Computers, Materials & Continua
DOI:10.32604/cmc.2022.020585
Article

Tech Science Press

Multi-Step Detection of Simplex and Duplex Wormhole Attacks over Wireless Sensor Networks

Abrar M. Alajlan*

Self-Development Skills Department, Common First Year Deanship, King Saud University, Riyadh, KSA
*Corresponding Author: Abrar M. Alajlan. Email: aalajlan1@ksu.edu.sa
Received: 30 May 2021; Accepted: 20 July 2021

Abstract: Detection of the wormhole attacks is a cumbersome process, particularly simplex and duplex over the wireless sensor networks (WSNs). Wormhole attacks are characterized as distributed passive attacks that can destabilize or disable WSNs. The distributed passive nature of these attacks makes them enormously challenging to detect. The main objective is to find all the possible ways in which how the wireless sensor network's broadcasting character and transmission medium allows the attacker to interrupt network within the distributed environment. And further to detect the serious routing-disruption attack "Wormhole Attack" step by step through the different network mechanisms. In this paper, a new multi-step detection (MSD) scheme is introduced that can effectively detect the wormhole attacks for WSN. The MSD consists of three algorithms to detect and prevent the simplex and duplex wormhole attacks. Furthermore, the proposed scheme integrated five detection modules to systematically detect, recover, and isolate wormhole attacks. Simulation results conducted in OMNET++ show that the proposed MSD has lower false detection and false toleration rates. Besides, MSD can effectively detect wormhole attacks in a completely distributed network environment, as suggested by the simulation results.

Keywords: Wireless sensor network; wormhole attack; node validation; multi-step detection

1 Introduction

Many applications that use WSNs can be vulnerable to a wide range of security threats [1]. The sensors are strategically placed to monitor real-time events that may be utilized for a variety of business and domestic purposes. WSNs, on the other hand, have difficulties dealing with security risks [2]. Wormhole attacks, which have significant impacts on the network layer, are one of the biggest dangers. Wormhole attacks, according to research, can disrupt network routing, location-based wireless security, and data aggregation [3–6]. A wormhole attack can be launched by a single node or by a pair of cooperating nodes [7]. Because it may disrupt the network discretely, this attack is extremely difficult to detect [8]. Even if one does not understand the different cryptographic algorithms employed [9], it is usually caused by one or more nodes [10].

The consequences of a wormhole attack are quite severe [11]. For example, a wormhole-enabled node may conspire to falsify the routing configuration in order to obtain total control of the network traffic [12]. As a result, the nodes may disrupt processes that rely on topological proximity [13]. These attacks can also raise node power consumption by allocating various resources and transmitting excessive data [14]. Wormholes cannot be prevented using various cryptographic algorithms and cryptic keys since they just replay data packets that already exist in WSNs [15]. Because WSNs connected to IoT have various hardware flaws, solutions in range-free localization are more likely to seek cost-effective solutions [16,17]. The adoption of the DV-hop algorithm to avoid wormhole attacks is one example of a low-cost approach [18,19].

This paper presents a new scheme for the multi-detection of wormhole attacks to address these security concerns. The proposed scheme consists of the following three modules: neighbor node validation process (NNVP), fake link reduction process (FLRP), and wormhole isolation.

The NNVP determines whether or not the node is infected and whether or not it is a neighbor node. The links that originate from a wormhole are referred to as "false links". These connections can be removed using the FLRP. Finally, the isolation module guarantees that the detection and recovery processes are carried out properly, isolating all traces and instances of the wormhole. This paper contributes as:

- The proposed MSD involves five detection methods, which can detect the successfully classified simplex and duplex wormhole attacks.
- MSD is supported with a valid locator detection feature, which can adjustably fine-tune a threshold value to make a sensor node easily to detect the valid locator(VL). Once VL is identified, then the detection process is used to determine the wormhole-enabled node for the WSN connected with IoT.
- MSD consists of a self-healing procedure that determines the wormhole attack and points to the positions of wormhole-enabled nodes.
- Secret key and signature generation processes are used to guarantee the secure communication process among the sensor node and adjacent sensor nodes or sensor node and base station.

2 Related Work

This section explores into the key aspects of striking approaches. To detect and recover from wormhole attacks in multi-hop WSNs, the distributed self-healing method was suggested [20]. It also determines the locations of malicious nodes and separates them from the network. It is the first approach that carries out both routing organization recovery and wormhole node quarantine in response to wormhole attacks. However, it requires proper localization capabilities as well as time analysis. The proposed method relies solely on network connection in a distributed manner. The simulation results showed that the suggested technique detects all wormhole-enabled nodes with 100 percent accuracy and zero percent erroneous detection. In terms of power usage and overhead, the result also shows that the suggested technique outperforms other competing alternatives.

The cloned and wormhole node detection method is introduced in Maheswari et al. [21]. This method examines each node's behavior to determine if it is a wormhole or not. If the node has not received authorization from the base, it is not permitted to participate in the communication. To solve the problem of wormhole and Grayhole attacks, the lightweight trust-driven approach was proposed [22]. The suggested method uses direct trust, which is determined based on the

node's characteristics. It has also been utilized to establish indirect trust based on the perspectives of nearby sensor nodes. According to the authors, the suggested technique is energy efficient and would not add extra overhead to data flow.

The directional antennas are introduced to prevent wormhole attacks [23]. To avoid a wormhole, each node exchanges a secret key with its neighbors and maintains a current list of all neighbors. The direction in which a signal is heard from a neighbor is used to build all lists in a secure way, provided that all nodes antennas are aligned. However, it only mitigates the threat of wormhole attacks to a limited extent. It only protects against wormhole attacks, in which hostile nodes try to trick two nodes into thinking they are neighbors. In wireless sensor networks, the effects of wormhole attacks are widely examined utilizing IoT [24].

The authors proposed the label-based DV-hop localization method to defend against the possibility of wormhole attacks. Furthermore, the correctness of the approach is also proved using the simulation results.

DAWN: A Distributed detection algorithm is proposed for controlling the Wormhole in WSN [25]. The suggested method made an attempt to establish a lower constraint on efficient detection rate. The authors investigated the battle of DAWN against collusion and wormhole attacks. Furthermore, the suggested technique has no increased cost due to the use of additional testing messages. DAWN is supported by substantial experimental findings, as all existing wormhole detection techniques increase communication overhead and false negatives. The proposed technique, on the other hand, has a low communication overhead and a high accuracy rate.

3 Proposed Multi Detection Scheme

This section presents the proposed multi-detection scheme for detecting wormhole attacks. Thus, the data distribution process is of paramount vital before detecting the attacks. The Poisson distribution [26] has been used for the data distribution over the network. The data is available at different locations of a WSN. Each data location has a degree of self-sufficiency, is capable of handling local as well as global applications. Data distribution is shaped either by captivating a prevailing single location or excruciating it over different locations. The data uncertainty of data distribution can be computed as:

$$D_c = \sum_{i=1}^{n} P_i log_2 P_i \tag{1}$$

where p_i: probability of the event

The proposed scheme consists of the three modules, which are discussed in the subsequent sections:

- Neighbor node validation process (NNVP),
- Fake link reduction process (FLRP),
- Wormhole isolation.

