Computers, Materials & Continua
DOI:10.32604/cmc.2021.015259
Article

Tech Science Press

Energy Optimised Security against Wormhole Attack in IoT-Based Wireless Sensor Networks

Hafsa Shahid[1], Humaira Ashraf[1], Hafsa Javed[1], Mamoona Humayun[2], Nz Jhanjhi[3,*] and Mohammed A. AlZain[4]

[1]Department of Computer Science and Software Engineering,
International Islamic University Islamabad, Islamabad, Pakistan
[2]Department of Information Systems, College of Computer and Information Science,
Jouf University, Al-Jouf, Saudi Arabia
[3]School of Computer Science and Engineering (SCE), Taylor's University, Selangor, Malaysia
[4]Department of Information Technology, College of Computers and Information Technology,
Taif University, Taif, 21944, Saudi Arabia
[*]Corresponding Author: Nz Jhanjhi. Email: noorzaman.jhanjhi@taylors.edu.my
Received: 12 November 2020; Accepted: 23 February 2021

Abstract: An IoT-based wireless sensor network (WSN) comprises many small sensors to collect the data and share it with the central repositories. These sensors are battery-driven and resource-restrained devices that consume most of the energy in sensing or collecting the data and transmitting it. During data sharing, security is an important concern in such networks as they are prone to many threats, of which the deadliest is the wormhole attack. These attacks are launched without acquiring the vital information of the network and they highly compromise the communication, security, and performance of the network. In the IoT-based network environment, its mitigation becomes more challenging because of the low resource availability in the sensing devices. We have performed an extensive literature study of the existing techniques against the wormhole attack and categorised them according to their methodology. The analysis of literature has motivated our research. In this paper, we developed the ESWI technique for detecting the wormhole attack while improving the performance and security. This algorithm has been designed to be simple and less complicated to avoid the overheads and the drainage of energy in its operation. The simulation results of our technique show competitive results for the detection rate and packet delivery ratio. It also gives an increased throughput, a decreased end-to-end delay, and a much-reduced consumption of energy.

Keywords: IoT; Internet of Things; energy; wormhole; WSN; wireless sensor networks

1 Introduction

WSNs are one of the most advanced technologies in the present world. These networks have enabled many possibilities such as modern and satellite telecommunication, space communication,

military systems, and underwater networks. This technology is also used in traffic monitoring, weather monitoring, fire detection, forest monitoring, smart homes, and the Internet of Things (IoT).

The IoT networks follow the basic WSN architecture [1], as shown in Fig. 1a. IoT is a fast-growing field due to its high applicability in everyday life, as shown in Fig. 1b. Some of its most important applications are traffic monitoring, healthcare services, energy-saving smart grid-stations, fleet management, agriculture, water supply, and home security systems.

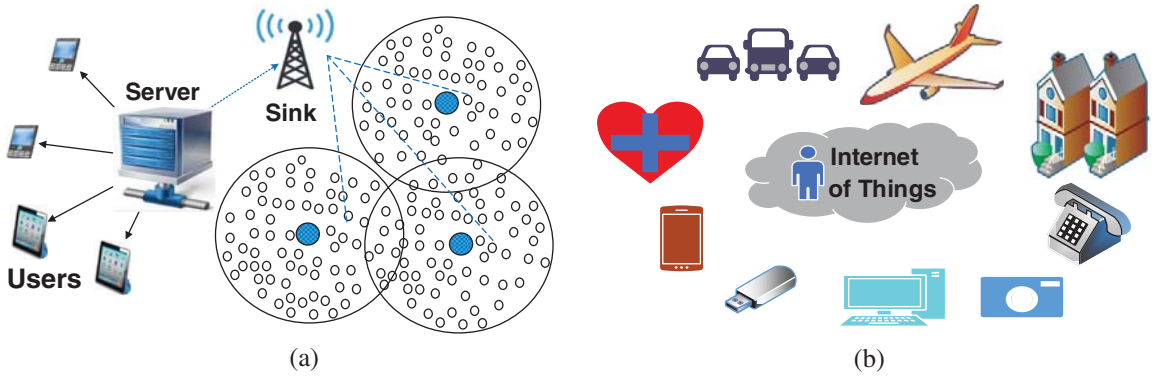

Figure 1: (a) WSN architecture (b) Internet of Things

Security is a major concern due to the decentralised nature of WSNs. These networks are prone to many security attacks based on node capture and node hacking, leading to the compromise of data and security. IoT networks are comprised of sensor-based networks; therefore, the threats posed to the WSNs are equally dangerous and applicable to the IoT networks. One of the most severe threats is the wormhole attack [2]. This attack is most easily launched as no legitimate nodes from the network are compromised and no shared key is required by the attacker. This attack can affect the system on different levels depending on the type of attack and the area of the network in which it is launched. If the attack is launched in the localisation protocol, it misguides the system about the node's location by transmitting false coordinates; if it is launched in the routing protocol, this attack leads to the compromise of data security.

Wormhole attacks are launched in two ways, internally and externally. In an internal wormhole attack, the attacker is a part of the system and a virtual wormhole tunnel is created by a series of malicious nodes that are hacked by the attacker, as shown in Fig. 2a. This is done by using the packet encapsulation method where the packet is encapsulated when it arrives at the first malicious node. It is then sent through the legitimate network path, but the hops of the wormhole tunnel are not counted. Upon arriving at the last node of the wormhole tunnel, the packet is de-encapsulated, and the hop count is increased by one only. In an external wormhole attack, the attacker is not a part of the system but is an outside intruder party. This is launched by using the packet relay method where the attacker transmits a packet between two far-away nodes, disguising them as each other's neighbours. The diagram in Fig. 2b shows a high-speed out-of-band channel established between two distant nodes, creating the illusion of neighbourhood at both ends of the wormhole tunnel [3].

