ORIGINAL RESEARCH PAPER
Pages: 29-52

An Improved DV-Hop for Detecting Wormhole Attacks in Wireless Sensor Networks

G. Farjamnia[1], Y. Gasimov[2], C. Kazimov[3]
[1]Institute of Applied Mathematics, Baku State University, Baku, Azerbaijan,
[2]Azerbaijan University, Baku, Azerbaijan,
[2]Institute of Physics Problems, Baku State University, Baku, Azerbaijan,
[2]Institute of Mathematics and Mechanics, ANAS, Baku, Azerbaijan,
[3]Department of Applied Mathematics and Cybernetics, Baku State University, Baku, Azerbaijan
ghasem.farjamnia@gmail.com, yusif.gasimov@au.edu.az, cavanshir.kazimov@au.edu.az
Corresponding author: ghasem.farjamnia@gmail.com

DOI10.22070/jce.2020.5227.1152

***Abstract*- One of the major against in Wireless Sensor Networks (WSNs) is wormhole so that two or more attacker nodes help each other to rob communications and record the information in another place. Wormhole attacks can disrupt communications, change routing, or cause some other localization errors. This attack can also bring about physical access without permission, cause package losses, and increase traffic in the network. Attacker nodes can convince ordinary sensor nodes that they are neighbors and can observe their information and any other traffic that they send in the link length. Localization is an important problem in WSNs. DV-Hop (Distance Vector-hop) is a traditional algorithm for localizing sensor nodes using a hop distance assessment. The DV-Hop model has poor localization accuracy. This paper improves DV-Hop and increases wormhole attack detection accuracy in WSNs based on localization method. In this paper, a new distance based on correction of Hop-size and gap measurement is proposed to minimize the error that exists in DV-Hop. The results of simulation and assessment show that the proposed model carry outs better than DV-Hop in different topologies, in which proposed model has significantly higher localization accuracy.**

***Index Terms*-** Wireless Sensor Networks, Wormhole, DV-Hop, Improved DV-Hop

I. INTRODUCTION

WSNs are inexpensive, can be used for many purposes, and can be easily installed [1]. Their reasonable price, the applicability for many items, and easy installations have turned WSNs into an emerging technology [2, 3]. While the need for WSNs grows in different applications, the security becomes one of the most important disputes. Wormhole attack as a security threat has the ability to

Manuscript received 16-Jan.-2020 and revised 19-April-2020,
Accepted on 23-May-2020
P- ISSN: 2322-4088
E- ISSN: 2322-3936

rob information and deactivate network operation [4]. Wormhole attack is one of most common attacks against WSNs. In this attack, the offender deploys two malicious nodes in two different areas of the network and establishes proprietary channel and high-speed between the two [5]. Afterward, they transfer the network traffic from one spot to their allies in another spot causing the normal nodes in two different locations of the network to think of each other as two-way neighbors. Hence, this attack affects localization algorithms to a large extent [5].

Security is considered to be the most important issue in WSNs as sensor nodes can be easily captured by the attacker nodes without suitable security, and their information can be robbed consequently [6]. Before WSNs are successfully decorated, security issues should be taken into account. Takings into account the vulnerability of wireless communications to eavesdropping, every attacker can manipulate the traffic trend, stop the operations, or forge the packages. Therefore, false information is sent wormhole nodes. Due to sensor nodes having a synoptic transfer board and limited resources, an attacker with high processing ability and the more communicational board can attack several sensors simultaneously to modify real information when transferring.

In WSNs that could be affected by various types of attacks, in some cases, a malicious node making several forged identities, is able to distract other network nodes [7]. Nearly all WSN security protocols believe that a sensor node can be fully controlled by the enemy or penetrator through direct communication. WSNs can be targeted by two types of offenses namely inactive and active. During the inactive type, the offender spies on the network without being recognized. Thus, an attacker can eavesdrop secretly, masquerade as a normal node, and leave the network after taking the collected information at a given time [8]. In general, all the nodes of a network collaborate with each other as a single and collaborating unit. In the external attacks the offender attacks the network out of the network's area, and unusually these kinds of attacks have limited damages.

WSNs, while having energy constraints, face attacks. One of the most typical attacks among the WSNs is the wormhole attack. In this kind of attack the offender creates a fast link with low delay between points within the network. This attack is possible by either, collaboration of two or more nodes or the addition of the latest attacker nodes of the network. The attacker collects the records from one aspect of the hyperlink using the created link and delivers it to the other aspect using the fast hyperlink made [9]. This attack brings approximately modifications in the system of network statistics and might distract the normal nodes. In this paper, we have proposed a stepped forward model for detecting of wormhole attacks based on DV-Hop localization for secure routes [10]. DV-hop algorithms have troubles which include now not being knowledgeable about new positions of neighboring nodes by using beacon nodes. Therefore, the DV-Hop set of rules has no criterion for the assessment of the communications among beacon nodes. Specifically, if an attacker node penetrates into the community, it does not use the distance criterion for the detection of the primary interval of

beacon nodes. In DV-Hop development, the criterion of the distance between beacon nodes is used for the cause of detecting the attacker node to the network area.

Wormhole attacks could interrupt communications, alter routing, or cause localization mistakes. The attack can also lead to physical permission-free access, cause package losses and increase network traffic. Attacker nodes can convince normal sensor nodes to be neighbors and can track their data and traffic in the link length [11]. DV-Hop is a localization algorithm that used to identify wormhole attacks [10]. In the localization method, certain nodes are used that known as beacon nodes. These nodes come with GPS location devices that allow them to occupy a certain space. First, beacon nodes spread spatial information over the network and therefore specifying either the average of interval between the two nodes, or the average length of one step. Based on the number of steps towards each beacon node, ordinary sensor nodes examine the shortest route by receiving the averages of the step lengths and finding the interval between the beacon nodes. The distance of their locations is calculated using the mentioned estimate.

Other networks are totally different to WSNs. In wireless communications, security is worth a great deal. Unknown range of the wireless nodes makes them vulnerable to different kinds of threats and onslaughts. The nodes scattering in an unknown range are more vulnerable to attacks. Combative nodes receive or substitute false information for true information using the access they gain to wireless nodes. Limitation of node resources and the additional communication load which leads to the termination of node resources are of the major safety requirements. The following are some of the WSNs' safety requirements:

- **Confidentiality of Information:** In wireless communications, confidentiality of information is an essential part. It should be confidential to transmit the information to the wireless network; in other words, the receiver should receive the information only. The codes are used to keep node information, including access keys and node identity information confidential [12, 13].
- **Data Authentication:** Significant data are encrypted and authenticated to ensure the relationships between sensor nodes [12]. Management of the Key is therefore very important and prerequisite in data protection for authentication and coding. The pre-distribution key mechanism offers an effective balance between storage load and processing ability among all key management mechanisms for WSNs and therefore, it is the most suitable mechanism for WSNs. Authentications such as re-planning or controlling sensor nodes are required in a variety of management programs. The offender is able to send messages to any of the nodes within the network; thus, the recipient must ensure that it is an allowed node. Digital signature and coding mechanisms are used to confirm the identity of the sender for the sake of authentications [14, 15].

- **Data Integrity:** Integrity prevents changes being made on data during the data transmission process in the sensor network. Inaccurate or incorrect data usage has catastrophic upshots; therefore, a serious concern is lack of integrity. Certain applications of sensor networks such as healthcare and environmental monitoring rely heavily on the question of integrity, and therefore protection against modifying or intercepting information transmitted through the network is extremely important .
- **Non-repeatability of Data:** non-repeatability of data in WSNs is when the offender penetrates the network and repeatedly attempts to send the received data [12]. The goal of doing so is in order to deplete the energy of the sensor nodes. In this attack the security protocol must detect whether the data is new or repeated and so if the latest is the case, it should throw them away and prevent their increase [16, 17].

The main contributions of this paper are as follows:

- In this paper is proposed a new distance between nodes and beacons in order to decrease of localization error.
- Proposed model improves localization algorithm to overcome the existing drawback of DV-Hop.
- Detecting wormhole attacks in wireless sensor networks based on new distance.
- Proposed model is evaluated based on Probability of wormhole attack detection and Localization error.

The overall structure of this paper is as follows: in Section 2, a review of the literature is made. In Section 3, improved DV-Hop is presented. In Section 4, the results of the simulation are shown and also an evaluation is made of the proposed model and its results and eventually the proposed model and DV-Hop model are compared. Finally, Section 5, there are the conclusions and discussion concerning future works.

II. RELATED WORKS

In [18], a model against Sybil attack for discovery and defense on DV-Hop is proposed. Assessments results demonstrated that the model can extraordinarily improve the security of the node localization in WSN. When the number of beacon sensor nodes are 50, the proposed model is decreased the average localization error by 3% than the common DV-Hop.

A new DV-hop based on Locally Weighted Linear Regression (LWLR-DV-hop) is proposed [19]. In the proposed model, kernel method is used to improve the localization accuracy by enhance the weight of neighboring beacon nodes. Evaluation models have been done based on two arrangements and three various patterns: the orderly and distributed arrangements, the L-shaped, O-shaped and X-shaped topologies. As efficiency factors, the Average Localization Error and the Cumulative

Distribution Function are applied. The outcomes of Implementation and evaluation demonstrated that LWLR-DV-hop carry outs better than DV-Hop in anisotropic networks of various patterns, in which localization accuracy is repaired by about 40% on average.