3.1 Neighbor Node Validation Process

For each type of wormhole attack detected, there are corresponding different identification protocols. They are as follows.

There are different types of wormhole attacks. They could be classified as either simplex or duplex wormhole attacks [27,28]. In this work, different detection processes have been applied to identify the wormhole attacks.

3.1.1 Duplex Wormhole Link Attack

To detect whether a network is experiencing the problem due to the duplex wormhole attack, the sensor node attempts to recognize all its Valid Locators (VLs) prior to the self-discovery process. Let us take X_2 as a locator depicted in Fig. 2; when the sensor node initiates the Location Request Message (LRM), then X_2 returns a Location Acknowledgement Message (LAM) to the sensor node because it is within the communication range of X_2. Furthermore, LAM also travels from point Z_2 through the wormhole attack link to another point Z_1 before it arrives at the sensor node. Thus, the sensor node receives several times LAM from the X_2. Nevertheless, there are three diverse scenarios:

- The locator is within the range of transmission of the sensor node. Thus, the sensor node received three times message from X_4, as shown in Fig. 2.
- The locator is not within the range of the sensor nodes' transmission; then the sensor node receives the message twice from the as X_7, as shown in Fig. 2.
- The locator is within the range of transmission of the sensor node, then the sensor node receives the message twice from the X_2, as shown in Fig. 2. Based on the ranges, X_2 and X_4 are considered as the VLs, but not X_7. The sensor node can apply five VLs processes to identify the V-locators.

The attacker node has a capability of changing the location in order to attack the legitimate node. Let us assume that distance between attacker and victim is symbolized as $|A_d - v_d|$. The random change $[-1, 1]$ can be characterized as '$\Delta\beta$'. Thus, $cos(2\pi\Delta\beta)$ denotes the circular path of the attacker around the victim node. Thus, the control is transferred to the victim node when detection movement of the malicious node is determined that is computed by:

$$(v_d + 1) = |A_d - v_d.cos(2\pi\Delta\beta)| + A_d \tag{2}$$

where A_d: Attacker distance; v_d: Victim distance

When an attacker node knows that its position is exposed, then it attempts to update the position. However, the victim node can identify whenever an attacker moves away from there based on a random-change. Hence, if the random change is greater than 1 or less than -1 that provides the clue to the victim node. The moving process of the attacker node 'A_m' and identifying process time predicted by and victim node 'v_{pp}' are mathematically expressed in Eqs. (3) and (4) respectively.

$$A_m = |2G.A_d\,(rc) - A_d| \tag{3}$$

$$(\ddot{v_d} + 1) = |2G.A_d(rc)| - v_{pp} \tag{4}$$

$v_d(rc)$ Random change in the attacker node's distance; G: Constant variable for the global change in the position.

If the response time of victim node is faster then, it can identify the movement of an attacker node efficiently depicted in Fig. 1.

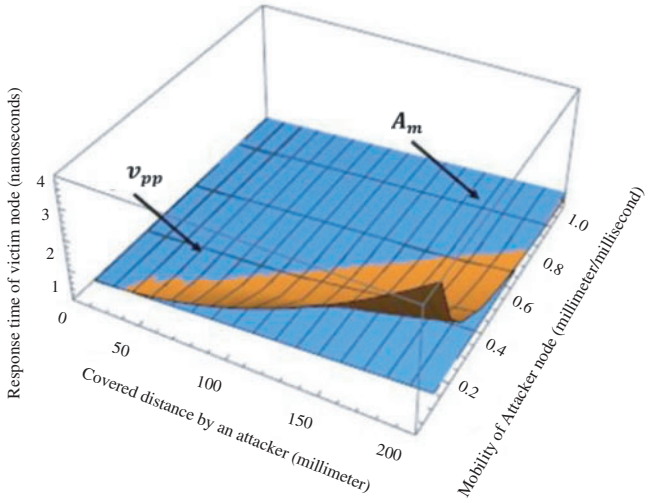

Figure 1: Response time of victim node

- Detection Process-1

In the first scenario, if the sensor node gets victim due to a wormhole attack and receives three times LAM of the Neighbor Locator (NL), then a bit of the LAM should be set to 1. Thus NL is declared as a VL that is shown as X_4 in Fig. 2. The sensor node only nullifies the minimum Medium Access Control (MAC) delay of a locator. On the other hand, message traveling and the response time delays get longer when the message comes through the wormhole link. Therefore, the measured distance based on the LAM comes from VL takes the shortest response time.

In the second scenario, if the sensor node gets the LAM twice from the NL, then a bit of the LAM should be set to 1, and NL is considered as a Suspicious Locator (SL) such as X_7 can be determined and as shown in Fig. 2.

Definition 1: Data reiteration rate 'D_{rr}' of the given samples reflect the malicious behavior of the sensor node because of repetition of the continuous packets.

$$D_{rr} = \frac{\left|S_p.t - S_r.t\right|}{S_p.t} \tag{5}$$

where S_p: Sent samples; t: Time for sending the samples; repeated samples.

Definition 2: If the observation time for the sample-sending $S_s(t)$ is too large then, it may cause of duplex wormhole link attack. On the other hand, if the sample-sending rate is lower, then it may also cause of duplex wormhole link attack.

$$S_s\,(t) = \frac{\left(S_p.t - S_{sv}.t\right)}{\left(S_p.t\right)} \tag{6}$$

where S_{sv}: The sample-sending value

In the third scenario, if the sensor node gets the LAM twice from the NL, then a bit of the LAM should be set to 0, and NL is regarded as the VL. Also, measured distance based on the LAM is considered as correct with the shorter response time as X_2 shown in Fig. 2.