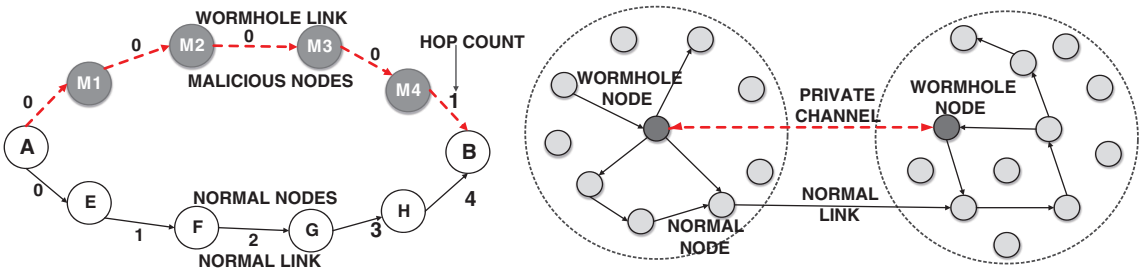

Figure 2: (a) Encapsulation (b) high transmission power channel

In the literature, many techniques have been proposed to tackle this deadly attack [4]. We have presented our analysis on competent techniques from the literature in Section 2. There are also significant techniques for the prevention of wormholes in the IoT networks. Surveys have been performed to analyse the effect and value of these techniques [5]. Studies have been conducted for a detailed evaluation of the countermeasures of the wormhole attacks in the IoT networks [6]. The scheme proposed in this paper has been implemented using the AODV protocol as it allows the scope for energy efficiency in the IoT-based sensor networks [7]. The proposed scheme comprises two phases. Phase 1 performs the finding of the suspicious nodes in the network. Phase 2 performs the detection of a possible wormhole on the suspicious nodes. If the wormhole links and the malicious nodes are found, the tunnel is disconnected, and a secure communication path is re-established. The malicious nodes are reconfigured for the next rounds of communication. We have implemented our scheme in a simulation in MATLAB 2019, and have presented the results of our technique with the help of graphs and tables. We have also compared our results with the results of a competent existing technique [8] showing the improved performance of the ESWI technique.

The major contributions of this research are:

(1) The developed ESWI technique detects and eliminates the wormholes during communication in IoT-based WSN.
(2) The ESWI technique has been designed to be simple and less complicated for efficient wormhole handling with minimum overheads.
(3) The ESWI technique has been made to consume less energy with a quality output to optimise the resources in a constrained IoT-based WSN.
(4) The performance results of the ESWI technique have been compared with a competent technique for the performance evaluation.

The rest of the paper is presented as follows: Section 2 elaborates the literature review with parameter-based analysis of schemes under study; Section 3 presents our proposed scheme with the algorithms and the flowcharts; Section 4 explains the simulation and the results of the proposed scheme; Section 5 concludes our work; and Section 6 provides the directions for the intended future work.

2 Literature Review

We have performed an extensive study on the existing techniques against wormhole attacks in WSNs. The findings of our literature study have been categorised and are presented below.

2.1 Neighbourhood and Connectivity Information-Based Techniques

Energy Preserving Secure Measure (EPSMAW) with the AODV routing protocol attempts to reduce the false-positive rate in a sparse network. It does not require additional hardware, nor does it cause the transmission overhead. Although malicious nodes can fabricate the neighbourhood lists to manipulate the detection method, they rarely detect wormhole tunnels shorter than 4 hops [8]. A Network Neighbourhood and Connectivity Information (NCI)-based method efficiently detects a wormhole attack with a minimised storage cost and without the need for additional hardware. This approach cannot be applied to the dynamic WSN [9]. The neighbour discovery and path verification method (NDPV) applies to the AODV protocol and does not need specialised hardware. It has a processing overhead and a low PDR (packet delivery ratio) [10].

The neighbourhood information and alternate path calculation (NIAPC) works on the AODV routing protocol and shows the detection without high storage requirement but with a high false-positive for the shorter wormholes [11]. A spanning trees-based scheme uses only the connectivity information of the node and its neighbourhood. It does not require additional hardware; hence, it does not increase the cost. The performance is not affected by an increased number of wormholes. It performs well for the longer wormhole paths, but the false positive rate increases in the case of the shorter wormholes [12]. The credible neighbour discovery (CREDND) protocol uses the hop difference and the local monitoring based on neighbour information. The internal, as well as the external wormholes, were detected without any additional hardware, and time and energy were also saved. The performance decreases in the case where all the nodes have a different communication range and they conform to another distribution [13]. An artificial neural network-based method shows a better detection rate for uniform networks than for non-uniform networks [14]. In another article, the author uses the node connectivity information to detect the encapsulation-based wormholes. They propose to increase the connection of the density between the neighbouring nodes. A more precise localisation can lead to even better performance [15].

2.2 Round-Trip Time-Based Techniques

An AODV-based RTT mechanism uses the round-trip time (RTT) mechanism where the delay and the system overhead are minimized without the need for specialised hardware. It applies to only the stationary nodes and does not work in a dynamic environment. It is also not able to handle the delays caused by queuing or congestion [16]. Another author used the EIGRP protocol-based round-trip time variation technique to identify the shortest path and detect the malicious nodes. It is less complicated and shows a better performance result, but it still needs to be enhanced in terms of the performance and compared to other existing techniques [17]. The trust-based wormhole mitigation (TBWM) is implemented in the AODV protocol using the two-tier round-trip time concept. It does not require additional hardware or tight clock synchronisation. The throughput still needs to be improved [18].

2.3 Transmission Power-Based Techniques

The MAODV technique implements a Modified AODV protocol to identify malicious nodes by measuring their transmission power. This method shows an increased latency [19]. The MHTPW (Mitigation of High transmission power-based wormholes) method uses the AODV protocol where the throughput and the PDR are enhanced while the delay is reduced. The repeated authentication may increase the delay in communication [20].

2.4 Statistical Method-Based Techniques

The poster mechanism in the duty cycling network detects the wormholes using the information of the delays caused in synchronised communication. This paper shows the detection results for only the type of wormholes that were launched by the node pairs which are both hidden and collaborative [21]. The wormhole-resistant hybrid technique (WRHT) uses the watchdog and the Delphi method to calculate the probability of the wormhole's existence. This method detects all types of wormholes without requiring additional hardware. However, the performance is decreased due to the independent use of the watchdog and Delphi schemes [22]. The SPRT-based method uses the sequential probability ratio test to detect the wormholes in the network. Using this method, the wormholes were detected more rapidly, using only a few nodes in the high mobility environment. However, it has a high false-positive ratio [23].