DV-Hop often trapped by the wormhole attack that this algorithm is a localization method based on distance vector routing. To dispel this problem, a security DV-Hop localization method against wormhole attack (AWDV-hop) is presented [20]. First, the algorithm makes the neighbor node relationship list (NNRL) by broadcast flooding. All the nodes achieve the ID numbers of their neighbor nodes via NNRL. The malicious beacon nodes can be discovered by comparing the computational and real number of neighbor nodes. Then, the malicious beacon nodes compute the distances to other beacon nodes in their NNRL to discover the real attacked beacon nodes. The attacked beacon nodes in the various regions of wormhole attack are marked with 1 or 2. at last, the unknown nodes sign with 1 or 2 pursuant to the beacon nodes signed previously. In the next round of localization, the nodes signed with 1 and the nodes signed with 2 dismissed from each other. The assessment results demonstrated that the localization error of the proposed AWDV-hop is decreased by about 80% than that of DV-hop algorithm suffering from the wormhole attack. The AWDV-hop is decreased the localization error compared to label-based DV-HOP (LBDV-hop) and secure neighbor discovery based DV-HOP (NDDV-hop) algorithm, by approximately 7 and 34%, respectively.

The accuracy of the DV-Hop is low in computing the average distance per-hop, and it considerably affects the positioning precision. Therefore, a new BFO-DV-HOP (Bacterial Foraging Optimization DV-HOP) model is presented [21]. Compute average distance per-hop in the common DV-Hop algorithm based on the Euclidean distance and the minimum number of hops straightly, and the random dissemination of the anomalous network structure leads to the low precision in average hop distance prediction. In BFO-DV-HOP model, the average distance per-hop is computed by the BFO using the minimum hops of nodes and the position information of beacon nodes. Assessment outcomes demonstrated that 30% beacon beacons can significantly decrease the positioning error, and 10% beacon nodes can get a better efficiency compared with common models.

In localization discussion, the distance vector is common in any localization algorithm, in order to improve location error, an improved localization algorithm based on hop vector distance is presented [22]. Firstly, various connection distances are defined for various nodes. Each distance corresponds to a hop. Second, if the hop number is less than one, the average distance of the nearest anchor node is used as the unknown node distance. In contrast, the weighted average distance of the nearest four beacon nodes are used as the unknown node distance. In the simulations, the proposed algorithm is compared with the distance vector per hop and the distance vector based on the weight per hop. Obtained results demonstrated that the proposed method has less error for localization of unknown node than other models.

In order to minimize the error has been proposed a new distance error correction hop-based models such as DV-Hop [23]. It has been simulated in MATLAB for the results confirmation and comparison. In addition, the efficiency of the proposed model is measured for different metrics such as the average localization error, error variance and accuracy in match to the parameters like the total node number, the beacon node and range. Assessment results illustrated that the proposed error correction-based method reported in this paper performed outstandingly well against the common DV-Hop, improved DV(IDV) Hop and Particle Swarm Optimization (PSO) based DV-Hop and so improved the overall localization operations of the total network.

Wormhole-free DV-hop Localization scheme (WFDV) [24] model has been proposed based on beacon for the detection of wormhole attack. In WFDV, nodes distance and data-distribution messages are broadcast. Detecting attacker node based on distance vector is held up to beacon. The results obtained in 1000×1000 circumference with 100 sensor nodes have shown that WFDV detection accuracy is more than DV-Hop. A new security model has been proposed based on sensor radius for detecting wormhole attack [25]. In the proposed model, each sensor is related only to the neighboring nodes. Evaluations made in 100×100 area with 50 sensor nodes have shown that the presented model has better operation in comparison with such models as SERLOC model.

K-Means algorithm has been used for detecting and clustering attacker nodes [26] in which the algorithm puts alike nodes into a single group. Identification of neighboring nodes is done by using the HELLO messages. Evaluation on 50 sensor nodes in a 100×100 area showed that the detection accuracy rate of the new model got higher with the increase of fake channels.

three models (iDV-Hop1, iDV-Hop2, and Quad DV-Hop) to localization are proposed [27]. In iDV-Hop1 and iDV-Hop2, all levels of the DV-Hop are saved, and multiple levels based on geometry improvements of the localization problem are combined to catch better localization accuracy. The Quad DV-Hop programmed the localization problem as bounded least squares problem, to be solved by quadratic model. Assessments are done on the four various types of network environment by including nodes radius range, number of beacon nodes and number of sensor nodes. Comparison of models with the DV-Hop and Improved DV-Hop models are defined. It is shown that iDV-Hop1 can outstandingly decrease the localization error (up to three times) in configurations with atypical structures compared to DV-Hop and Improved DV-Hop. In configurations with atypical structures, iDV-Hop2 and Quad DV-Hop demonstrated better efficiency compared to DV-Hop and Improved DV-Hop (up to 11 % lower localization error).

In WGDD [17] for detection of wormhole attack is used the geographical distance of sensor nodes. The shortest path for data transmission can be found in WGDD based on Digester algorithm sensor nodes. Obtained results in 100×100 area with 50 sensor nodes showed that the attacker nodes detection rate was more accurate in comparison with DV-Hop. A model has been proposed based on

radio radius and ID of sensor nodes for detecting wormhole attack [28]. In the proposed model, the sensor ID of every node is stored in distance vector, and on sending data to a neighboring node the ID is first assessed. The proposed model has a 100% detection accuracy rate for 50 sensor nodes in a 100×100 circumference.

In Fully-Monitored Criterion model (FMC) [29], the network area decoration is grid and each sensor set out to send data only in the area that belongs to it. Sensor range is divided into eight 16×16 parts, and if any node wants to collaborate in localization of data-transfer in multiple-step area the node will not be headed and will be regarded as an attacker node. The detection accuracy of this model equals 85% for 25 sensor nodes in a 100×100 circumference. LITEWORP [30] model based on sensor wear has been proposed to confront wormhole attack. Obtained results in 80×80 and 204×204 circumference with 20-150 sensor nodes have indicated that detection accuracy of LITEWORP equals 95% and has been able to detect attacker nodes with high accuracy. Ad hoc On-demand Distance Vector (AODV) [31] protocol which is among the common localization protocols with a change in the calculation of Euclidean distance has been proposed to prevent wormhole. Obtained results on 100×100 area with 50 sensor nodes by the enhanced AODV has better operation ability than the ordinary model and can detect the attacker nodes better.

Improvement of Wormhole attack detection is proposed based on the beacon nodes [10]. In the mentioned model, beacon nodes with their specifications taken from neighboring nodes, guard and help localization during data-transfer. Obtained results on 50×50 area with 50 sensor nodes showed that detection accuracy rate increased based on increase number of beacons and has better detection rate in comparison with common method.

Visual-Assisted Wormhole Attack Detection (VA-WAD) model [32] is proposed based on detecting connections between attacker node and attacker node. A circular model for the detection of connections between sensor nodes was used in this model. In the circular model, the primary decoration of the sensor nodes removes the attacker nodes. The accuracy of detection in an area of 100×100 with 50 sensor nodes is proven to be 98%. A new range-free model based on superiority of Genetic Algorithm (GA) to optimize multi-objective functions in computing an unknown position of normal node has been proposed [33]. This model used GA to find the optimal path to real position of unknown node. Simulation is done on four beacon nodes in a square area 50×50, and then 20 unknown nodes are distributed randomly. The proposed range-free localization model is more efficient than range -base models.

The position of the nodes is made use of by researchers as a prevention measure against Wormhole attacks [34]. The locations of the sensor nodes are first stored in a central slim hole and the nodes are only able to send data to nodes neighboring them on their specific positions. The act of localization can go on either one-step or two-step. Obtained results in 1000×1000 circumference with 500 sensor

nodes have proven the accuracy of detection to be 98%. All Distances Test (ADT) [35] model has been proposed based on sensor nodes distance to prevent wormhole attacks. In the mentioned model, the interval between neighboring nodes is calculated and in case the threshold value is surpassed, these two nodes cannot make any relations. Obtained results in a 500×500 circumference with 300 nodes have shown that attack detection rate increases with the increase of radio range and sensor nodes.

A new DV-Hop based on correctional average size of a hop, HDCDV-Hop algorithm, has proposed [36]. The generalized model amends the guessed distance between the unknown node and various beacon nodes based on fractional hop count data and nearly precise locations of the beacon nodes data and it apply the generalized Differential Evolution algorithm to get the estimate location of unknown nodes so as to further decrease the localization fault. Assessment outcomes illustrated that proposed model has lower localization error and higher localization precision compared with the common DV-Hop algorithm and different original generalized algorithms.

In order to expand the localization accuracy, an expanded DV-Hop algorithm based on dynamic beacon node set (DANS IDV-Hop) has presented [37]. Specifically, to the existing DV-Hop models which apply whole beacon nodes, DANS IDV-Hop applies section of beacon nodes to take part in localization. Firstly, the selection of beacon nodes is complex discovery into a hybridization optimization problem. For selecting suitable beacon nodes, a new binary particle coding layout and objective function are proposed. Secondly, the Binary PSO (BPSO) algorithm is utilized to build the DANS, and the localization is performed on the DANS. At the end, the continuous PSO algorithm is used to further ameliorate the unknown node locations. Assessment results demonstrated that DANS IDV-Hop has great localization precision than that of the DV-Hop and other DV-Hop based expanded models.

AODV model has been developed to detect attacker nodes [38]. Interval between and the specific ID for each sensor node has been used in their proposed model. Each node can have relationships with other nodes to three steps based on distance. Results obtained from 750×750 circumference with 100 sensor nodes have indicated that the AODV model which has been developed has better function.