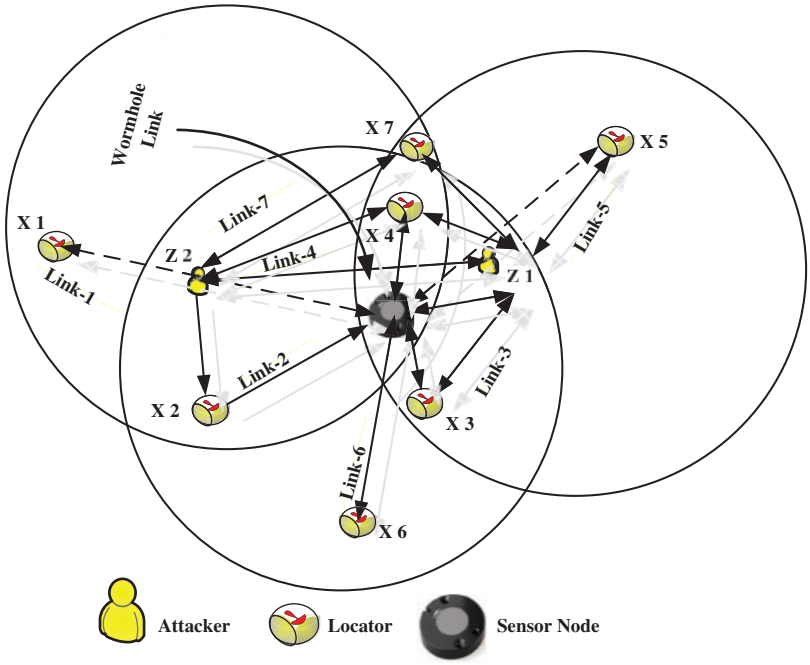

Figure 2: Showing Duplex wormhole attack process

Let us take a set of locators such that $L = \{(a_1, b_1), (a_2, b_2), \ldots, (a_p, b_p)\}$ and corresponding measured distances $S = \{l_1, l_2, \ldots, S_p\}$, where (a_i, b_i) is the location 'L' of the locator X_i and r_i that is the distance from a sensor node to X_i, where $J = (1, 2, 3, \ldots, p)$. Thus estimated location of the sensor node can be determined as (a_0, b_0). Thus, the mean square error (MSE) rate for the location can be defined as:

$$\delta 2 = sj = \frac{1\,[li - (a0 - aj)\,2 + (bo - bj)\,2]\,2}{s} \tag{7}$$

The distance dependability property (DDP) of the legal locators demonstrates that the MSE of the estimated location is based on the exact distance that is smaller than a minimum threshold. On the other hand, the MSE of the estimated location is based on the distance that involves some inappropriate distance measurements that is not smaller than a threshold value. More VLs are detected using the DDP of the VLs.

- Detection Process-2

If the sensor node has detected not less than two VLs using Detection Process 1; thus, it detects other VLs by examining whether an estimated distance is dependable. A predefined threshold 'β' of the MSE is identified (i.e., an estimated distance with the MSE lesser than β is regarded to be steady). The sensor node can recognize X_2, X_3, and X_4 as VL despite changing the location, as shown in Fig. 1. Furthermore, an accurate estimated distance 'D_{acc}' can be obtained.

$$D_{acc} = \frac{1}{2}\sum_{i=1}^{M}(\Psi - \gamma)^2 \tag{8}$$

where Ψ: distance of valid locator; γ: distance covered by the sensor in case of mobility.

When a new locator joins the network, then it is of paramount significance to calculate the distance of the new locator 'D_{nl}' to avoid and minimize the error rate given by

$$D_{nl} = \sum_{i=1}^{M} \left[c_i f_i (a_i) + \frac{1}{2} b_i f_t^2 (c_i) \right] + \omega (f - t) \tag{9}$$

where $c_i = \partial_x^{(t-1)} l\left(x_i, x^{(t-1)}\right)$ & $b_i = \partial^2_{x^{(t-1)}} l\left(x_i, x^{(t-1)}\right)$

The objective function is used to analyze the nature of the link, whether wormhole or not.

The sensor node initiates the detection process one by one for the uncertain locators (ULs). For example, to examine whether X_1 is the VL. Thus, it is also important that the sensor node should be capable of calculating its own location using measured distance to X_1, X_2, X_3, and X_4. If the measured distance to X_1 is inappropriate, then the MSE of the calculated distance dimension can surpass the β, which implies that X_1 should not be considered as VL. If the sensor node identifies the distance stability of X_2, X_3, X_4, and X_6, it also checks that the MSE is lesser than β; therefore, X_6 should be considered as VL and measured distance to X_6 should be considered as accurate. After examining each uncertain NL, the sensor node can determine all VLs with the exact measured distance.

Theorem 1: When a sensor node becomes victim due to duplex wormhole link attack, $\forall L_j$ such contention location $C(L_j) \neq \rho, L_j \in D_A$.

Proof: When a sensor node is a victim due to duplex wormhole link attack as depicted in Fig. 1. All of the locations in $SL\,(Atk_1)\,USL\,(Atk_2)$ are NLs for the sensor nodes. According to the given theorem:

$\forall L_j \in SL\,(Atk_1)\,U, SL\,(Atk_2), C\left(L_j\right) SL\,(Atk_1)\,USL\,(Atk_2)$.

For each $L_i \notin SL\,(Atk_1)\,USL\,(Atk_2)$.

Thus, the message cannot be advanced to wormhole link, and there is no anomaly for the interchange of the message interchange between L_i and other locators, consequently

$C\left(L_j\right) = \rho$. Hence, $\forall L_j$ such that $C\left(L_j\right) \neq \rho, L_j \epsilon D_A$.

Tab. 1 shows the notations and their description.

Table 1: Used notations and description

Notations	Description
$C\left(L_j\right)$	Contention Location
D_A	Duplex Attack
Atk_1	Attacker-1
Atk_2	Attacker-2
SL	Suspicious Locator
NL	Neighbor locator
S_{Nid}	Sensor Node Identity
T_k	Transaction Key

3.1.2 Simplex Wormhole Link Attack

When the sensor node discovers the simplex wormhole attack, then it adopts the VLs' detection processes.

- Detection Process-3

If the sensor node gets the victim due to simplex wormhole link attack as depicted in Fig. 2. If the sensor node receives the LAM of an NL twice, then that NL is considered as a VL. For example, if X_3 replies a LAM to the sensor node as depicted in Fig. 1, this message travels through two different routes to the sensor node: one route goes directly from X_3 to the sensor node whereas, the other from X_3 to Z_1 via the wormhole link to the sensor node. Hence, the sensor node is capable of determining that X_3 is a VL. To further achieve the accurate measured distance to X_3, the sensor node matches the response times of the LAM from X_3 through different routes. The measured distance with the shortest response time is deliberated as correct and accurate. Likewise, X_4 is also recognized as a VL, and its accurate measured distance can be determined. Thus, the spatial property is used to identify VLs. Duplex and simplex wormhole attack detection processes are given in Algorithm 1.

Property 1: The sensor node is unable to get the messages from two NLs concurrently if the measured distance between these two NLs is larger than $2d$.