The distance & maximum likelihood estimation (DMLE) method is applied with the range-free localisation technique. This method does not put the computational load on the resource-constrained unknown nodes, however the detection rates require improvement and a high anchor-to-sensor node ratio increases the cost of the network [24]. Another technique (TESRP) is a sequence number method-based scheme that applies two sequence numbers to prevent the wormholes, but it is still prone to node capture threats [25]. The EFM technique suggests encapsulating the message and adding extra four-bit information to the message which would be de-capsulated at the destination. It also suggests dividing the message into several fragments and sending them via different routes. It has a poor PDR result [26]. The intrusion prevention system (IPS) with the AODV routing protocol has a possibly increased overhead and increased communication cost due to the repeated broadcasting about the malicious nodes [27].

In another article, the hound packets are used in a modified AODV protocol for the wormhole launched by an out-of-band channel and the encapsulation [28]. This method additionally requires the time for processing the hound packets which contributes to the failure in detecting the attacks in a smaller network. In another method, the author uses the distributed detection algorithm for the wormholes launched by using an out-of-band channel [29]. This method uses the transmission direction of the deviated innovative packets and produces a high processing cost when applied in a dense network. Another method uses a hybrid approach to detect the encapsulation and the packet relay-based wormholes, and uses the location and neighbour-connectivity information of the node [30].

2.5 Techniques Based on Location Information and Localisation

The location information and time synchronisation technique (LITS) detects the wormholes using simple hardware without any complicated calculations. This technique requires a clock-synchronisation module which increases the cost of the network [31]. On the contrary, the AWDV-hop based method finds the suspicious nodes to evaluate the localisation error for them and drop them if they are malicious. This method has a false positive detection and an increased localisation error in the scenario of an uneven distribution of the nodes [32]. In another technique, the location-based information is used to detect an out-of-band channel-based wormhole. This location-aware scheme follows the adjacent nodes by obtaining their location information from their neighbour nodes. This scheme produces an increased overhead due to the repeated hops. It also gives a high false-positive value and is only applicable in dense networks [33].

2.6 Authentication Key-Based Techniques

A method in the (EDAK) management and the generation process generates dynamic keys using the pre-existing information. It does not need a secure channel or a sharing phase. The increased flexibility and scalability make it applicable to large networks. It should include data integrity and freshness [34]. The Hybrid key pre-distribution scheme (HKP-HD) combines the q-composite scheme and the polynomial scheme to reduce the probability of the node capture attack [35]. The polynomial pool-based key-pre-distribution (PPKP) scheme uses the channel shifting method. It gives the adversary an impression of communication being carried out at a different channel rather than itself. However; it is successful only at the initial stage because once the intruder obtains the current channel information, the network will be prone to both external and internal wormhole attacks [36].

2.7 Analysis of Schemes

The literature study in this paper explores the summary metrics mostly used for the performance comparison in the wormhole detection and prevention-based schemes. It also explores the findings and the limitations of these schemes. It has been observed that the detection rate is improved in EPSMAW [8], NIAPC [11], ANN-based [14], SPRT [23], and AWDV-hop [32] and eventually decreases for WRHT [22] and DMLE [24]. The security is improved in many techniques, especially in the authentication-based schemes, and energy consumption is reduced in these schemes. The localisation error rate is reduced in [24] and [32]. In an ANN-based scheme [14], the false-positive and false-negative detection rates are improved. The schemes NCI [9], NIAPC [11], and HKP-HD [35] minimise the storage costs, whereas the other schemes have not discussed it. The EPSMAW [8] dominates with a 100% detection rate. The PDR varies from 80 to 98% in most of the schemes but [20] lags with 22% and TESRP [25] excels with 100% PDR. In most of the schemes, special hardware is not required to mitigate the wormhole attacks except for in DMLE [24] that requires additional cost for hardware, and LITS [31] uses simple hardware.

3 Proposed ESWI Technique

We propose a lightweight and less energy-consuming scheme for the detection of a wormhole attack in IoT-based WSNs. We identified the suspicious links by using the information of the geographical distance between the sender and the receiver nodes. The detection algorithm is then run on the suspicious nodes, and the wormholes are detected by evaluating the hop-count time gap using the hop-time stamp. Tab. 1 explains the important terms and the variables used in the algorithm explained later.

Table 1: Notations for scheme algorithms

Rt	*Received time by the destination node*	W	*Wormhole existence flag*
St	*Send timestamp by the source node*	M	*Malicious node flag*
Dt	*Duration of travel by packets*	Ns	*Sender node*
Hi	*Hop interval stamp*	Nr	*Receiver node*
Tt	*Transmission threshold*	R	*Rate of transmission*
Th	*Hop interval threshold*	d	*Distance between source and destination*
S	*Suspicious flag*	dn	*The distance of node from farthest neighbor*

3.1 Phase 1: Finding Suspicious Nodes

As the communication starts and the wormholes are launched in the network, we need to find the malicious nodes and the wormhole links. To identify the suspicious nodes, we use the time travelled information, as shown in Fig. 3. We call the functions to evaluate the estimated time for the packets to move from a source to its destination. We mark the time of arrival of the packets when they reach the destination, and calculate the difference between the estimated time of arrival and the actual time of arrival to obtain the duration. This difference is compared with a predefined distance threshold. If this value exceeds the threshold, then we mark the communicating nodes as suspicious nodes. The detection algorithm is then run for the suspicious nodes to locate the wormhole links.

Algorithm 1: Finding Suspicious Links and Nodes

Step 0 *Deploy sensor network, configure nodes, establish communication*
Step 1 *Set transmission time threshold,* $\mathbf{Tt = R * d}$
Step 2 *Embed, source and destination address,* ***St*** *with data packets, add hop time stamp at each hop*
Step 3 *For arriving packets from* ***Ns*** *at node* ***Nr,*** *Mark stamp* ***Rt***
Step 4 *Find duration of travel by packets,* $\boldsymbol{Dt = Rt - St}$
Step 5 *Check* ***if*** $\boldsymbol{(Dt > Tt)}$
    then:
        Step 6 *Mark suspicious flag* $\mathbf{S =}$ "TRUE," suspicious node found
        Step 7 *Call Detection algorithm for suspicious nodes* ***Ns*** *and* ***Nr***
    Else:
        Step 7 *Consider the path Safe and continue communication*

The flowchart in the Fig. 3 describes the working of the first phase of our algorithm in which we find the suspicious nodes. The wormhole detection algorithm is run for the suspicious nodes in the second phase. The flowchart describes the checking of a condition and the decision of declaring the nodes as either suspicious or not by choosing between the true or false options.

