The Security DV-Hop Algorithm against Multiple-Wormhole-Node-Link in WSN

Jianpo Li*, Dong Wang
School of Computer Science, Northeast Electric Power University
Jilin, Jilin 132012 - China
[jianpoli@163.com; 1260570211@qq.com]
*Corresponding author: Jianpo Li

Received May 16, 2018; revised August 20, 2018; revised October 14, 2018; accepted November 11, 2018; published April 30, 2019

Abstract

Distance Vector-Hop (DV-Hop) algorithm is widely used in node localization. It often suffers the wormhole attack. The current researches focus on Double-Wormhole-Node-Link (DWNL) and have limited attention to Multi-Wormhole-Node-Link (MWNL). In this paper, we propose a security DV-Hop algorithm (AMLDV-Hop) to resist MWNL. Firstly, the algorithm establishes the Neighbor List (NL) in initialization phase. It uses the NL to find the suspect beacon nodes and then find the actually attacked beacon nodes by calculating the distances to other beacon nodes. The attacked beacon nodes generate and broadcast the conflict sets to distinguish the different wormhole areas. The unknown nodes take the marked beacon nodes as references and mark themselves with different numbers in the first-round marking. If the unknown nodes fail to mark themselves, they will take the marked unknown nodes as references to mark themselves in the second-round marking. The unknown nodes that still fail to be marked are semi-isolated. The results indicate that the localization error of proposed AMLDV-Hop algorithm has 112.3%, 10.2%, 41.7%, 6.9% reduction compared to the attacked DV-Hop algorithm, the Label-based DV-Hop (LBDV-Hop), the Secure Neighbor Discovery Based DV-Hop (NDDV-Hop), and the Against Wormhole DV-Hop (AWDV-Hop) algorithm.

Keywords: wormhole attack, wireless sensor networks, security DV-Hop algorithm, multi-wormhole, neighbor list

http://doi.org/10.3837/tiis.2019.04.027 **ISSN : 1976-7277**

1. Introduction

Wireless Sensor Networks (WSN) consists of a large number of stationary or moving sensors with self-organizing and multi-hop characteristics [1].It is commonly used to collaboratively perceive, collect, process, and transmit information about perceived objects within a geographic area of a network. In WSN, the unknown nodes communicate with the beacon nodes to acquire the corresponding information and use the certain rules to locate themselves. This technology, which is called node localization technology, is widely used in environmental awareness, military monitoring, etc. Node localization is one of the core functions in WSN [2]. Usually, WSN is deployed in the secure environment by default, but any premeditated attack will have serious consequences for it. The DV-Hop algorithm plays an important role in range-free localization algorithm because of wide application, but it is vulnerable to the wormhole attack [3].

The wormhole attack can damage the routing structure and interfere with the routing for data transmission [4]. A wormhole link usually consists of two or more designated attack nodes [5,6]. Because the wormhole attack has no effect on communication integrity, it is difficult to be detected [7]. There are three types of wormhole attack, including packets tampering, replaying data packets with high power, and out-of-band hidden channel [8,9]. This paper mainly concentrates on the third type. One attack node receives information from normal nodes and sends the information through the other corresponding attack node(s) [10]. It means the attacked nodes can receive information from other attacked nodes, although they may not receive before.

Once WSN is attacked by the wormhole link(s), it will disrupt the broadcast flooding of DV-Hop algorithm [11]. When the beacon nodes calculate the average hop distances, other nodes will obtain the incorrect hops, resulting in a sharp increase in average hop distance [12]. Moreover, the unknown attacked nodes obtain the erroneous hops and average hop distance, resulting in a sharp growth in the localization error. The attacked nodes will also receive a large amount of forwarding information, it will greatly increase energy consumption and reduce network lifetime. Therefore, how to decrease the influences of wormhole attack is very important.

Currently, researches have limited attention to Multi-Wormhole-Node-Link (MWNL). The schemes against wormhole attack focus on four aspects: the routing, the nodes exclusion, the hardware, and the algorithm optimization.