Algorithm 1: Detection process for the wormhole attack

1. **Initialization:** {L_{rm}: Location request message; N_l: Neighbor locator; L_{am}: Location acknowledgement message; D_γ: Detection methods-1-2; D_δ: Detection methods-3-5; S_{wh}: Simplex wormhole attack; D_{wh}: Duplex wormhole attack}
2. **Input:** {L_{rm}; L_{am}}
3.. **Output:** {S_{wh}; D_{wh}}
4. Sensor broadcasts a L_{rm}
5. Each NL sends L_{am} to sensor node including message abnormality detection outcome.
6. Sensor node waits for L_{am} to measure the distance to each NL and compute the response time of each NL
7. If the sensor node detection $=D_\gamma$ then
8. Detected as D_{wh}
9. if the sensor node detection $= D_\delta$ then
10. Detected as S_{wh}
11. Else No
12. A simplex wormhole link attack is discovered.
13. Else if No wormhole attack
14. End if
15. End if
16. End else if

In Algorithm 1, the simplex and duplex detection processes are explained. In step-1, variables are initialized. Steps-2 provides the input. Step-3 gives the output. In step-4, the sensor node broadcasts the location request message. In step-5, each neighbor locator sends location acknowledgment message to the sensor node, including message irregularity detection result. In step-6, each neighbor locator sends the location acknowledgment message to measure the distance to

each neighbor locator and computes the response time for each node locator. In step-7, if the sensor node detection methods fall within the category of dections: 1–2 methods, then the duplex wormhole method is observed. In step-8, if the sensor node detection methods fall within the category of detections; 3–5 methods, then the simplex wormhole method is observed. In step-9, if a sensor node is neither falling within the processes of D_γ nor D_δ, then it is considered that no wormhole link attack is discovered.

- Detection Process-4

When the sensor node becomes victim due to the simplex wormhole link attack as depicted in Fig. 2, if two NLs violate the spatial property, it is noticeable that one of them is a valid locator (VL) and explained in the Algorithm-2, and the other is a Suspicious Locator (SL). Let us take an example of X_2 and X_5 in Fig. 2, as the distance between X_2 and X_5 is larger than 2d. After receiving LAM from them, the sensor node can detect that two NLs cannot hold the spatial property. Thus, VL can be differentiated from SL using the response time of both NLs as the LAM from X_5 is transmitted to the sensor node through the wormhole link. It also takes a longer response time than that from X_2. The sensor node considers X as a VL and X_5 as a SL because X_2 has a shorter response time. Therefore, the distance to X_2 is also deliberated as correct. The distance consistency property is used of VLs to determine more VLs when the sensor node becomes a victim due to the simplex wormhole link attack.

Algorithm 2: Detection of Valid Locators

1. **Initialization:** {VL: Valid Locator; D_γ: Detection methods-1-2; D_δ: Detection methods-3-5; S_{wh}: Simplex wormhole attack; D_{wh}: Duplex wormhole attack; S_N: Sensor node}
2. **Input:** {D_γ ;D_δ}
3. **Output:** {VL}
4. If $S_N = D_{wh}$ then
5. Set $D_{\gamma=}1$ and detect VLs
6. If $S_N = D_{wh}$ then
7. Set $D_{\gamma=}2$ and detect VLs
8. End if
9. End if
10. If identified VLs ≥ 2 then
11. Initiate detecting process of other VLs
12. End if
13. Elise if $S_N = S_{wh}$ then
14. Set $D_\delta = 3, 4$ & 5 and detect VLs
15. End else if

In Algorithm 2, the valid locators are identified. In step-1, variables are initialized. In steps-2–3, give the input and output. In steps-4–7, when the sensor node detects the duplex wormhole attack, then it initiates the 'D_γ' detection method-1 or detection method-2. In steps-8–9, the process of detecting other valid locators is initiated. In step-13–14, when the sensor node detects the simplex wormhole attack, then it starts to use detection methods-3–5. And based on the detection methods, the valid locators are detected.

Let us take a 'bs_i' as a malicious parameter done by a simplex wormhole link attack that can be denoted by

$$bs_i = \left(bs_{i,1}, bs_{i,2}, \ldots, bs_{i,j}\right)^T \tag{10}$$

Let us take a 'Gd_k' as a malicious parameter done by a duplex wormhole link attack that can be indicated by

$$gd_k = \left(gd_{k,1}, gd_{k,i}, \ldots, gd_{k,j}\right)^T \tag{11}$$

For the data coming from each sensor node is evaluated for every event. As we get $i = 1, 2, \ldots, 50$, $k = 1, 2, \ldots, 50$, and $k = 1, 2, \ldots, 10$. The set bs_i is used to generate the template for detection of simplex wormhole link attack for the sensor node 'i'. While the set gd_k is used for the template generation of duplex wormhole link attack. It can be determined if each $gd_k \in Gd_k$ can be segregated from each $bs_i \in Bs_i$.

- Detection Process-5

When the sensor node becomes the victim of the simplex wormhole attack, similar to Detection Process 2, if the sensor node uses detection processes 3–4 for detecting minimum two VLs, it can detect other VLs based on the Distance Consistency Property (DCP) of VLs. Considering the scenario of Fig. 3, the sensor node can detect X_2, X_3, and X_4 as VLs and obtain the correct measured distance. The sensor node can further detect other VLs by examining distance consistency. A MSE smaller than β can be obtained when the sensor node estimates its location based on X_1, X_2, X_3, and X_4 because they are all VLs. The sensor node can then determine that X_1 is a VL and the measured distance to X_1 is found as correct.

The procedure of the basic VLs detection approach is enumerated in Algorithm 2: When the sensor node gets a victim of the duplex wormhole link attack, then it needs to execute the detection Process 1 to determine the VLs. As the distance stability process requires at least three VLs, if the sensor node classifies no less than two VLs, it can use the detection process 2 to detect other VLs. In case if the sensor node becomes the victim due to simplex wormhole link attack, then it adopts the detection processes 3–4 to identify the VLs. After that, if at least two VLs are identified, the sensor node executes the detection process 5 to identify other VLs.

3.2 Prolonged Node Validation Process

In the basic VL detection process, if the sensor node detects less than three VLs, it terminates the self-localization. This occurs because the statistical method of maximum likelihood estimation (MLE) used in the self-localization needs at least three distance measurements. However, when using detection processes based on the distance consistency property of V-locators, many VLs cannot be determined due to the threshold of MSE, β is set incorrectly at a trivial value.

A prolonged valid locators' identification approach is used to handle the above problem. The proposed approach can adaptively adjust the threshold value of β to make the sensor node easier to detect more VLs. If the sensor node gets a victim of the duplex wormhole link attack, it conducts detection process 1 to detect VLs. If the sensor node detects no less than two VLs, it replicates to detect other VLs using detection process 2 and updates the β with an augmentation of $\Delta\tau 2$ until the minimum three VLs are recognized, or β is higher than β max. In case, the sensor node notices that it gets a victim due to simplex wormhole link attack, it adopts the detection processes 3–4 to detect the VLs. If at least two VLs are detected, the sensor node repeats

to conduct the detection process 5 to identify other VLs and update β with an increment of $\Delta\beta$ until at least three VLs are recognized, or β is larger than β max. The procedure of the prolonged VLs' detection process is explained in Algorithm 3.