Cross-Layer Media access control (CL-MAC) [39] has been proposed based on petri-net for detecting wormhole attacks. Petri net can model such items as bi-processing, co-production, mutual and contrastive exclusion. In CL-MAC model, detecting the attacker nodes has been carried out revolving around factors such as time and coverage limits. In CL-MAC model, petri net deals with attacker using multiple conditional situations for node evaluations.CL-MAC model has proven to have suitable detection accuracy against attacker nodes in a 100×100 circumference with 50 sensor nodes present.

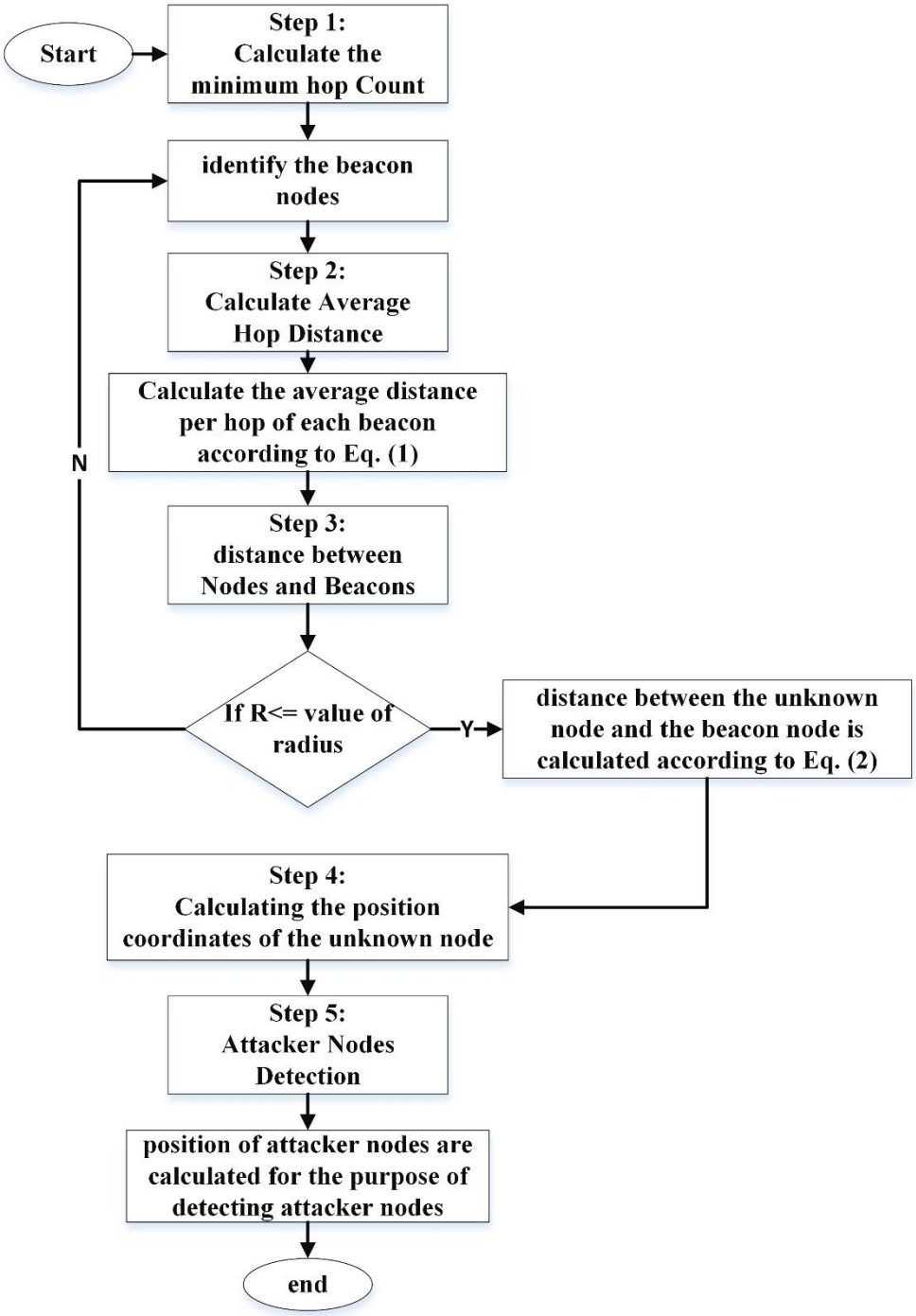

Fig. 1. flowchart of proposed model

III. PROPOSED MODEL

In this section, we proposed an improved DV-Hop to decrease localization errors, which will be based on the deployment of beacon nodes, hop counts between nodes hop size of beacon nodes and size of beacon nodes. The process of the proposed model shown in Fig .1.

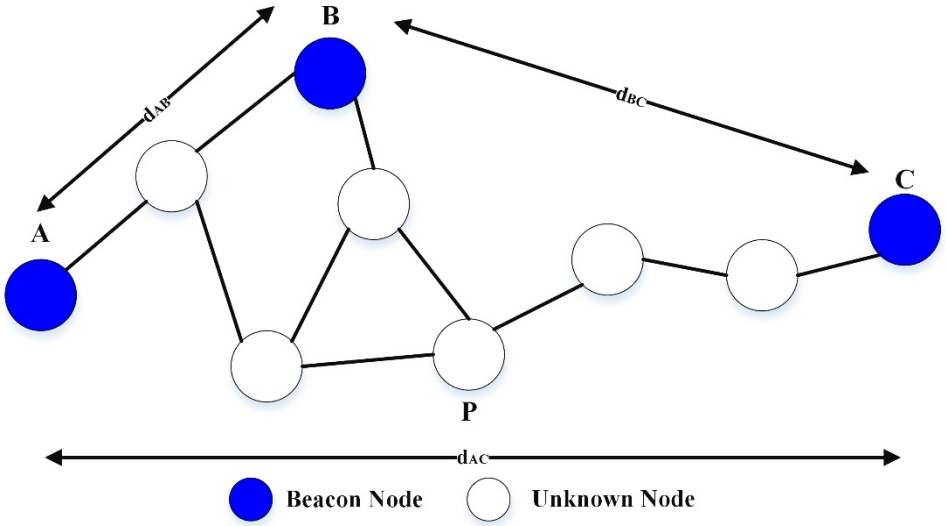

Fig. 2. The illustration of beacon nodes in DV-hop Algorithm.

First Step (Calculate the minimum hop Count): In the proposed model, every beacon node sends a message in the form of $\{id_i, x_i, y_i, hop_i\}$ in the first step. The aim is to identify the beacon nodes. *Id*, *x*, and *y* parameters are the node ids and their positions respectively and hop count is the least amount of distance between the nodes. The shortest path is to be found between each node of the beacon and sensor nodes. The broadcast message of each beacon node includes ID, location, hop count. The minimum hop count message is saved from each beacon node by each sensor node, increasing the hop count value by one and afterward it propagates the message. After this stage, each node keeps routing table $\{ID_i, x_i, y_i, hop_i\}$ where $\{x_i, y_i\}$ shows the position of beacon node (x, y) and the minimum hop count number between sensor nodes is hop_{ij} and beacon node xy_i.

If a packet containing lower hop count value to a specific beacon node is received, hop count value of the table is remodeled with hop count value of received packet, then it is forwarded in the network increasing the hop count value by 1; in other respect, this packet is dropped. Using this scheme, all nodes in the network take minimum hop count value from the present beacon nodes.

Step Two (Calculate Average Hop Distance): At this point, beacon *i*, determines a parameter called $HopSize_i$ its definition is: the average of the distance of one hop. Usually, this parameter is used for converting hop count to physical distance which is calculated by the Eq. (1) [10].

$$HopSize_{ij} = \sum_{i \neq j}^{n} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \Big/ \sum_{i \neq j}^{n} h_{ij} \tag{1}$$

Where (x_i, y_i) and (x_j, y_j) are the coordinates of beacons *i* and j respectively, *n* is the number of beacons and h_{ij} defines the hop count between these two beacons. After this phase, each beacon

broadcasts the calculated $HopSize$ value. The unknown nodes saving only $HopSize$ of the closest beacon, broadcast it again.

Step Three (distance between Nodes and Beacons): an unknown node computes the distance d_{ij} based on Eq. (2) from the beacon nodes by multiplying the $HopSize_i$ to the hop count from beacon nodes after receiving the average distance per hop as Eq. (2). In DV-Hop method, the distance between the unknown nodes and beacon nodes is calculated by taking the average of hop distance and the hop count. It should be noted that the path between the beacon node and the unknown node is mostly not a direct line in practical network. The DV-Hop method will recommend distance errors if used as mentioned. The best way to increase the DV-Hop method localization accuracy is to improve the accuracy of the distance calculation between the beacon nodes and the unknown nodes. This method has so much in common with the DV-Hop method with their difference being that the developed method provides corrections when it calculates the distance between beacon nodes and unknown nodes. Among them, h_{ij} is the hop count between the unknown node *i* and beacon node j, d the average hop, *R* being the communication range of nodes. In this paper, it is proposed a new distance for decreasing localization error. According to Eq. (2), the interval between the unknown node and the beacon node is changed.

$$d_{ij} = \frac{h_{ij} \times (R - d)}{R} + h_{ij} \times d \tag{2}$$

Fourth Step (Calculating the location coordinates of the unknown node): In this step, the location of each unknown node is calculated using Trilateration algorithm and the computational conditions are the distances to the first three contacted beacon nodes acquired in the previous step. Now, the system of equations is designed by taking into account the coordinates of all beacon nodes and their estimated intervals to the unknown node is calculated as follows:

$$\begin{cases} \sqrt{(x - x_1)^2 + (y - y_1)^2} = d_1 \\ \sqrt{(x - x_2)^2 + (y - y_2)^2} = d_2 \\ \vdots \\ \sqrt{(x - x_n)^2 + (y - y_n)^2} = d_n \end{cases} \tag{3}$$

Where (x, y) is the estimated coordinate of unknown node. Eq. (3) can be expanded according to Eq. (4).