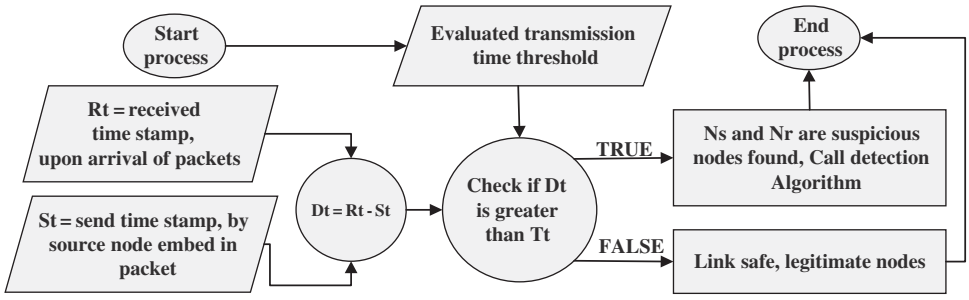

Figure 3: Flowchart of algorithm used to find suspicious nodes

3.2 Phase 2: Detecting and Handling Wormhole Attack

Once a link is found to be suspicious, we run a detection algorithm on the suspicious nodes to detect the wormhole. The detection algorithm is based on two methods; the first method checks if the hop-interval duration surpasses the threshold and the second method checks the existence of a high-power transmission channel. If either is found, a wormhole path is confirmed, and the

malicious nodes are identified, as shown in Fig. 4. We disconnect the wormhole path, kill the malicious nodes and re-establish a secure path for safe communication between the source and the destination nodes. Later, we reconfigure the dead nodes for the next rounds of the communication.

Algorithm 2: Detection and Handling of Wormhole Link and Malicious Nodes

Step 0 *Access suspicious sender node* ***Ns and its other end Nr*** *and their information,*
Step 1 *Set hop interval threshold,* $Th = dn * R$
Step 2 *Check* ***if*** $((\mathbf{Hc} == 1)$ ***is True***
then
Step 3 *Check* ***if*** $(\mathbf{Hi} > \mathbf{Th})$
then
Step 4 *Mark* $\mathbf{W} =$ *"TRUE"*
else
Step 4 *Mark* $\mathbf{W} =$ *"FALSE"*
Step 5 *Check* ***if*** $(\mathbf{W} ==$ *"TRUE"*$)$
Then
Step 6 *Delink path between* ***Ns*** *and* ***Nr***
Step 7 *Re-establish communication by secure route*
Step 8 *Allow* ***Ns*** *and* ***Nr*** *to reconfigure*
Else
Step 6 *Consider path safe and allow to continue communication*

The flowchart in Fig. 4 describes the detection of a wormhole link if it is present between the suspicious nodes. The hop-interval duration indicates if the packets have skipped any hops, indicating the presence of a wormhole link. When the packet travels on a wormhole path, its hop-count does not increase except for once at the last hop while reaching the destination.

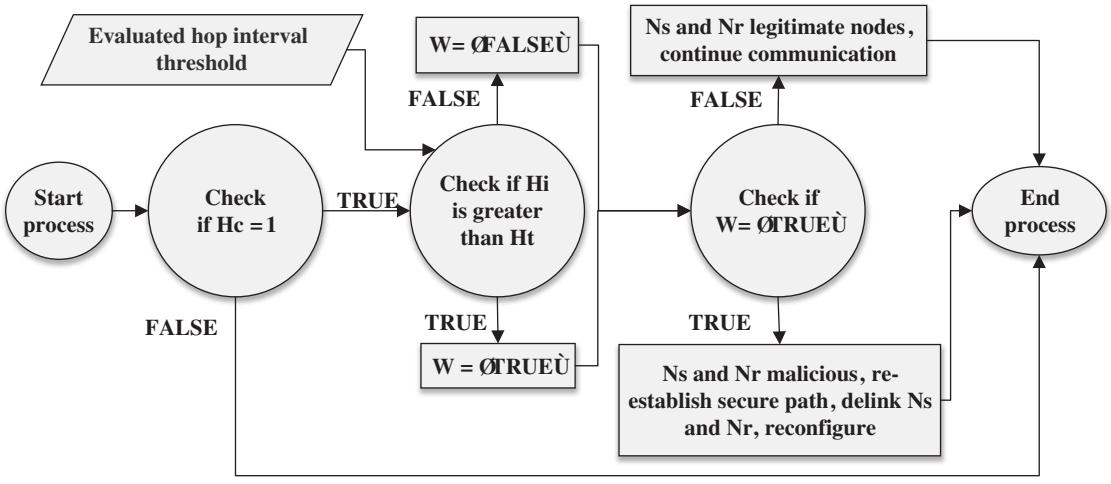

Figure 4: Flowchart of the detection of malicious nodes and wormhole links

We check the possibility of skipped hops to identify the wormhole links. In the second part of the condition, we also check whether a high-speed private channel exists between the source and destination. If this condition is true, then this private channel represents an external wormhole.

Therefore, we eliminate this link, reconfigure the attacked nodes and add them to the monitoring list for the next few rounds of communication. We re-establish secure communication between the nodes and make the network safely functional again.

4 Simulation and Results Evaluation

The network simulation was performed in MATLAB 2019. The AODV routing protocol was used and the random wormholes were launched in our simulation. The visualisation of the network, the experiment of the simulation, and the results of our detection algorithm are discussed below.

4.1 Simulation Environment

The parameters involved in our simulation experiment and their values are given in Tab. 2.

Table 2: Parameter values for the simulation environment

Routing protocol	AODV
Network area	100 m × 100 m
Network size	50, 100, 150 nodes
Transmission range	20 meters
Packet size	500 bytes
Sensor positioning	Random
Mobility	Static
Simulation time	500 seconds

4.2 Experiment

The following series of graphs elaborate the whole experiment stepwise, describing how a wormhole attack is detected and network security is enhanced. We experimented with three network sizes, including 50, 100 and 150 nodes. The simulation for each set of nodes is explained with two images, one showing a network under attack and the other showing a removed wormhole and a new and safe communication path.