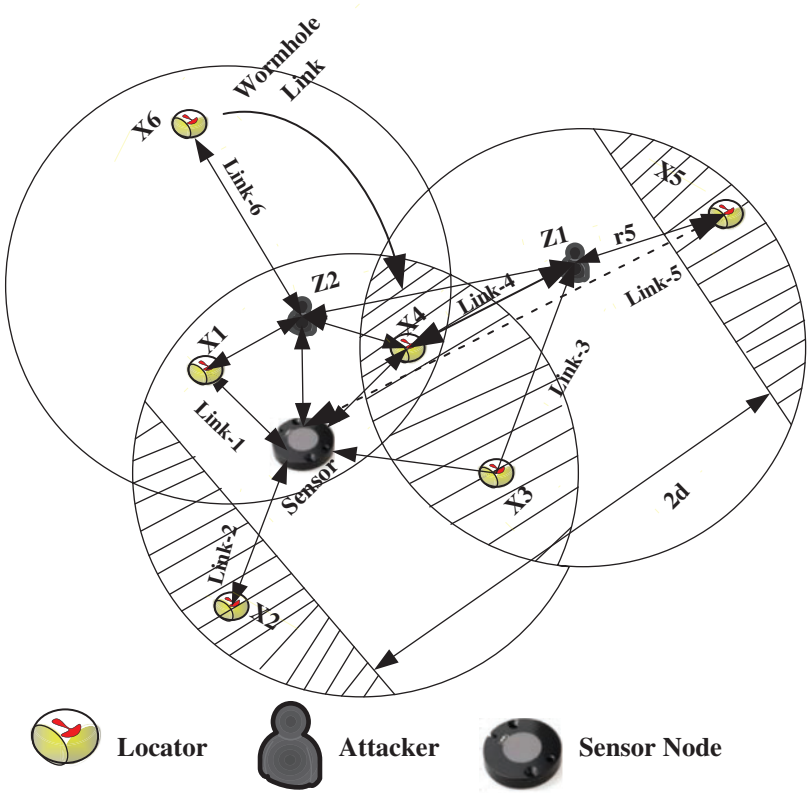

Figure 3: Showing Simplex wormhole attack process

After the wormhole link attack detection and VLs' identification, the sensor node can detect VLs from its NLs. Furthermore, the sensor node can calculate the accurate distance for the VLs. If the sensor node gets minimum three correct measured distances to its NLs, it performs the Maximum Likelihood Estimation (MLE) localization process based on the locations and distances of the associated NLs.

Algorithm 3: Prolonged Node Validation process

1. **Initialization:** {VL: Valid Locator; β: Predefined threshold; D_γ: Detection methods-1-2; D_δ: Detection methods-3-5; S_{wh}: Simplex wormhole attack; D_{wh}: Duplex wormhole attack; S_N: Sensor node}
2. **Input:** {D_γ ;D_δ}
3. **Output:** {VL}
4. If $S_N = D_{wh}$ then
5. Set D_γ to detect VL
6. If identified $VLs \geq 2$ then

(Continued)

7. Repeat
8. Conduct D_γ to detect other VLs
9. Set $\beta \leftarrow \beta + \Delta\beta$
10. .Compare $\beta > \beta max$
11. Until identified VLs ≥ 3
12. End if
13. End if
14. Else, if $S_N = S_{wh}$, then
15. conduct D_δ to detect VLs
16. If an identified VLs ≥ 5, then
17. Repeat
18. Conduct D_δ to identify other VLs
19. Set $\beta \leftarrow \beta + \Delta\beta$
20. Compare $\beta > \beta max$
21. Until the identified VLs ≥ 5
22. End Else if
23. End if

In Algorithm 3, the Prolonged node validation process is explained. In step-1, used variables are initialized. Steps-2–3 specify the input and output. Steps-4–5 shows the detection process of the duplex wormhole link attack conducted by the sensor node; then it initiates to conduct the detection process-1 to identify the VLs. In steps-6–7, the value of the identified VLs is compared; if identified VLs are greater than or equal to 2, then this process will be continued until determine for the rest of the detection methods. The steps-8–9 show the process of detecting other VLs; then the threshold value is set by adding the maximum threshold value and incremental of a predefined threshold value.

In steps-10–13, the predefined threshold value is compared with the maximum incremental predefined threshold value; this process continues until an identified VLs are greater than or equal to 3. In steps-14–20, the sensor node detects the simplex wormhole attack, then the detection process of valid locators is begun. By applying the detection methods 3–5, then other valid locators are determined. Finally, the threshold values are set in order to identify all the valid locators.

3.3 Secret Key and Signature Generation Process

The sensor nodes are tiny, and their data sending process is vulnerable. Thus, the proposed approach wants to secure the data communication process. Hence, the secret key is generated for sending the data confidentially. In addition, the signature is created to validate the sent message.

3.3.1 Secret Key Generation Process

When the sensor node interacts either with an adjacent sensor node or the base station, then it requires to generate the secret key for interacting and sending the data.

Let us assume that the sensor node 'S_N' intends to communicate, then a secret key is calculated as:

For $i \in \{0, 1\}$, then two hash values 'H_v' should be calculated. Hence, $T_k = L_1\left('S_{Nid}, i\right), T_i \in O_1$. Thus, the output produces a secret key 'S_k' calculated by

$$S_k = H_v T_k \tag{12}$$

where T_k: Transaction key.

3.3.2 Signature Generation Process

The signature must be calculated, and the sensor node obtains the received file 'X'. The file X must be split into 'm' number of the chunks 'c_k' that can be written as

$$C_t \to \{c_1, c_2, \ldots, c_{n-1}, c_m\}, m \in X \tag{13}$$

where C_t: Total number of the chunks

The sensor node computes the pair of the signature

$\{S_k, T_k\}$ for each file of chuck.

First, Calculating two hash value as:

$$H_v = L_2\,(filename)$$

$x_k = L_3(q_k, S_{Nid}, filename)$,

q_k: chunk's pointer c_k in the given file X, $1 \le k \le m$.

Once two hash values are calculated, then start a file of secret sharing $SS_{(\tau,d)}$ with $z\,(x) = H_v + q_1 x + \ldots + q_{r-1} x^{r-1}$ and calculates *r–1* points.

$$U_p = \left\{(e_1, y\,(e_1))\,, (e_2, y\,(e_2))\,, \ldots, (e_{r-1}, y\,(e_{r-1}))\,|e_l \in \{0,1\}^*\right\} \tag{14}$$

U_p: A universal parameter.

Finally, compute the number of the random variables 'n' given by

$v_k \in K_t, 1 \le k \le n$, then calculates

$$R_k = v_k T_k \tag{15}$$

where v_k: Random variable

Therefore, the signature generation process is secure that also supports the sensor nodes to avoid impersonation and identity attacks.