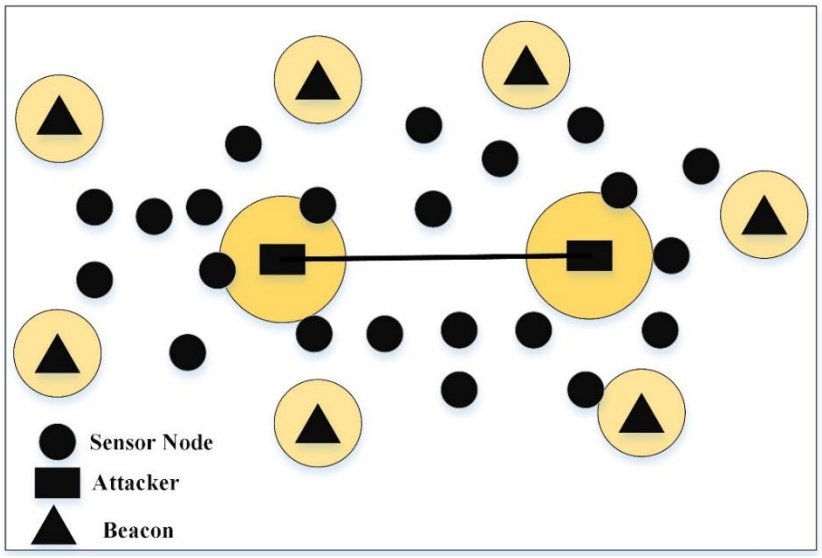

Fig. 3. The radio range of beacon and attacker nodes.

$$\begin{cases} x_1^2 + x_n^2 - 2(x_1^2 + x_n^2)x + y_1^2 + y_n^2 - 2(y_1^2 + y_n^2)y = d_1^2 - d_n^2 \\ x_2^2 + x_n^2 - 2(x_2^2 + x_n^2)x + y_2^2 + y_n^2 - 2(y_2^2 + y_n^2)y = d_2^2 - d_n^2 \\ \vdots \\ x_{n-1}^2 + x_n^2 - 2(x_{n-1}^2 + x_n^2)x + y_{n-1}^2 + y_n^2 - 2(y_{n-1}^2 + y_n^2)y = d_{n-1}^2 - d_n^2 \end{cases} \quad (4)$$

Eq. (4) could be converted into matrix format as $AX=b$, where a, b and X are:

$$A = 2\begin{bmatrix} (x_1 - x_n) & (y_1 - y_n) \\ (x_2 - x_n) & (y_2 - y_n) \\ \vdots & \vdots \\ (x_{n-1} - x_n) & (y_{n-1} - y_n) \end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \end{bmatrix}, \; b = \begin{bmatrix} x_1^2 + x_n^2 + y_1^2 + y_n^2 + d_n^2 - d_1^2 \\ x_2^2 + x_n^2 + y_2^2 + y_n^2 + d_n^2 - d_2^2 \\ \vdots \\ x_{n-1}^2 + x_n^2 + y_{n-1}^2 + y_n^2 + d_n^2 - d_{n-1}^2 \end{bmatrix} \quad (5)$$

The estimate position of the unknown nodes could be determined by calculating this matrix equation with the least square method. By using Eq. (6), the coordinate of the unknown node P could be found. Where A^T represents the transpose of matrix A.

$$X = (A^T A)^{-1} A^T b \quad (6)$$

Fifth Step (Attacker Nodes Detection): The detection of attacker nodes based on radio range is done. The reason for the use of radio range is that attacker nodes have more radio range because of greater amount of energy. However, ordinary nodes have shorter life time in terms of energy. The radio range of beacon and attacker nodes have been illustrated in Fig .3. Attacker nodes have more energy and greater radio range in comparison with beacon nodes.

In the proposed model, Eq. (7) and (8) were used for the entry of attacker nodes into the network. The purpose of these criteria is that first the position of nodes is calculated, next, the position of nodes along with the position of attacker nodes are calculated in order to detect the attacker nodes. Afterwards, the interval of w_p and w'_p values are calculated. The total number of unknown sensor nodes is defined as *N*. If the value of *P* is zero in Eq. (9) the attacker node will not attack the network otherwise the attacker node will be active in the network.

$$w_p = \sum_{i,j\neq 1}^{N} \frac{(x_i - x_j)^2 + (y_i - y_j)^2}{N} \tag{7}$$

$$w'_p = \sum_{i,j\neq 1}^{N} \frac{(x_i - x_j)^2 + (y_i - y_j)^2}{N} \tag{8}$$

$$P = \sum\nolimits_{i,j} (w_p - w'_p)^2 \tag{9}$$

IV. Performance Evaluation

WSNs are wrought of a number of small nodes with little processing memory, limited calculation power, and small radio board [40]. These nodes are related to each other and collaborate with each to transfer data and fulfill their own duties. WSNs should face such problems as the attacks coming from the enemies plus the limited lifetime of the sensor nodes. Wormhole attack is one of the common types of attack made against WSNs. In this type of attack, the offender makes a quick link with little delay between the two spots of the network causing disruptions in the localization protocols. The attack is performed by adding several destructive nodes to the network. This makes nodes which are not physically neighboring to identify each other as neighbors unconsciously.

All experiments are implemented and tested on a PC having the following features: Intel Core i5 2.30 GHz CPU, 6 GB RAM, and a Windows 8.1 operating system. The proposed model has been evaluated and compared with other models in MATLAB 2017a simulation. The tests and simulations were done on 50m×50m, 100m×100m and 200m×200m areas with 100, 200, 300 sensor nodes.

A. Performance Metrics

Regarding the labeling designs of the beacon nodes, as long as the beacon nodes exist in the communication range of two attacker nodes, the beacon nodes can successfully detect wormhole attack. If P_s is the probability of successful detection of attacker nodes by the beacon nodes, and P_f is the probability of a failure to detect attacker nodes by the beacon nodes, then $Ps = 1 - P_f$. Wormhole attack is not detected in two conditions. Condition one: beacon node does not exist

in $D_R(A_1)$. Condition two: beacon node does not exist in $D_R(A_2)$. Beacon nodes are scattered in the network range in a random manner with probability $P(A) = e^{-p_b D_R(A_1)}$. Provided the beacon nodes do not exist in $D_R(A_1)$. Naturally, providing $P(B) = e^{-p_b D_R(A_2)}$ the beacon nodes do not exist in $D_R(A_2)$ [10].

$$P_f = P(A \cup B) = P(A) + P(B) - P(AB) = 2e^{-P_b \Pi R^2} - e^{-P_b D_R(A_1) \cap D_R(A_2)} \tag{10}$$

The probability of attack detection is assessed according to Eq. (11).

$$P_s = 1 - P_f = 2e^{-P_b \Pi R^2} - e^{-P_b D_R(A_1) \cap D_R(A_2)} \tag{11}$$

Since $D_R(A_1) \cap D_R(A_2) = 2R^2$. Hence, the Eq. (12). In Eq. (12), *L* is the length of wormhole length.

$$P_s = 1 - 2e^{-P_b \Pi R^2} + e^{-P_b 2R^2 \arccos \frac{L}{2R} - L\sqrt{R^2 - \frac{L^2}{R}}} \tag{12}$$

Localization error is calculated according to Eq. (13). Eq. (14) is used for calculating the average of localization error of all sensor nodes.

$$e_i = \frac{\sqrt{(x_i - x_i')^2 + (y_i - y_i')^2}}{R} \times 100 \tag{13}$$

$$e_i' = \sum_{i=1}^{n} \frac{e_i}{N} \tag{14}$$

In Eq. (13), (x_i, y_i) are the evaluated coordinates of sensor *i*, and (x_i', y_i'), is the real coordinate of the unknown node *i*, *R* is the communication range of sensor nodes, *N* is the total number of unknown sensor nodes, and *n* is beacon node count. The transmission range of each node equals to 10m. The criteria of position detection and the error rate of the beacon nodes have been used for the purpose of DV-Hop improved. The localization error reflects the accuracy of the localization algorithm. If the localization error is low, the model shows better performance accordingly.

In the proposed model, the distance between all beacons is calculated, if the distance is greater than the radio radiuses, then the nodes in this path are considered as suspicious nodes. The combination of these operations allows the malicious node to be detected if no beacon is inside the wormhole area.