4.2.1 Simulation for 50 Node Network Size

A sensor network with the size of 50 nodes is shown under a wormhole attack in Fig. 5a, where node 22 is the source and node 14 is the destination. A random wormhole path exists between nodes 1 and 32. It is clear that the security of the communication has been compromised.

It can be seen in Fig. 5b that the wormhole link has been eliminated. The malicious nodes have been marked, while a secure path has been established between the source node and the destination node.

4.2.2 Simulation for 100 Node Network Size

An under-attack network with the size of 100 nodes is shown in Fig. 6a. Here, node 12 is the source and node 39 is the destination. A wormhole path exists between nodes 80 and 49. The security of the network is compromised due to the data packets entering the wormhole.

It is shown in Fig. 6b that the wormhole link has been disconnected, and the malicious nodes have been killed and marked for reconfiguration. A secure communication path has been established between the source and destination nodes.

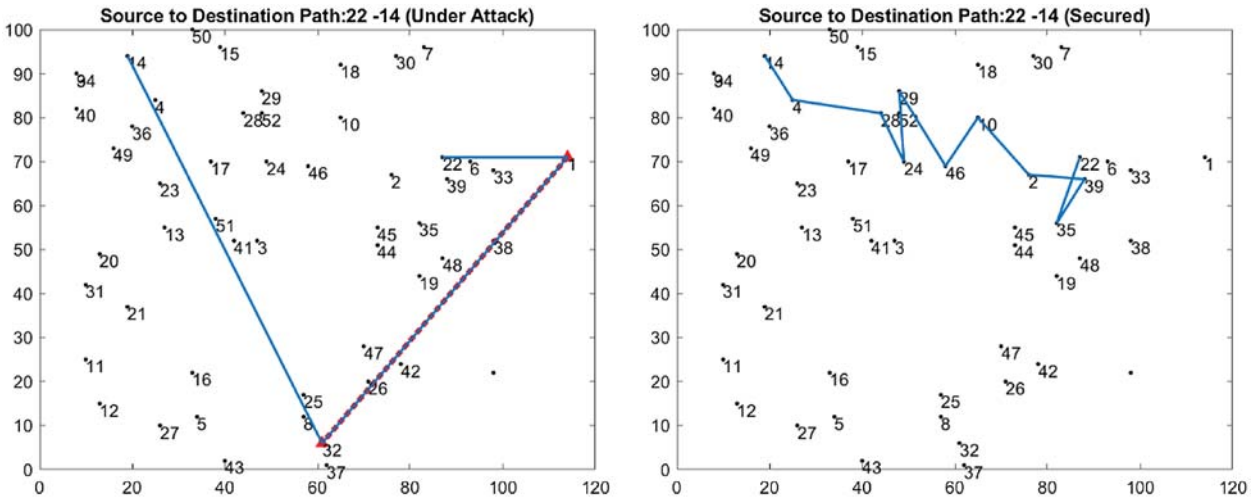

Figure 5: (a) Attacked & security compromised (b) wormhole eliminated & secure path

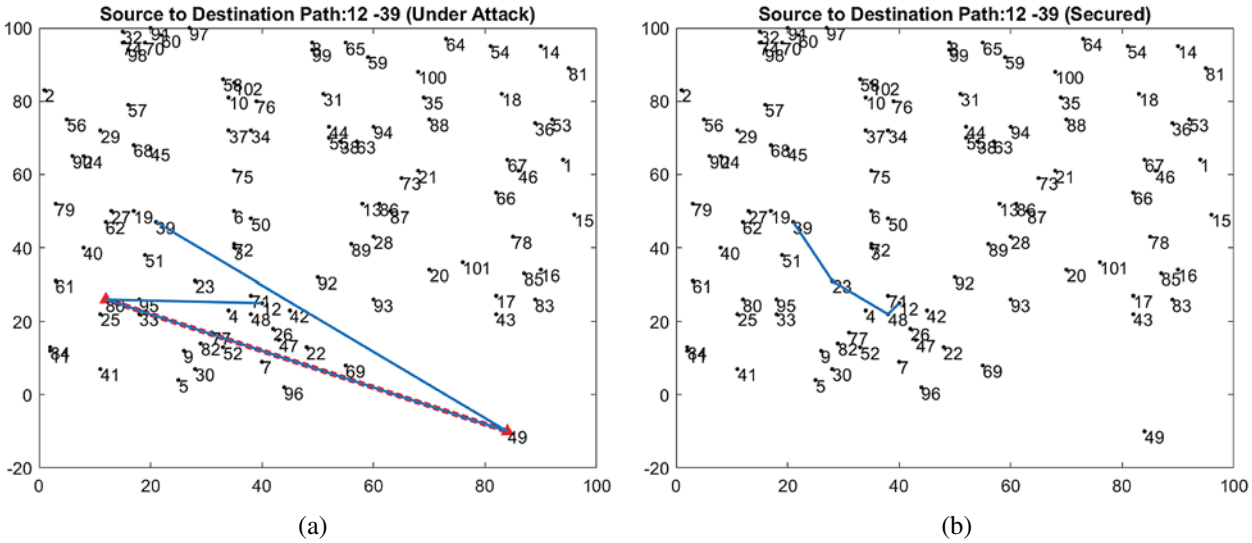

Figure 6: (a) Attacked & security compromised (b) wormhole eliminated & secure path

4.2.3 Simulation for 150 Node Network Size

The image in Fig. 7a shows an under-attack network, where node 74 is the source and node 30 is the destination. A wormhole exists from nodes 85 to 50. It is clear that the message is diverted due to the wormhole and the communication has been compromised.

It can be seen in Fig. 7b that the wormhole path has been de-linked and the malicious nodes have been killed. A new and safe path has been established between the source and destination nodes.