4 Experimental Results

To validate the effectiveness of the proposed MSD approach, the simulation is conducted using OMNET++ 5.6.2 simulator. Based on the simulation results, the performance of MSD approach has been analyzed and compared with existing state-of-the-art schemes: Hybrid Algorithm to Eliminate Wormhole Attack (HAW) [20], Dynamic Detection and Prevention (DDP) [21], and Wormhole and Gray attack (WGA) [22]. The sensor nodes are distributed randomly to serve the data sending process. The deployed sensor nodes are connected using the end-to-end reliable and bi-directional approach.

The main goal of the simulation is to balance the bandwidth usage and proper data exchange. Several scenarios (Malicious and Non-Malicious) are generated to conclude the realization of the proposed approach. The simulation scenarios resemble the tangible WSN situation. The given outcomes demonstrate alike to a realistic environment. The simulation network consists of 450×450 square meters with 270 sensor nodes. The transmission and sensing ranges are 45 and 30, respectively. Each sensor node has 80 Kb/Sec bandwidth capacity and buffers the 80 frames. The size of the data packet is 512 bytes with 10 seconds' pause time, and the entire simulation takes 15 minutes. The summary of the simulation parameters is given in Tab. 2.

Table 2: Summary of simulation parameters

Parameters	Description
Node's initial energy	4.5 Joules
Sensing Range of the Nodes	30 meters
Total sensor nodes	270
Buffering capacity of each sensor node	80 frames
Number of maximum malicious nodes	10%
Antenna type	bidirectional
Packet size	512 bytes
Packet rate	0.568 b/s
Transmission range	45 meters
Node's Bandwidth	80 Kb/Sec
Contending Schemes	MSD, HAW, DDP, and WGA
Size of each region	450 × 450 square meters
Simulation time	15 min
Simulator	OMNeT++ 5.6.2
Operating System	Windows-10
Pause time	10 seconds
Rx energy consumption	14.3 mW
Tx energy consumption	15.2 mW
Idle energy consumption	14.3 mW
Sleep energy consumption	0.05 mW

Based on simulation outcomes, the following metrics have been achieved.

- Accuracy
- Detection (false negative, true positive and false positive)

4.1 Accuracy

Accuracy requires both precision and authenticity. Fig. 4 shows the accuracy of the proposed MSD and other contending schemes (HAW, DDP, and WGA). The accuracy of the proposed approach and contending approaches has been measured using the variable number of valid sensor nodes up to maximum 180 with the 10% malicious sensor nodes. The result demonstrates that the MSD produced a maximum of 99.93% accuracy. Whereas other contending schemes produced 98.74%–99.47%.

When the number of sensor nodes increase then, accuracy is marginally affected with 10% malicious nodes. The results demonstrate that proposed MSD obtain 99.904% accuracy with 270 sensor nodes. Whereas, the contending approaches obtain the accuracy 97.9%–98.6% with 270 sensor nodes. HAW produced less accuracy with 270 sensor nodes as shown in Fig. 5. The testing procedure involves true negative, and true positive. Thus, the accuracy is given by:

$$= \left(\sum_{j=0}^{P} T_p + \sum_{k=0}^{Q} T_n \right) / T_{wm} \tag{16}$$

where T_p: True positive, T_n: True negative, T_{wm}: Total wormhole attacks.

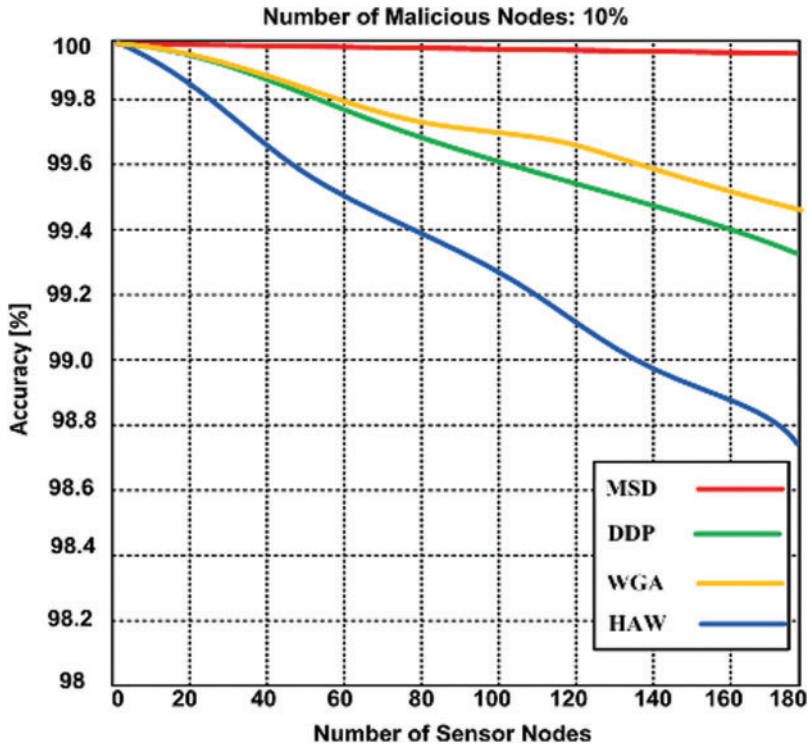

Figure 4: Accuracy of proposed MSD and contending with 180 nodes

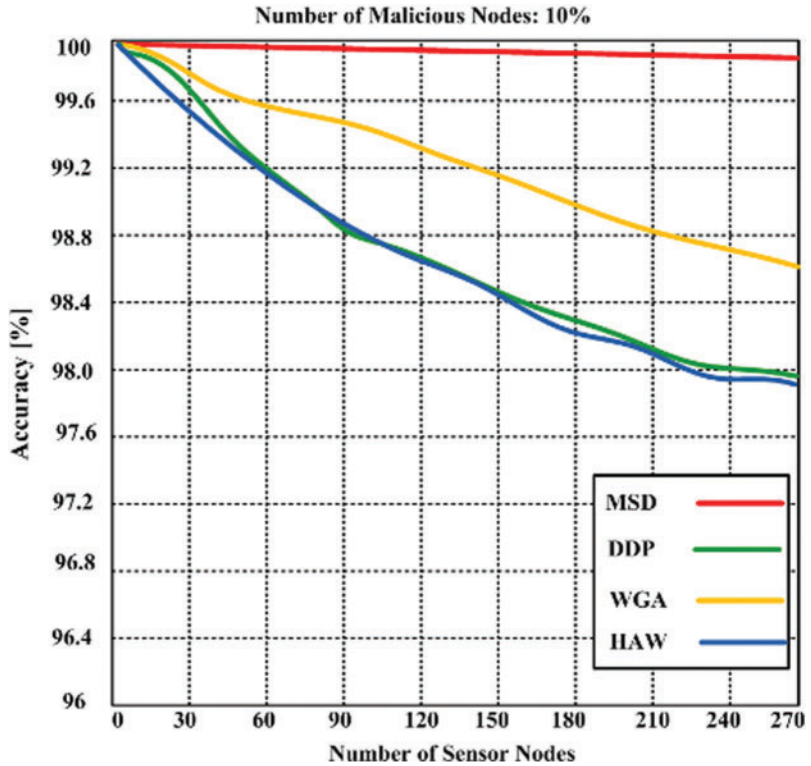

Figure 5: Accuracy of proposed MSD and contending HAW, DDP, and WGA with 270 sensor nodes

The reason behind better accuracy for the proposed approach is to use five detection methods and secret key and signature generation processes that determine the precise true negative and true positive successfully.