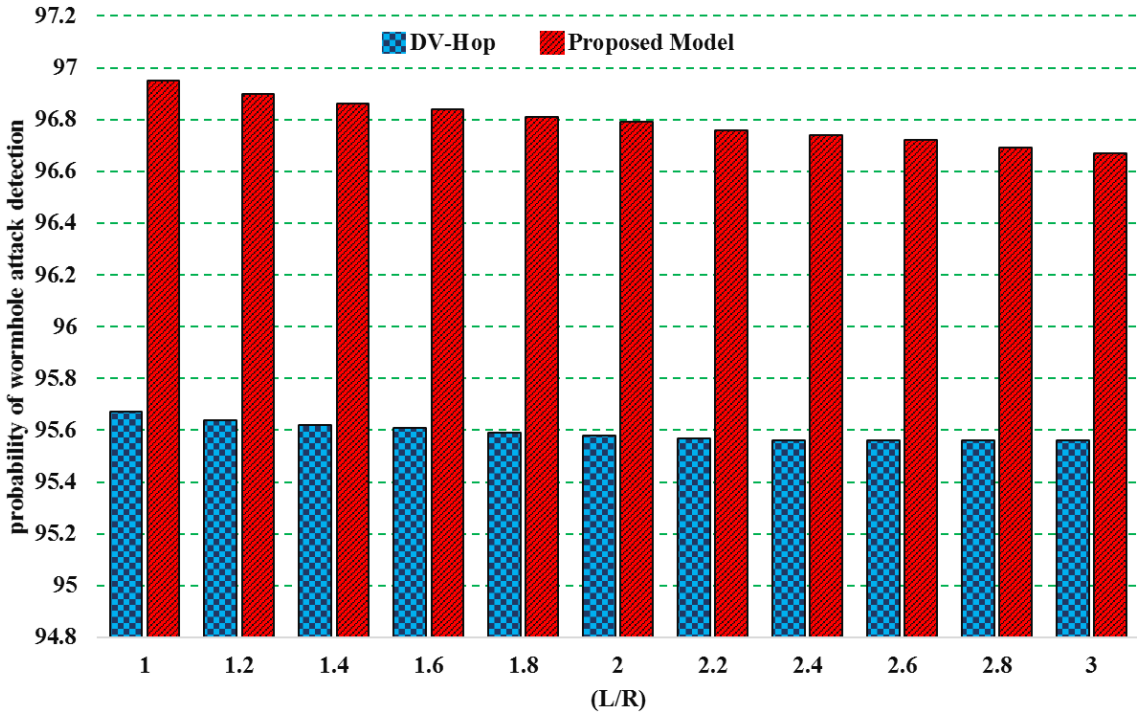

Fig. 4. The probability of wormhole attack detection based on length of link and range for 50m×50m with 100 nodes.

B. Result Analysis

a) Probability of wormhole attack detection

Fig .4 shows the diagram of the probability of wormhole attack detection based on length of link and the radio range (L/R) for 50m×50m with 100 sensor nodes. Based on the indications made in Fig. 4, the detection rate of the proposed model is proven to be higher than the DV-Hop [10]. The proposed model has 96.95% while DV-Hop model has 95.67% detection rate. As shown in Fig .4, the detection accuracy rate decreases as the link length and the radio range increase in the two models. The detection probability in DV-Hop model has stopped at 95.56%. While, the detection accuracy rate of the proposed model has stopped at 96.67%. Hence, it is concluded that the proposed model is stronger for the nodes with longer link length and can detect them better.

According to the results of Fig. 4 if link length is to be shorter, probability of wormhole attack detection in the proposed model and DV-Hop would be higher. In DV-Hop model, with the increase of link length, the percentage of attack detection decreases. However, even with an increase in the link length, the proposed model has higher probability for detection of Wormhole attacks. According to Fig. 4, we can come to the conclusion that even if L/R=3, the proposed model has the probability of wormhole attack detection rate than DV-Hop model in a way that detection percentage in L/R=3 mode is respectively 96.67% and 95.56% for the proposed and DV-Hop models.

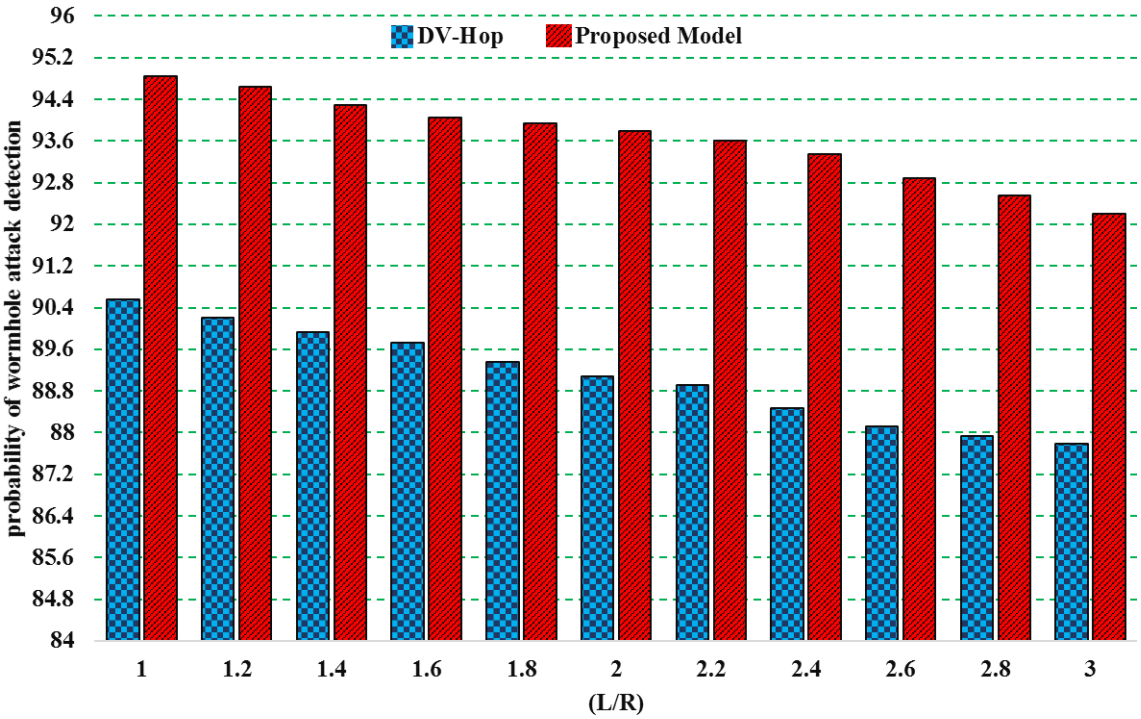

Fig. 5. The probability of wormhole attack detection based on length of link and range for 100m×100m with 200 nodes.

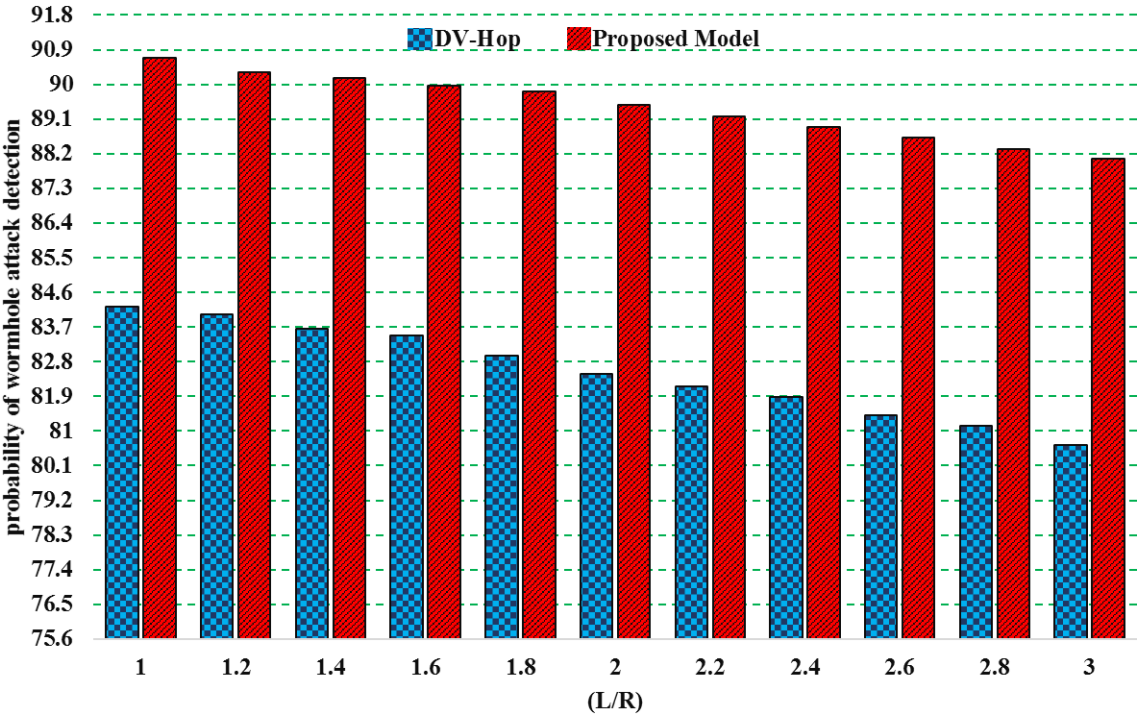

Fig. 6. The probability of wormhole attack detection based on length of link and range for 200m×200m with 300 nodes.