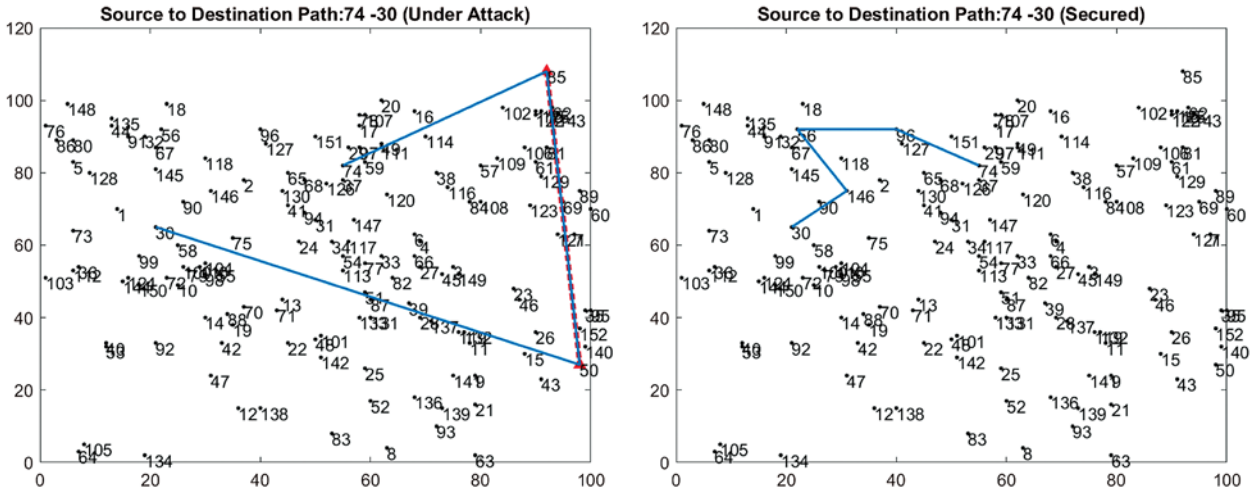

Figure 7: (a) Attacked & security compromised (b) wormhole eliminated & secure path

4.3 Evaluation Parameters

The ESWI technique has shown exceptional performance. The evaluation parameters are: throughput (kbps), end-to-end delay (seconds), packet delivery ratio%, detection rate% and energy consumption (joules). This technique gives a 99% detection rate and 99% packet delivery ratio. Our false-positive values were 0.0187, 0.1642, and 0.0364 for 50, 100 and 150 nodes, respectively. These values are very low compared to a few techniques in the literature that have described their false positive values [12,14,23]. The other important parameters are discussed below.

4.3.1 Detection Rate

This is the proportion of wormholes detected correctly by the security algorithm to all of the wormholes launched in the network. It is a measure of the performance of the security algorithm applied in the network [37]. It is usually measured in terms of % percentage, and is evaluated with the formula, where DR is the detection rate as $DR = (Wd)/(Wd + Wt)$, Wd is the number of the detected wormholes, and Wt is the total number of the launched wormholes. The detection rate results of the ESWI technique are parallel to the EPSMAW [8].

4.3.2 Packet Delivery Ratio

This is the ratio of the total packets delivered successfully to the total number of packets transmitted in a communication session [38]. The performance of a network increases with an increase in the packet delivery ratio. It is measured in terms of % percentage and evaluated with a formula, where PDR is the packet delivery ratio, Pt is the transmitted packets and Pr is the packets received in a communication round. It is formulated as, $PDR = (\sum Pr)/(\sum Pt)$ for the total packet delivery ratio in a transmission session. The PDR of the ESWI technique is parallel to that of EPSMAW [8].

4.3.3 Throughput

The throughput of a sensor network is an important factor for the performance evaluation. It is the number of packets successfully received per-second in a transmission session between

the source and destination nodes [38]. An increased throughput signifies an excellent speed of communication and increased performance. It is measured in unit kbps (kilobits per second). It is evaluated with the formula, where Th is the throughput, $Th = (\sum Pr)/sec$ and Pr is the packets received. The graph in Fig. 8a shows the increased throughput (kbps) values of 56.5, 79.1, and 124.7 for network sizes of 50, 100, and 150 nodes, respectively.

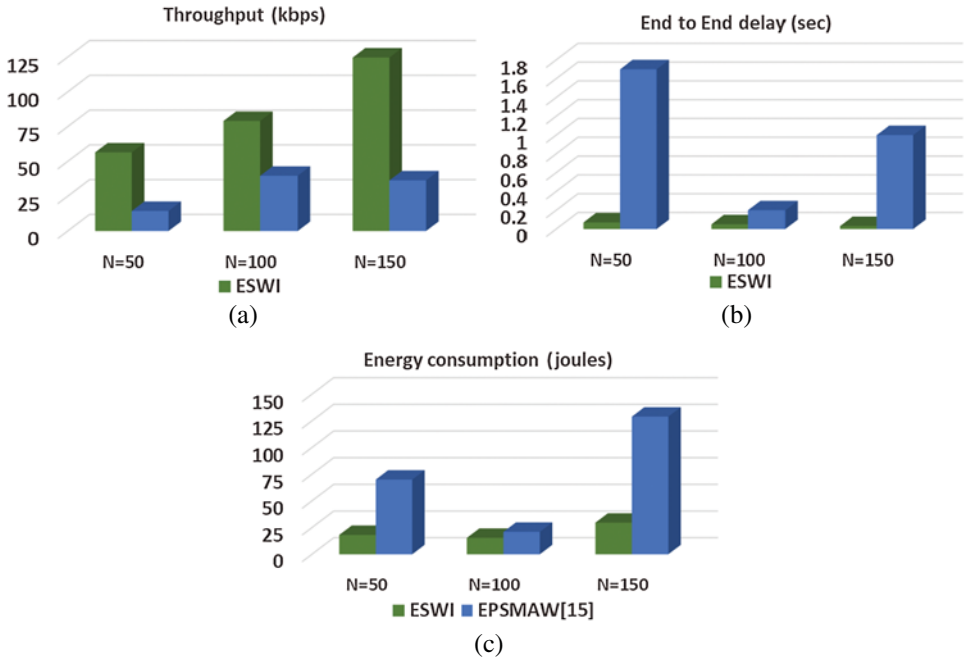

Figure 8: Results comparison of the ESWI and EPSMAW [8] techniques for (a) throughput, (b) end-to-end delay, and (c) energy consumption

4.3.4 End-to-End Delay

It is the time required by the packets to get from the source to the destination. The processing and queuing time are added to it if they are not zero. This parameter signifies the speed and the efficiency of the network [38]. It is measured in seconds or milliseconds and is evaluated using the formula, $D = \lambda * Ti + td * (N - 1)$, where λ is the number of hops, Ti is the time delay by the considered packet, N is the total number of nodes, td is the transmission delay and D is the total end-to-end delay. This is an important parameter in terms of the performance of a sensor network. The ESWI technique has been designed to give a reduced end-to-end delay, which is 0.0709 s, 0.0506 s, and 0.0321 s, as shown in Fig. 8b.