4.2 Detection (True Positive, False Negative and False Positive)

The proposed MSD and contending schemes (HAW, DDP, and WGA) have been measured using False-positive 'F_{pos}' and true positive 'T_{pos}' rates. True positive and false positive rates are depicted in Fig. 6. It has been observed, based on the outcomes of the simulation that the proposed MSD possesses a greater true positive rate. On the other hand, contending schemes have a lesser true positive with the false positive rates. DDP gets lower positive rate. False negative 'F_{neg}' and true positive rates have been depicted in Fig. 7.

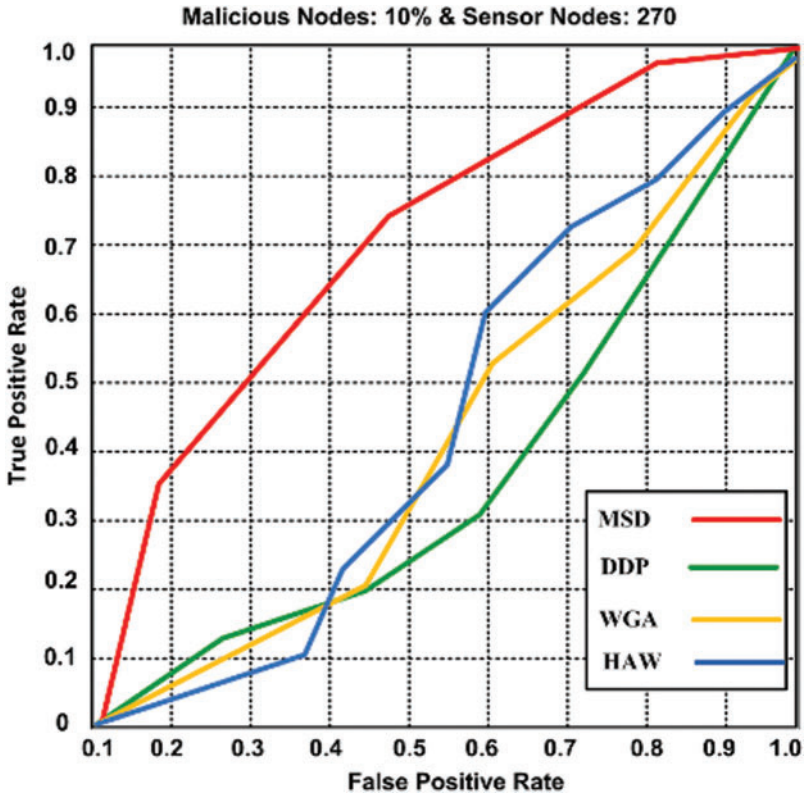

Figure 6: False positive rate and true positive rate for proposed MSD and competing schemes (HAW, DDP, and WGA)

The trend of the result in the graph demonstrates that the proposed MSD gets a higher true positive rate, and only 0.015 false-negative rates are detected, while contending schemes show the higher false-negative rate that is counted as 0.023–0.072. MSD gains the higher false-negative rage that is measured to be 0.072. Based on the outcomes, it has been confirmed that the proposed scheme attains the true higher positive and gains lower false-negative rates. Thus, true positive,

false positive and false negative rates can be calculated using Eqs. (17)–(19).

$$F_{pos_{(r)}} = \frac{F_{pos}}{(F_{pos} + T_{neg})} \tag{17}$$

$$T_{pos_{(r)}} = \frac{T_{pos}}{(T_{pos} + T_{neg})} \tag{18}$$

$$F_{neg_{(r)}} = \frac{F_{neg}}{(T_{pos} + F_{neg})} \tag{19}$$

where $F_{pos_{(r)}}$: False positive rate; T_{neg}: True negative; $F_{neg_{(r)}}$: False negative rate, and $T_{pos_{(r)}}$: True positive rate.

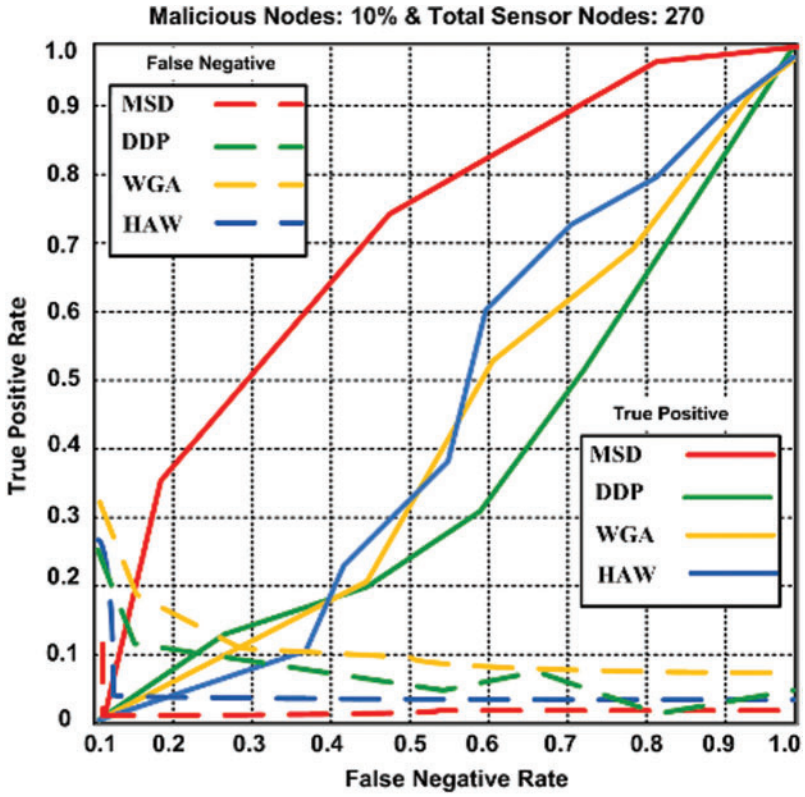

Figure 7: False negative rate and true positive rate for proposed MSD and competing schemes (HAW, DDP, and WGA)

5 Conclusion

A new multi-detection scheme has been executed for detecting the wormhole attacks in WSNs over the distributed environment. In the proposed scheme, different integrated detection modules implemented to systematically detect, recover, and isolate wormhole attacks. In this multi-step detection (MSD) scheme, the neighbor node validation process plays a crucial role in identifying the infected nodes and the false neighbors. In addition, the proposed MSD can be used to

eliminate all fake links (i.e., the links which originate from a wormhole). Finally, the performance of isolation module ensured that detection and recovery are highly effective and thereby isolates the wormhole completely from the network. To support the proposed scheme, different algorithms were executed that provide specific details of how exactly each component (e.g., Wormhole attack detection scheme and Extended Node Validation process) of the proposed scheme was effectively detected and successfully recovered the network inside the distributed environment. Current limitations on assessing after the rerouting and rescheduling in real time traffic management for the detection model should be taken into consideration towards further research. In future, attacks in integrated network scenarios around the distributed environment will be evaluated through non-traditional algorithms for optimum desirability to detect and recover the WSN from the wormhole attacks.