In the routing part, Multi-path transmission is used to resist the wormhole attack [13], the data packets of source nodes are transmitted to the destination node through different paths. Reference [14] and [15] uses the different paths to detect the wormhole attack. The data packets of different paths are compared to find the paths that suffer from wormhole attack, and then the attacked paths are filtered out. Both of them can find and filter the wormhole links effectively, but they need to establish different paths in advance, which consume a large number of network resources and reduce the efficiency of data transmission as well as network lifetime.

In the nodes exclusion part, reference [16] and [17] modified the DV-Hop algorithm. It closes all the attacked nodes to resist the wormhole attack, but it will also close numbers of normal nodes. Security DV-Hop (SDV-Hop) [18] is an algorithm against wormhole attack based on the upper limit of localization error. The beacon node whose error exceeds the upper

limit will be removed from the network. The loss of the beacon nodes also causes the waste of network resource.

In the hardware part, the Round-Trip Time (RTT) is proposed in [19] and [20]. The RTT method requires the nodes to add the clock synchronization modules. The nodes can detect and exclude the attacked routing paths by comparing transmission time and the average time difference, but the clock synchronization is needed. Reference [21] and [22] use the time stamp. The transmission time is used to estimate the distance between nodes and it can detect the attack nodes effectively. However, it also requires clock synchronization module that increases the cost of networks significantly. The Senleash proposed in [23] requires the nodes to add the directional antenna. It can exclude the attack node by the transmitting direction of signal. Reference [24] and [25] add the measurement module for signal strength. It can find the attack nodes through measuring the transmission and reception signal strength. Then the nodes in network take corresponding measures to avoid suffering wormhole attack. These methods can eliminate the wormhole attack effectively except for the increase on networks cost.

In the algorithm optimization part, reference [26] and [27] use the average hop distance to detect attacked nodes. When the wormhole attack exists, the attacked beacon node will correct the hop count automatically. It does not add too much work burden, but it has limited effects on resisting wormhole attack. The against wormhole DV-Hop (AWDV-Hop) algorithm [28] combines the nodes exclusion with node marking. It can avoid the influence of wormhole attack effectively. However, it cannot solve the MWNL problem. In addition, the algorithm also adds the localization error to a certain extent in the marking process.

Based on the analysis above, there are two main problems in the research of the wormhole attack. The first is that the current researches focus on DWNL and have limited attention to MWNL. The second is that the current methods for resisting wormhole attack have some problems, such as requiring precise clock synchronization and directional antennas, or at the expense of a loss of numerous nodes, etc. So an improved security DV-Hop localization algorithm is proposed to resist the wormhole attack. The proposed algorithm is applicable to the DWNL and the MWNL. The algorithm uses flooding routing protocol to establish the Neighbor List (NL). All the nodes can obtain the information of neighbor nodes through the NL. When the numbers of neighbors exceed the threshold, it will trigger the attack detection.

The rest of this paper is organized as follows. Section 2 introduces the principle of DV-Hop localization algorithm and execution process. The third part is the core of this paper. It mainly proposes the AMLDV-Hop algorithm and describes its principle in detail. In section 4, we analyze the simulation results under the different conditions. And the conclusion is made in section 5.

2. Basic Principle of DV-Hop

The DV-Hop localization algorithm can locate unknown nodes based on the distance vector routing. During the initialization phase of DV-Hop algorithm, the flooding protocol is used to transmit the data packets of the beacon nodes to the other nodes in the network. The algorithm steps are as follows [3].

Step1. Calculating the minimum hop counts

Each beacon node broadcasts a data packet $\{ID, x, y, hops\}$. The symbol ID represents the identity number, (x, y) represents the coordinate of beacon node and $hops$ represents the hop counts. The data packet of each beacon node is sent to other nodes in the network by broadcast flooding which is also used in DV-Hop algorithm. When other node receives the packet, the

hop count will plus 1. At the same time, the minimum hops is saved. Then the packet is forwarded to the neighbor nodes. For the same data packet, each node in the network forwards the data packet only once to the neighbor nodes, it will ensure that the broadcast flooding is in control.