4.3.5 Energy Consumption

Energy is a limited resource in an IoT-based WSN. The algorithms used for other functionalities such as routing, localisation and security, etc. are required to consume less energy while performing efficiently [8]. The unit of the consumed energy is the simple Joule. There is no specific formula for calculating the consumed energy. However, this research modified the simplest formula given in [39] into the formula $Ed = \sum(\lambda i * (ET + ER)$, where ET is the transmitting energy, ER is the receiving energy, λi is the current hop on the routed path, and Ed is the sum of the total energy consumed on all the hops of the path from the sender to the receiver. This is the

most important parameter in our research as energy is a critical resource. The ESWI technique consumes 18.1 J for 50 nodes, 15.4 J for 100 nodes, and 29.6 J for 150 nodes, while [8] consumes 70 J, 21 J, and 129 J, respectively. Fig. 8c shows our results compared with a good existing technique.

4.4 Results Comparison

We have compared the results of the ESWI technique with those of the EPSMAW [8] in Fig. 8.

We can see that the throughput (kbps) of our scheme, as shown in Fig. 8a, is improved and increased in all three scenarios compared to the best-case value of [8]. The end-to-end delay of our scheme is improved and reduced; as shown in Fig. 8b, our technique gives a delay of fewer than 0.1 seconds in all three scenarios, which is even lower than the best-case value of 0.2 from [8].

Our algorithm has performed well in all three scenarios in the case of energy consumption, as shown in Fig. 8c. Our best case of energy consumption is for the network size of 50 and 100 nodes. The maximum energy is consumed for 150 nodes which are only 33 joules and is greatly reduced compared to [8].

5 Conclusion

The IoT-based WSNs are prone to many security attacks of which the wormhole attack is quite challenging. There has been ongoing research and development on the security against these attacks to propose a reliable solution. Initially, a detailed literature review was conducted through which the major limitations of the existing techniques were found. These limitations are the low detection rate, a poor packet delivery ratio, a decreased throughput, and high energy consumption. This study has provided the motivation for the research and for developing a technique against the wormhole attack with improved performance. The ESWI algorithm has been designed by simplifying the detection and handling process to give an excellent performance while consuming less energy from the network. Initially, the suspicious nodes are identified by using the transmission-time information between the sender and receiver nodes. Later, the detection procedure is performed on the suspicious nodes by using the hop-count and hop interval duration. The simulation for the ESWI technique shows a result of 99% for both the detection rate and the packet delivery ratio. It has given an increased throughput and a decreased end-to-end delay along with reducing the energy consumption in comparison with a competent existing technique.

6 Future Work

In the future, we will further review the impact of the wormhole attacks on the secure routing and data sharing schemes. We intend to explore the metaheuristic approaches for the optimisation of resources and to enhance the performance of the security algorithms for the IoT-based WSNs.

Funding Statement: Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. Li, X. Hu, K. Chen and K. He, "The applications of WiFi-based wireless sensor network in internet of things and smart grid," in *Proc. of the 2011 6th IEEE Conf. on Industrial Electronics and Applications*, Beijing, China, pp. 789–793, 2011.

[2] M. Goyal and M. Dutta, "Intrusion detection of wormhole attack in IoT: A review," in *Int. Conf. on Circuits and Systems in Digital Enterprise Technology*, Kottayam, India, pp. 1–5, 2018.

[3] P. Maidamwar and N. Chavhan, "A survey on security issues to detect wormhole attack in wireless sensor network," *International Journal of AdHoc Network Systems*, vol. 2, no. 4, pp. 37–50, 2012.

[4] N. Dutta and M. M. Singh, "Wormhole attack in wireless sensor networks: a critical review," *Advances in Intelligent Systems and Computing*, vol. 702, pp. 147–161, 2019.

[5] Y. A. Qadri, R. Ali, A. Musaddiq, F. Al-Turjman, D. W. Kim *et al.,* "The limitations in the state-of-the-art counter-measures against the security threats in H-IoT," *Cluster Computing*, vol. 23, pp. 2047–2065, 2020.

[6] I. Butun, P. Österberg and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2018.

[7] K. Machado, D. Rosário, E. Cerqueira, A. A. F. Loureiro, A. Neto *et al.,* "A routing protocol based on energy and link quality for internet of things applications," *Sensors*, vol. 13, no. 2, pp. 1942–1964, 2013.

[8] W. A. Aliady and S. A. Al-Ahmadi, "Energy preserving secure measure against wormhole attack in wireless sensor networks," *IEEE Access*, vol. 7, pp. 84132–84141, 2019.

[9] M. Patel and A. Aggarwal, "Detection of hidden wormhole attack in wireless sensor networks using neighbourhood and connectivity information," *International Journal on AdHoc Networking Systems*, vol. 6, no. 1, pp. 1–10, 2016.

[10] M. Okunlola, A. Siddiqui and A. Karami, "A wormhole attack detection and prevention technique in wireless sensor networks," *International Journal of Computer Applications*, vol. 174, no. 4, pp. 1–8, 2017.

[11] M. Patel, A. Aggarwal and N. Chaubey, "Detection of wormhole attack in static wireless sensor networks," *Advances in Intelligent Systems and Computing*, vol. 760, no. February, pp. 463–471, 2019.

[12] K. Harsanyi, A. Kiss and T. Sziranyi, "Wormhole detection in wireless sensor networks using spanning trees," in *2018 IEEE Int. Conf. on Future IoT Technologies, Future of IoT*, Budapest, Hungary, pp. 1–6, 2018.