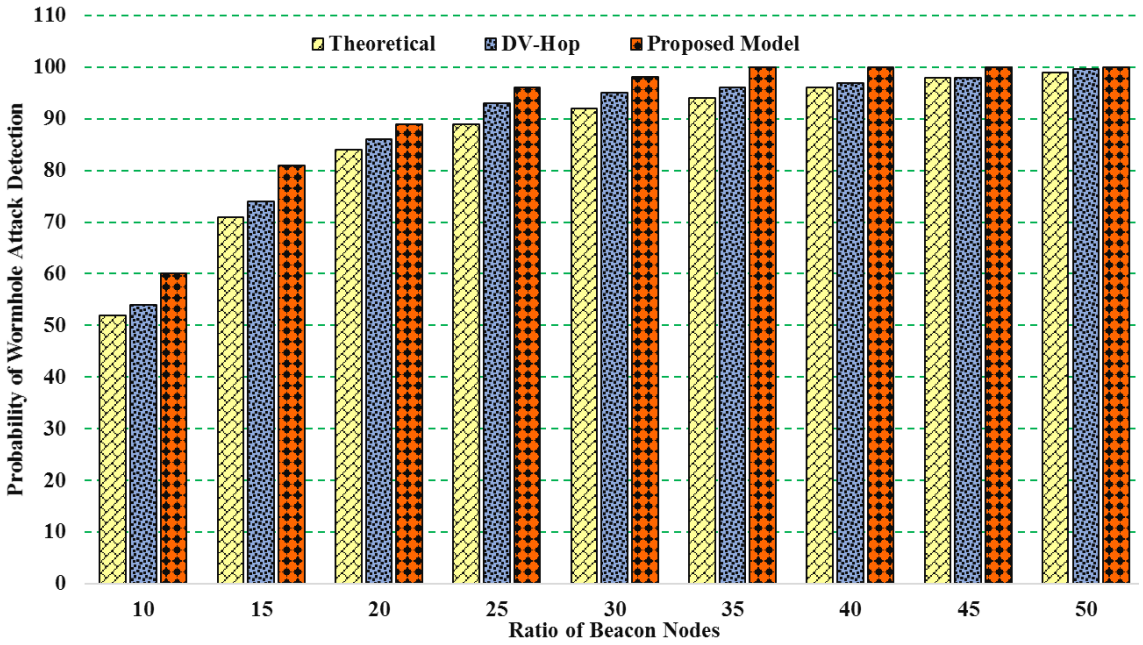

Fig. 7. Wormhole attack detection rate based on the ratio of beacon nodes.

In Fig. 7, wormhole attack detection probability has been shown based on the rate of beacon nodes for 50m×50m with 100 nodes. Fig. 7 indicates the direct relation between increasing beacon nodes directly increasing the probability of wormhole attack detection. Compared to the DV-Hop, the proposed model has higher probability for detecting wormhole attacks. That is because the proposed model uses the model for finding secure routes and calculates the distance length of the beacon nodes and informs the sensor nodes of this information. The probability of wormhole attack detection in DV-Hop model with 50 number of the beacon nodes is 99.6%. Also, the probability of wormhole attack detection in the theoretical model is lower versus the DV-Hop model. Wormhole attack detection rate in the proposed model with 30 beacon nodes present is 98.15% while with 50 number of the beacon nodes the percentage becomes 100%. According to the diagram given in Fig. 7, we can come to the conclusion that the wormhole attack detection rate of the proposed model is higher than DV-Hop and Theoretical models.

Fig. 7 indicates that the proposed model has higher wormhole attack detection rate in comparison with DV-Hop [10] and Theoretical [10] models. If the number of beacon nodes is equal with 40 then the detection percentage in the proposed model, DV-Hop, and theoretical models to be 100%, 97%, and 96% respectively.

b) Localization Error

Fig. 8 shows the localization error with different nodes in areas 50m×50 m, 100m×100m, 200m×200m. Fig. 8 shows the impact of the total number of the nodes on localization error. According to Fig. 8 by increasing the number of nodes in the proposed model, lower localization error

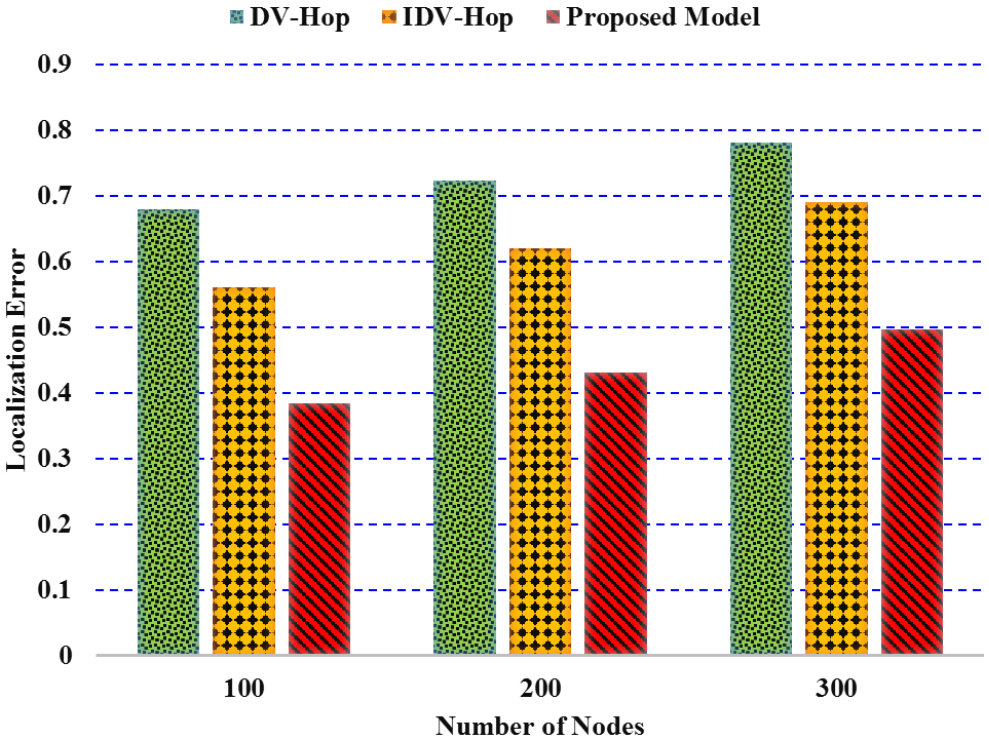

Fig. 8. Average Localization error with different sensor node count.

is achieved in comparison with DV-Hop. Based on the achieved results, it is obvious that the proposed model is better than the DV-Hop and IDV-Hop [41]. *R* is equal to 10m in Fig. 8 and the ratio of beacons is 20%. IDV-Hop [41] has been proposed based on minimum hops correction and reevaluate hop distance. In order to make correct comparisons, we used the IDV model simulation according to the parameters of this paper.

The results of the proposed model in Fig .9 to Fig. 11 are compared with the IDV-Hop [41] model. For correct comparison, the results of IDV-Hop implementation are compared with the proposed model. The aim is that performance of the proposed model in localization error is evaluated. In Fig. 9, the localization error has been presented based on the rate of beacon nodes for 50×50m area. The presented model has less error rate than basic and DV-Hop models. The reason is that the proposed model calculates the position of each beacon node. The highest error rate belongs to basic with attack model. Furthermore, the error rate of the DV-Hop is higher than the proposed and basic without attack models. According to Fig. 9, in the event that ratio of the beacon nodes is in the range of 30, the localization error in the proposed model is 35.12%.

The Fig. 9 to Fig 11 also shows that the proposed model is better in comparison with DV-Hop, IDV-Hop, and basic DV-Hop. According to Fig. 9, in the event that ratio of the beacon nodes is in the range of 25, the average localization error in the DV-Hop is approximately 51% while the proposed model standing on 37.42%.

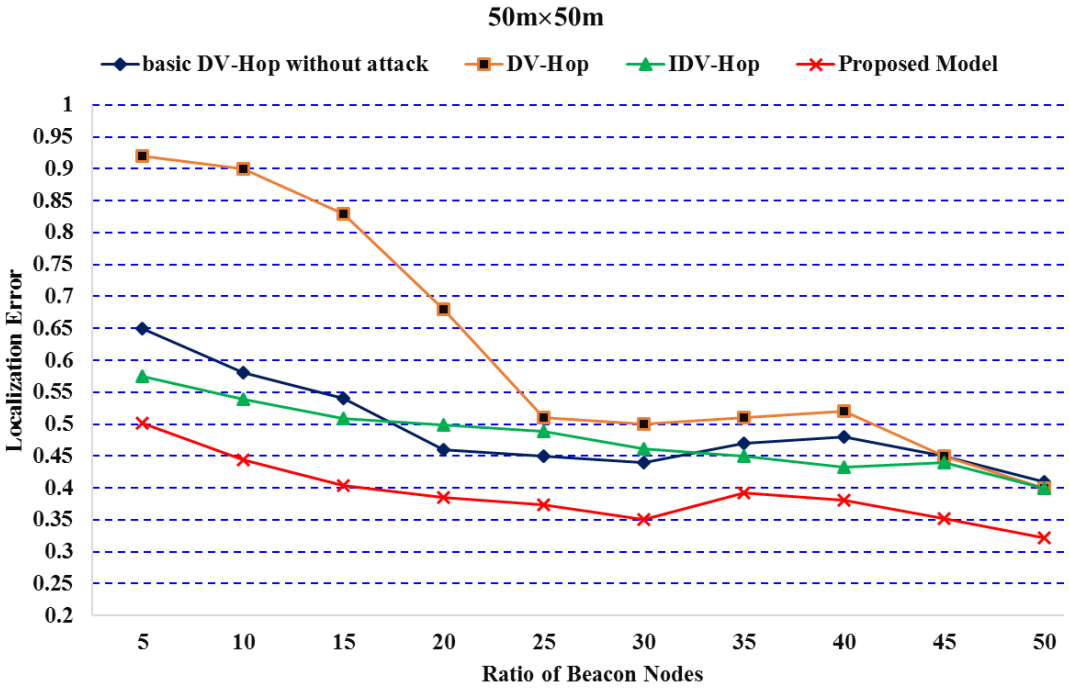

Fig. 9. Comparison of Localization Error based on Beacon Nodes for 50m × 50m with 100 sensor nodes.