Acknowledgement: This research was supported by the Deanship of Scientific Research, King Saud University, Kingdom of Saudi Arabia.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: The author declares that she has no conflicts of interest to report regarding the present study.

References

[1] P. P. Devi and B. Jaison, "Protection on wireless sensor network from clone attack using the SDN-enabled hybrid clone node detection mechanisms," *Computer Communications*, vol. 152, pp. 316–322, 2020.

[2] Bharat Bhushan and Gadadhar Sahoo, "Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective," in *Handbook of computer networks and cyber security*. Cham: Springer, pp. 683–713, 2020.

[3] O. R. Ahutu and H. El-Ocla, "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks," *IEEE Access*, vol. 8, pp. 63270–63282, 2020.

[4] R. Bhatt, P. Maheshwary, P. Shukla, P. Shukla, M. Shrivastava *et al.,* "Implementation of fruit fly optimization algorithm (FFOA) to escalate the attacking efficiency of node capture attack in wireless sensor networks (WSN)," *Computer Communications*, vol. 149, no. 2, pp. 134–145, 2020.

[5] H. Kalkha, H. Satori and K. Satori, "Preventing black hole attack in wireless sensor network using HMM," *Procedia Computer Science*, vol. 148, no. 1, pp. 552–561, 2019.

[6] K. Spurthy and T. N. Shankar, "An efficient cluster-based approach to thwart wormhole attack in adhoc networks," *Int. Journal of Advanced Computer Science and Applications*, vol. 11, no. 9, pp. 312–316, 2020.

[7] S. Deshmukh-Bhosale and S. S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based internet of things," *Procedia Manufacturing*, vol. 32, pp. 840–847, 2019.

[8] P. Kaliyar, W. Ben Jaballah, M. Conti and C. Lal, "LiDL: Localization with early detection of sybil and wormhole attacks in IoT Networks," *Computers & Security*, vol. 94, 2020.

[9] X. Li, J. Zheng, S. Liu and T. Zhu, "A novel wormhole-like mesoporous hybrid $MnCoO_x$ catalyst for improved ethanol catalytic oxidation," *Journal of Colloid and Interface Science*, vol. 555, pp. 667–675, 2019.

[10] J. Govindasamy and S. Punniakody, "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 735–744, 2018.

[11] G. Kumar, M. Kumar 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.

[12] M. Panic, C. Hernandez, E. Quinones, J. Abella and F. J. Cazorla, "Modeling high-performance wormhole NoCs for critical real-time embedded systems," in *Proc. RTAS*, Vienna, Austria, pp. 1–12, 2016.

[13] C. Lee and J. Suzuki, "SWAT: A decentralized self-healing mechanism for wormhole attacks in wireless sensor networks," in *Handbook on Sensor Networks*, Hackensack, NJ, USA: World Scientific, pp. 511–532, 2010.

[14] K. Dong, D. Zhu and A. Daniel Hill, "Mechanism of wormholing and its optimal conditions: A fundamental explanation," *Journal of Petroleum Science and Engineering*, vol. 169, no. 1, pp. 126–134, 2018.

[15] Panwar Pratyush, Rohan Verma, M. M. S. Rauthan and Varun Barthwal, "An overview on security issues, attacks, challenges and protocols in WSN," in *Proc. of Integrated Intelligence Enable Networks and Computing*, Gopeshwar, India, pp. 269–278, 2021.

[16] N. Labraoui, M. Gueroui and M. Aliouat, "Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks," *Transactions on Emerging Telecommunications Technologies*, vol. 23, no. 4, pp. 303–316, 2012.

[17] P. Shukla, "ML-IDS: A machine learning approach to detect wormhole attacks in internet of things," in *Proc. IntelliSys*, London, UK, pp. 234–240, 2017.

[18] M. S. Ahsan, M. N. M. Bhutta and M. Maqsood, "Wormhole attack detection in routing protocol for low power lossy networks," in *Proc. ICICT*, Karachi, Pakistan, pp. 58–67, 2017.

[19] X. Wang, F. Hu, C. Zhai, Y. Zhang, X. Su *et al.,* "Research on improved DV-HOP algorithm against wormhole attacks in WSN," in *Proc. ITA*, Les Ulis, France, vol. 7, 2016.

[20] Asmita Singh, Atul Kumar Sah, Arun Singh, Bhavnesh Jaint and S. Indu, "Wormhole Attack Detection in Wireless Sensor Network Using SVM and Delay Per-hop Indication," in *Data Engineering and Communication Technology*. Singapore: Springer, pp. 39–47, 2021.

[21] P. U. Maheswari and P. G. Kumar, "Dynamic detection and prevention of clone attack in wireless sensor networks," *Wireless Personal Communications*, vol. 94, no. 4, pp. 2043–2054, 2017.

[22] R. Mehta and M. M. Parmar, "Trust based mechanism for securing IoT routing protocol RPL against wormhole & grayhole attacks," in *Proc. I2CT*, Pune, India, pp. 1–6, 2018.

[23] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole attacks," in *Proc. NDSS*, San Diego, CA, USA, pp. 1–11, 2004.

[24] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang *et al.,* "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, no. 2, pp. 22–35, 2015.

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

[26] L. Dümbgen and J. A. Wellner, "The density ratio of poisson binomial versus poisson distributions," *Statistics & Probability Letters*, vol. 165, 2020.

[27] Patel Manish, Akshai Aggarwal and Nirbhay Chaubey, "Analysis of wormhole attacks in wireless sensor networks," in *Recent Findings in Intelligent Computing Techniques*. Singapore: Springer, pp. 33–42, 2018.

[28] M. Patel, A. Aggarwal and N. Chaubey, "Analysis of wormhole attacks in wireless sensor networks," in *Recent Findings in Intelligent Computing Techniques*, vol. 708. Singapore: Springer, pp. 33–42, 2018.