[13] X. Luo, Y. Chen, M. Li, Q. Luo, K. Xue *et al.,* "CREDND: A novel secure neighbor discovery algorithm for wormhole attack," *IEEE Access*, vol. 7, pp. 18194–18205, 2019.

[14] M. N. A. Shaon and K. Ferens, "Wireless sensor network wormhole detection using an artificial neural network," in *ICWN*, Winnipeg, MB, Canada, pp. 115–120, 2015.

[15] J. Zheng, H. Qian and L. Wang, "Defense technology of wormhole attack based on node connectivity," in *IEEE Proc. of Int. Conf. on Smart City/SocialCom/SustainCom, (SmartCity)*, Chengdu, China, pp. 421–425, 2015.

[16] P. Amish and V. B. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," *Procedia Computer Science*, vol. 79, pp. 700–707, 2016.

[17] K. Karthigadevi, S. Balamurali and M. Venkatesulu, "Wormhole attack detection and prevention using EIGRP protocol based on round trip time," *Journal of Cyber Security and Mobility*, vol. 7, no. 1, pp. 215–228, 2018.

[18] S. Kori, N. K. G. and N. Sidnal, "Distributed wormhole attack mitigation technique in WSNs," *International Journal of Computer Network and Information Security*, vol. 11, no. 5, pp. 20–27, 2019.

[19] S. Bhagat and T. Panse, "A detection and prevention of wormhole attack in homogeneous wireless sensor network," in *Proc. of 2016 Int. Conf. on ICT in Business, Industry, and Government*, Indore, India, pp. 1–6, 2017.

[20] M. K. Sharma and B. K. Joshi, "A mitigation technique for high transmission power-based wormhole attack in wireless sensor networks," in *Proc. of 2016 Int. Conf. on ICT in Business, Industry, and Government, ICTBIG*, Indore, pp. 1–6, 2017.

[21] T. Minohara and K. Nishiyama, "Poster: Detection of wormhole attack on wireless sensor networks in duty-cycling operation," in *Proc. of the 2016 Int. Conf. on Embedded Wireless Systems and Networks*, Graz, Austria, pp. 281–282, 2016.

[22] R. Singh, J. Singh and R. Singh, "WRHT: A hybrid technique for detection of wormhole attack in wireless sensor networks," *Mobile Information Systems*, vol. 2016, pp. 1–3, 2016.

[23] J. Padmanabhan and V. Manickavasagam, "Scalable and distributed detection analysis on wormhole links in wireless sensor networks for networked systems," *IEEE Access*, vol. 6, pp. 1753–1763, 2017.

[24] G. Kumar, M. K. Rai and R. Saha, "Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 99, pp. 10–16, 2017.

[25] R. Shukla, R. Jain and P. D. Vyavahare, "Combating against wormhole attack in trust and energy aware secure routing protocol (TESRP) in wireless sensor network," in *Int. Conf. on Recent Innovations in Signal Processing and Embedded Systems, RISE 2017*, Bhopal, India, pp. 555–561, 2018.

[26] M. T. Scholar and B. Yadav, "Predication and root selection of worm hole attack in WSN," *International Journal of Scientific Research & Engineering Trends*, vol. 5, no. 6, pp. 1937–1944, 2019.

[27] M. T. Scholar, R. Kant and A. D. Sen, "Collaborative decision for wormhole attack prevention in WSN," *International Journal of Scientific Research & Engineering Trends*, vol. 6, no. 2, pp. 440–446, 2020.

[28] S. Gupta, S. Kar and S. Dharmaraja, "WHOP: Wormhole attack detection protocol using hound packet," in *Proc. of IEEE Int. Conf. on Innovations in Information Technology*, Abu Dhabi, UAE, pp. 226–231, 2011.

[29] S. Ji, T. Chen, S. Zhong and S. Kak, "DAWN: Defending against wormhole attacks in wireless network coding systems," in *Proc. of IEEE INFOCOM*, Toronto, ON, Canada, pp. 664–672, 2014.

[30] P. Pongle and G. Chavan, "Real-time intrusion and wormhole attack detection in the internet of things," *International Journal of Computer Applications*, vol. 121, no. 9, pp. 1–8, 2015.

[31] B. Bhushan and G. Sahoo, "Detection and defense mechanisms against wormhole attacks in wireless sensor networks," in *Proc. 2017 3rd Int. Conf. on Advances in Computing, Communication and Automation (Fall), ICACCA 2017*, Dehradun, India, 2018.

[32] J. Li, D. Wang and Y. Wang, "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network," *IET Wireless Sensor Systems*, vol. 8, no. 2, pp. 68–75, 2018.

[33] M. Arai, "Reliability improvement of multi-path routing for wireless sensor networks and its application to wormhole attack avoidance," in *Proc. of Ubiquitous Intelligence and Computing and 2015 IEEE 12th Int. Conf. on Autonomic and Trusted Computing and 2015 IEEE 15th Int. Conf. on Scalable Computing and Communications and Its Associated Workshops*, Beijing, China, pp. 533–536, 2015.

[34] S. Athmani, A. Bilami and D. E. Boubiche, "EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs," *Future Generation Computer Systems*, vol. 92, pp. 789–799, 2019.

[35] P. Ahlawat and M. Dave, "An attack resistant key predistribution scheme for wireless sensor networks," *Journal of King Saud University, Computer and Information Sciences*, pp. 1–13, 2018.

[36] B. Zeng and L. Yao, "Design of a secure communication scheme using channel shifting in wireless sensor networks," *IOP Conf. Series: Earth and Environmental Science*, vol. 428, no. 1, 2020.

[37] R. Zhang and X. Xiao, "Intrusion detection in wireless sensor networks with an improved NSA based on space division," *Journal of Sensors*, vol. 2019, pp. 20, 2019.

[38] P. V. C. and A. F. S. Devaraj, "Evaluation of impact of wormhole attack on AODV," *International Journal of Advanced Networking and Applications*, vol. 4, no. 4, pp. 1652–1656, 2013.

[39] V. Casares-Giner, T. I. Navas, D. S. Flórez and T. R. V. Hernández, "End to end delay and energy consumption in a two-tier cluster hierarchical wireless sensor networks," *Information Technology: New Generations (ITNG 2018)*, vol. 10, no. 4, pp. 1–29, 2019.