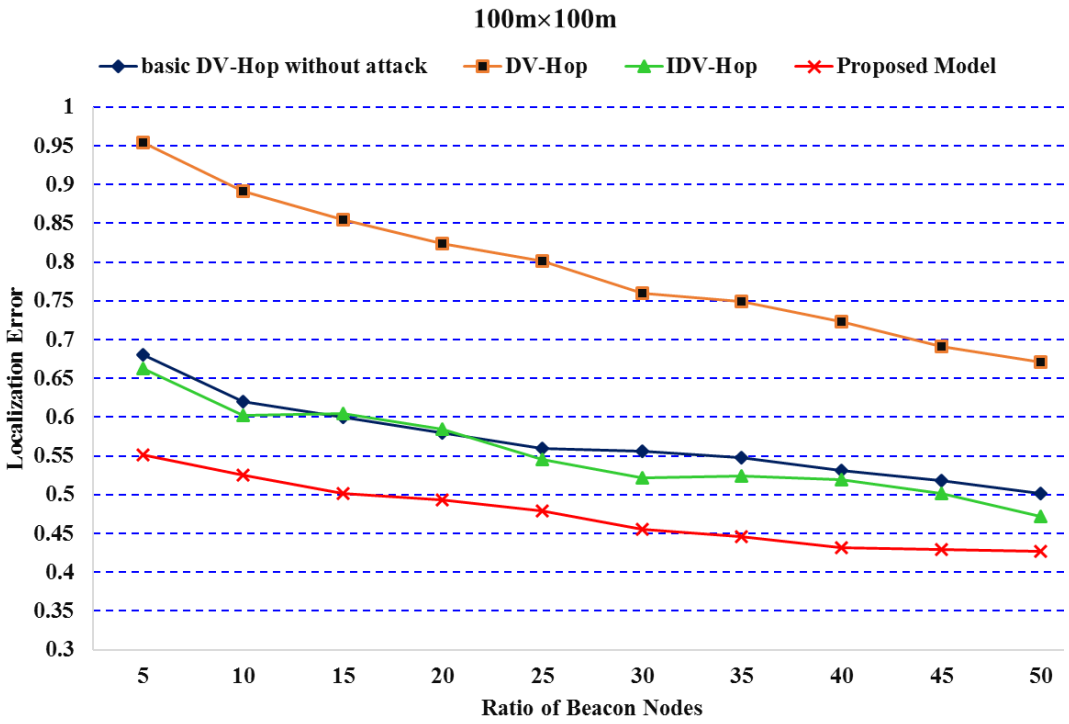

Fig. 10. Comparison of Localization Error based on Beacon Nodes for 100m × 100m with 200 sensor nodes present.

In this section, we compared and evaluated the models based on two criteria, attack detection probability and localization error. The achieved results showed that the proposed model has higher detection accuracy rate than DV-Hop and increase the detection accuracy rate of the proposed model directly related has to increasing the number of beacon nodes.

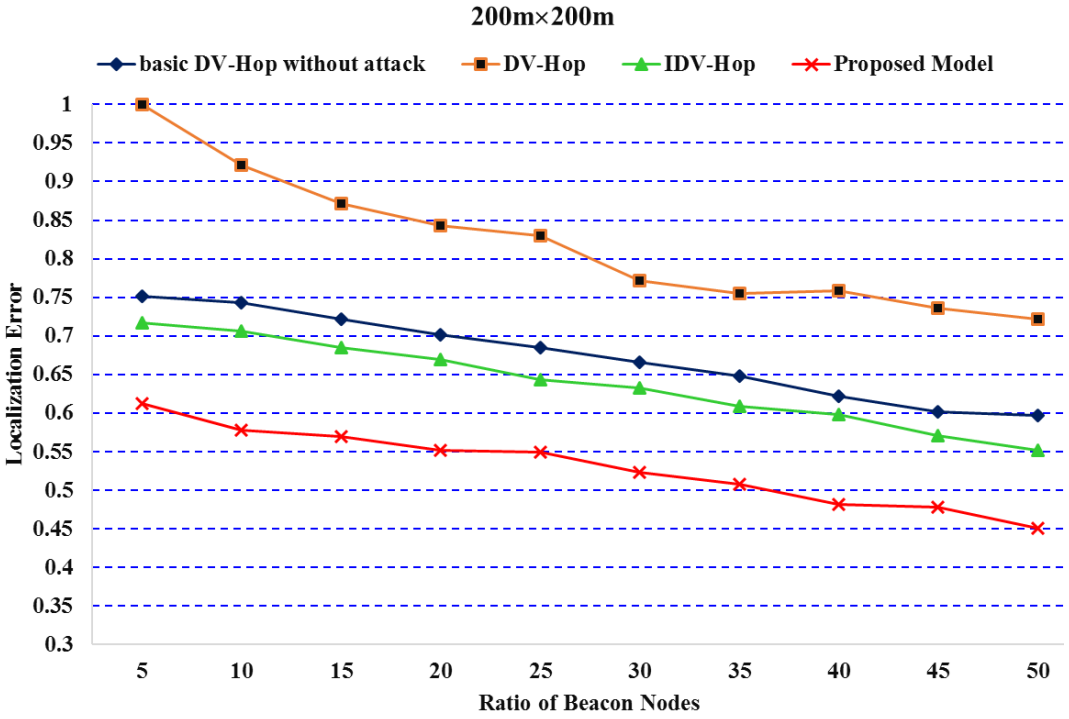

Fig. 11. Comparison of Localization Error based on Beacon Nodes for 200m × 200m with 300 sensor nodes present.

c) Discussion

The location of the sensor nodes in WSNs is one of the most important security assessments. Definition of location goes as a process in which the location of each network node is defined. This process helps to deepen the knowledge about the exact location that the nodes take when an external node enters and it is made aware of the hostile node's existence. Each node should also be positioned when providing data by sensor nodes. Node location information is a key requirement for many sensor network applications. There are two principal categories for the algorithms: centralized and distributed. The data collected is transmitted in centralized algorithms by the processing nodes, and their position calculated into a central database, which could be a small hole node, a guiding node or a special computer database. The results could be communicated to the node or not if necessary.

This method has the advantage of adapting the sensor network to the computational limits of the nodes. The location of security is also useful. Also, there is the disadvantage of large communication overload which is rather useful when moving nodes that are recurrently repeated. By making use of the information gained from their communication with or from the anchor nodes, each sensor node can calculate the position with the distributed algorithms. One of the advantages of this method is its potential for development and the fact that it needs less network communication. This method presents the problem of local errors in the calculations. Of course, in sensor nodes with rather limited resources, this method can be impractical. This is particularly useful when sensor node privacy is considered important. The tracking errors increase in methods that are separate from the guiding

nodes, in comparison to methods used with the guiding nodes, but they are sufficient for many WSNs applications.

To resist the wormhole attack, trust-based security methods can operate effectively since some of the nodes are hostile and cannot be trusted to get reliable information. Trust management procedures are powerful tools for the detection of unexpected network nodes. By pointing out the maladaptive nodes, their adjacent neighbors can utilize this information in order not to cooperate in data transmission, aggregation, and other collaborative activities. Trust power is more successful than traditional encryption methods and can solve problems such as identifying attacker nodes that cryptographic techniques cannot solve. A trust-based routing technique identifies nodes with abnormal functioning by monitoring their behavior and cancels them out of the routing cycle. Identity authentication strategies usually demand a large amount of memory to store vital identity authentication data (for example, shared encryption keys, identity certificates, etc.). Furthermore, received signal strength-based algorithms are not a suitable solution, because the radio signal is matched in the environment nodes with hostile node, consequently, it makes the detection of enemy nodes very demanding.

One of the strategies to tackle the worm attack is to utilize the Received Signal Strength Indicator (RSSI) [42]. Assume that in a sensor network, the two nodes *X* and *A* are neighbors. The *X* node detects the strength of the signal transmitted by node A to be abnormal and far more than the normal amount. This action can be easily implemented using techniques such as Received Signal Strength Indicator, in a manner that the voltage level of the received signal is compared with a threshold, if this number is greater, the signal is identified to be unconventional. The node *X* transmits the identification to the adjacent nodes with a frequency radius of *2r*. *R* is the frequency range of a node in normal mode.

Following the statement of the *X* node, the nodes receiving this message modify their routing table. All nodes delete node *A* from their routing table and the data is not sent to this node. After these actions are taken by node *X*, if this node is faced again with the previous state, this time node *X* will ask the adjacent nodes in the frequency range 2r not only avoid sending anything to this node but also announce their adjacent nodes not to send packages to node *A*. This method is a completely distributed method, so the energy is not wasted to exchange data with the small hole is not wasted and is executed more quickly. This method requires very little processing, and the data exchange between nodes is much less. Therefore, the wormhole attack is detected right away and thwarted.

Wireless communications are susceptible to intruding; therefore, any attacker can control the traffic flow, interrupt the operations, or make fake packets. In this situation, maybe wrong information is sent to the well. Because sensor nodes usually have limited resources and using a short range for transmission, an attacker with a much stronger processor can affect several sensors at the same time

and then change the actual data during the transmission. Since the platform of communication is wireless, the security of these networks is highly significant [1].

