Zhang, K. A wormhole attack detection method for tactical wireless sensor networks. *PeerJ Comput. Sci.* **2023**, *9*, e1449. [[CrossRef](#)] [[PubMed](#)]
27. Jatti, A.V.; Sonti, V.K. Sinkhole Attack Detection and Prevention Using Agent Based Algorithm. *J. Univ. Shanghai Sci. Technol.* **2021**, *23*, 526–544. [[CrossRef](#)]
28. Alaali, A.M.; Almesaeed, R. Mitigation of Sinkhole Attack in Dynamic Directional Routing for Mobile Wireless Sensor Networks. *Int. J. Comput. Digit. Syst.* **2023**, *14*, 10381–10394. [[CrossRef](#)]
29. Ahutu, O.R.; El-Ocla, H. Centralized routing protocol for detecting wormhole attacks in wireless sensor networks. *IEEE Access* **2020**, *8*, 63270–63282. [[CrossRef](#)]
30. Singh, S.; Saini, H.S. Intelligent ad-hoc-on demand multipath distance vector for wormhole attack in clustered WSN. *Wirel. Pers. Commun.* **2022**, *122*, 1305–1327. [[CrossRef](#)]
31. Kaur, T.; Kumar, R. Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol. In Proceedings of the 6th IEEE International Conference on Smart Energy Grid Engineering, SEGE, Oshawa, ON, Canada, 12–15 August 2018; pp. 288–292.
32. Amish, P.; Vaghela, V.B. Detection and Prevention of Wormhole Attack in Wireless Sensor Network Using AOMDV Protocol. *Procedia Comput. Sci.* **2016**, *79*, 700–707. [[CrossRef](#)]
33. Popli, L.D.R. Sinkhole Attack Detection In MANET Using Swarm Intelligence Techniques. *Int. J. Eng. Appl. Sci. Technol.* **2020**, *5*, 155–160.
34. Kumar, S.R.; Arumugam, U. Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks. *J. Sens.* **2015**, *2015*, 1–12.

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.