Step2. Calculating per hop distance

Each beacon node estimates the average hop distance based on the localization information of other beacon nodes and hops count. The average hop distance $\overline{d}$ can be calculated as:

$$\overline{d} = \frac{\sum_{j \neq i} \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}}{\sum_{j \neq i} hops_{ij}} \tag{1}$$

where (x_i, y_i) and (x_j, y_j) are the coordinates of beacon node X_i and beacon node X_j, $hops_{ij}$ is the hops between beacon node X_i and beacon node X_j. The unknown node will save the first received average hop distance. When the unknown node receives and saves the average hop distance, it multiplies the average hop distance and the minimum hops to get the distance between itself and the beacon node.

Step3. Calculating the node coordinates

When the unknown nodes obtain three or more distances from beacon nodes, their coordinates can be calculated by using the method of three-side-measuring.

3. AMLDV-Hop Algorithm against Wormhole Attack

The proposed AMLDV-Hop algorithm is applicable to DWNL and MWNL. The scheme consists of four parts: the detection of wormhole attack, the determination of wormhole link composition, the resistance scheme of wormhole attack, and the analysis of error source and special cases. The proposed algorithm uses the flooding protocol to transmit the data packets of beacon nodes or the neighbor information. After finishing the flooding process, each node in the network can acquire the data packets of other beacon nodes and the ID of their neighbor nodes. The security algorithm can find the suspect beacon nodes through the number of neighbor nodes. Each suspect beacon node determines whether it is under attack. Each attacked beacon node generates and broadcasts the conflict set. Then each attacked beacon node is marked according to the principle of progressive marking. Each attacked unknown node mark itself according to the marked beacon nodes. The unknown nodes, which are marked unsuccessfully, mark themselves according to the unknown nodes that have been marked already. The unknown nodes that still fail to be marked are semi-isolated. In some special case, they will be removed from the network.

3.1 WSN Model

For research convenience, we define the network as follows [28].

(1) The type of wormhole attack defaults to the out-of-band hidden channel, which doesn't involve information tampering.

(2) All the nodes including attack nodes are static.

(3) All the nodes including beacon nodes and unknown nodes know their own ID numbers, and the beacon nodes know their own coordinates.

(4) The nodes are evenly deployed in an area of $L \times L$.

(5) The broadcast flooding is controllable. For the same data packet, each node in the network forwards the data packet only once to the neighbor nodes.

3.2 Wormhole Attack Detection

In order to detect the wormhole attack, some schemes need the mutual information after network initialization. The mutual information maybe includes signal orientation vector, signal arrival time difference, routing feedback information, etc. The mutual information not only need to be transmitted among nodes, but also need to be further processed by nodes. During node localization, the beacon nodes provide some convenience to detect the wormhole attack. It is very convenient to establish NL in the initialization phase through the routing protocol. After the initialization phase, the nodes already have enough information (such as coordinate information of nodes) to detect the wormhole attack rather than acquiring additional mutual information from other nodes. Using these network resources rationally is helpful to reduce energy consumption during the process of detection. So we propose the following detection method.

Firstly, we can use the formula (2) to calculate the density of nodes n:

$$n = N/L^2 \tag{2}$$

Assume that the communication radius is R, its communication area S is:

$$S = \pi R^2 \tag{3}$$

As the nodes are evenly deployed in the network approximately, the number of neighbor nodes h for every node can be calculated as:

$$h = (\pi R^2) N/L^2 \tag{4}$$

Because of the forwarding property of the wormhole attack, the nodes affected by attack nodes in different wormhole areas can communicate with each other. If one wormhole link is composed of m attack nodes, the neighbor nodes of the attacked nodes turn into mh.