V. Conclusion And Future Works

Wormhole attack is one of the most common types of offense made on WSNs. In this attack, two attacker nodes create a short connection in the network topology to collaboration. In wormhole attack, attacker nodes create a short and quick route and suggest other sensor nodes to send the packages through the made link so that they can conduct traffic analyze, package deletion, and package robbery attacks. In this paper, an improved model was proposed based on DV-Hop. The purpose of the proposed model is to increase the wormhole attack detection rate compared to DV-Hop. In the proposed model, the technique of finding the shortest route to the beacon nodes; also, localization error is less in the proposed model than DV-Hop. The proposed model has its method based on the beacon nodes which use distance information and needs no hardware. In this paper to find real neighboring nodes was used list of neighboring nodes. The simulation results in MATLAB 2017a showed that the detection accuracy of the proposed model is higher compared to DV-Hop models. When the number of beacon nodes is 40, the proposed model reduces the detection rate by 3% than the DV-Hop. Future works will be the discussion of the security aspects and large environments in the proposed model.

REFERENCES

1. G. Farjamnia, Y. Gasimov, and C. Kazimov, "Review of the Techniques Against the Wormhole Attacks on Wireless Sensor Networks," *Wireless Personal Communications*, vol. 105, no. 4, pp. 1561-1584, Feb. 2019.
2. M. Sajwan, D. Gosain, and A.K. Sharma, "Hybrid energy-efficient multi-path routing for wireless sensor networks," *Computers & Electrical Engineering*, vol. 67, no. 1, pp. 96-113, April 2018.
3. M. Sadeghizadeh and O.r. Marouzi, "Securing Cluster-heads in Wireless Sensor Networks by a Hybrid Intrusion Detection System Based on Data Mining," *Journal of Communication Engineering*, vol. 8, no. 1, pp. 1-19, Aug. 2019.
4. S. Yahiaoui, M. Omar, A. Bouabdallah, E. Natalizio, and Y. Challal, "An energy efficient and QoS aware routing protocol for wireless sensor and actuator networks," *AEU - International Journal of Electronics and Communications*, vol. 83, no. 1, pp. 193-203, Jan. 2018.
5. M. Patel, A. Aggarwal, and N. Chaubey, Performance Evaluation of Wireless Sensor Network in the Presence of Wormhole Attack, in *Progress in Advanced Computing and Intelligent Engineering*, Singapore: Springer Singapore, Dec. 2019.
6. M. Imran, F.A. Khan, T. Jamal, and M.H. Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs," *Procedia Computer Science*, vol. 56, no. 1, pp. 384-390, 2015.
7. H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 644-653, May 2014.

8. 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, Dec. 2018.
9. M. Patel, A. Aggarwal, and N. Chaubey, Variants of Wormhole Attacks and Their Impact in Wireless Sensor Networks, in *Progress in Computing, Analytics and Networking*, Singapore: Springer Singapore, April 2018.
10. H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xia, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, no. 1, pp. 22-35, Jan. 2015.
11. R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Networks*, vol. 13, no. 1, pp. 27-59, May 2007.
12. B. Bhushan and G. Sahoo, "Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 98, no. 2, pp. 2037-2077, Sept. 2018.
13. J. Cui, L. Shao, H. Zhong, Y. Xu, and L. Liu, "Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 11, no. 5, pp. 1022-1037, Sept. 2018.
14. D. Giri, S. Borah, and R. Pradhan, Approaches and Measures to Detect Wormhole Attack in Wireless Sensor Networks: A Survey, in *Advances in Communication, Devices and Networking*, Singapore: Springer Singapore, May 2018.
15. K. Lee, H. Jeon, and D. Kim, *Wormhole Detection Method based on Location in Wireless Ad-Hoc Networks*, in *New Technologies, Mobility and Security*, H. Labiod and M. Badra, Editors. 2007, Springer Netherlands: Dordrecht. p. 361-372.
16. N. Dutta and M.M. Singh, Wormhole Attack in Wireless Sensor Networks: A Critical Review, in *Advanced Computing and Communication Technologies*, Singapore: Springer Singapore, July 2019.
17. Y. Xu, G. Chen, J. Ford, and F. Makedon, Detecting Wormhole Attacks in Wireless Sensor Networks, in *Critical Infrastructure Protection*, Boston, MA: Springer US, 2008.
18. S. Dong, X.-g. Zhang, and W.-g. Zhou, "A Security Localization Algorithm Based on DV-Hop Against Sybil Attack in Wireless Sensor Networks," *Journal of Electrical Engineering & Technology*, vol. 15, no. 2, pp. 919-926, Feb. 2020.
19. W. Zhao, S. Su, and F. Shao, "Improved DV-Hop Algorithm Using Locally Weighted Linear Regression in Anisotropic Wireless Sensor Networks," *Wireless Personal Communications*, vol. 98, no. 4, pp. 3335-3353, Oct. 2018.
20. 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, March 2018.
21. H. Huang, H. Chen, S. Cheng, and F. Li, An improved DV-HOP algorithm for indoor positioning based on Bacterial Foraging Optimization, in *2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*, Oct. 2016.
22. P. Hu and B. Zhang, An Improved Localization Algorithm Based on DV-HOP in WSN, in *2019 International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI)*, Nov. 2019.
23. D. Prashar and K. Jyoti, "Distance Error Correction Based Hop Localization Algorithm for Wireless Sensor Network," *Wireless Personal Communications*, vol. 106, no. 3, pp. 1465-1488, March 2019.
24. N. Labraoui, M. Gueroui, and M. Aliouat, Proactive Defense-Based Secure Localization Scheme in Wireless Sensor Networks, in *Digital Information and Communication Technology and Its Applications*, Berlin, Heidelberg: Springer Berlin Heidelberg, Sept. 2011.

25. H. Chen, W. Lou, and Z. Wang, A Consistency-Based Secure Localization Scheme against Wormhole Attacks in WSNs, in *Wireless Algorithms, Systems, and Applications*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.
26. B. Tian, Q. Li, Y.-x. Yang, D. Li, and Y. Xin, "A ranging based scheme for detecting the wormhole attack in wireless sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, no., pp. 6-10, June 2012.
27. S. Tomic and I. Mezei, "Improvements of DV-Hop localization algorithm for wireless sensor networks," *Telecommunication Systems*, vol. 61, no. 1, pp. 93-106, Jan. 2016.
28. H. Wang and T. Li, Distributed Detection Approach for Wormhole Attack in Wireless Sensor Networks, in *Advances in Computer Science and Information Engineering*, Berlin, Heidelberg: Springer Berlin Heidelberg, Dec. 2012.
29. R. de Graaf, I. Hegazy, J. Horton, and R. Safavi-Naini, Distributed Detection of Wormhole Attacks in Wireless Sensor Networks, in *Ad Hoc Networks*, Berlin, Heidelberg: Springer Berlin Heidelberg, Sept. 2010.
30. I. Khalil, S. Bagchi, and N.B. Shroff, "LiteWorp: Detection and isolation of the wormhole attack in static multihop wireless networks," *Computer Networks*, vol. 51, no. 13, pp. 3750-3772, 2007.
31. S.M. Naidu and V.B. Himaja, Handling Wormhole Attacks in WSNs Using Location Based Approach, in *Proceedings of the First International Conference on Computational Intelligence and Informatics*, Singapore: Springer Singapore, Dec. 2017.
32. E. Karapistoli, P. Sarigiannidis, and A.A. Economides, Visual-Assisted Wormhole Attack Detection for Wireless Sensor Networks, in *International Conference on Security and Privacy in Communication Networks*, Cham: Springer International Publishing, Nov. 2015.
33. T. Najeh, H. Sassi, and N. Liouane, "A Novel Range Free Localization Algorithm in Wireless Sensor Networks Based on Connectivity and Genetic Algorithms," *International Journal of Wireless Information Networks*, vol. 25, no. 1, pp. 88-97, March 2018.
34. T. Dimitriou and A. Giannetsos, Wormholes No More? Localized Wormhole Detection and Prevention in Wireless Networks, in *Distributed Computing in Sensor Systems*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.
35. L. Buttyán, L. Dóra, and I. Vajda, Statistical Wormhole Detection in Sensor Networks, in *Security and Privacy in Ad-hoc and Sensor Networks*, Berlin, Heidelberg: Springer Berlin Heidelberg, July 2005.
36. G. Liu, Z. Qian, and X. Wang, "An improved DV-Hop localization algorithm based on hop distances correction," *China Communications*, vol. 16, no. 6, pp. 200-214, July 2019.
37. Y. Cao and Z. Wang, "Improved DV-Hop Localization Algorithm Based on Dynamic Anchor Node Set for Wireless Sensor Networks," *IEEE Access*, vol. 7, no. 1, pp. 124876-124890, Aug. 2019.
38. S. Bhagat and T. Panse, A detection and prevention of wormhole attack in homogeneous Wireless sensor Network, in *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, Nov. 2016.
39. A. Louazani, L. Sekhri, and B. Kechar, A time Petri net model for wormhole attack detection in wireless sensor networks, in *2013 International Conference on Smart Communications in Network Technologies (SaCoNeT)*, June 2013.
40. W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Jan. 2000.
41. W. Fang, H. Xu, and G. Yang, Improved DV-Hop Algorithm Based on Minimum Hops Correction and Reevaluate Hop Distance, in *2019 5th International Conference on Information Management (ICIM)*, March 2019.
42. S. Marian and P. Mircea, Sybil attack type detection in Wireless Sensor networks based on received signal strength indicator detection scheme, in *2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics*, May 2015.