In practice, the nodes including the attack nodes may be distributed at the edge of the geographic. So we propose the Suspect Node Determination Coefficient G to reduce the misjudgment of the suspect nodes.. When a node determines that the number of neighbor nodes M is greater than threshold K, the node is considered as a suspect node. Threshold K is:

$$K = hG \tag{5}$$

In order to obtain good performance, the coefficient G should be reasonable. If the wormhole link is composed of m attack nodes, the number of neighbor nodes of the attacked node is mh theoretically. The range of G should be $1 < G < m$. So G can be evaluated from 1 to m, increasing 0.01 each time. Through comparing the node misjudgment rate and the unjudged node rate for different K values, the best coefficient G can be obtained.

The nodes whose neighbor nodes are more than K will be judged as attacked nodes. Some normal nodes, whose neighbor nodes are more than K because of the uneven distribution of nodes in some cases, may be misjudged as attacked nodes. Correspondingly, some attacked nodes, whose neighbor nodes are less than K because of the uneven distribution of nodes in some cases, may be misjudged as normal nodes. By numerous simulations, we can know how many nodes are misjudged for the different G values. Here we propose two indicators to measure whether the value of G is the best. One is node misjudgement rate (the ratio of normal nodes which are misjudged as attacked nodes to the whole attacked nodes) and the other is unjudged node rate (the ratio of attacked nodes which are misjudged as normal nodes to the whole attacked nodes). The smaller the values of two indicators are, the better the value of G is.

The number of neighbor nodes M can be obtained as follows.

Step1. Each node initializes NL and hop count, the initial value of hop count is 0.

Step2. Each beacon node broadcasts a data packet $\{ID, x, y, hops\}$.

Step3. When other nodes receive this packet, the hop value will plus 1. For the packet from the same beacon node, every node which has received this packet checks the hops and saves the minimum hops. This packet with the node ID number will continue to be forward to next neighbor nodes. According to the received ID number and its own ID number, each node can set the Corresponding Value of Relationship (CVR) to 1 in NL, which is shown in **Table 1**.

Table 1. The NL of node X_i

CVR (Node / Node)	X_2	X_3	X_5	.....	X_N
X_i	1	1	1	.....	1

X_2 X_3 X_5 ….. X_N represent the nodes. After the flooding process, the CVR of X_i to a certain node is set to 1 if this node can communicate with X_i. Through the NL, node X_i can obtain the number of neighbor nodes and the ID.

If $M > K$, the beacon node determines itself as a suspect beacon node. The distances from the other beacon nodes whose CVR are 1 in NL is:

$$d_{X_i X_j} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \tag{6}$$

where, $X_i\ (x_i, y_i)$ is the suspect beacon node, $X_j\left(x_j, y_j\right)$ is the other beacon node that can communicate with the suspect beacon node. If $d_{X_i X_j} > R$, WSN is under attack.

Some papers also propose the detection schemes by calculating the average hop distance $\overline{d}$ between every two beacon nodes. If $\overline{d} > R$, it indicates that the network is under attack. It can detect the wormhole attack effectively, but calculating $\overline{d}$ is still troublesome. The proposed detection scheme of wormhole attack uses NL to find the suspect beacon nodes. It can reduce the calculation amount and the number of beacon nodes involved in the calculation. So the computation complexity and energy consumption can be decreased.

3.3 Wormhole Attack Resistance Scheme

For current problems, we propose AMLDV-Hop algorithm which is applicable to DWNL and MWNL. This paper takes the MWNL which is composed of three attack nodes as an example.

Symbol B represents beacon nodes, S represents unknown nodes, W represents attack nodes, the subscript represent their ID numbers. U_1, U_2 and U_3 represents the set of nodes within the circle with the center point W_1, W_2, and W_3 respectively. U_1, U_2 and U_3 are considered as the sets of different wormhole areas, the areas affected by the attack nodes are called different wormhole areas. $U_R\left(B_i\right)$ is the set of beacon nodes which can communicate with the beacon node B_i, R is communication radius, i is its ID number.

Similarly, $U_R(W_1)$, $U_R(W_2)$, $U_R(W_3)$ are the set of beacon nodes in the set of U_1, U_2 and U_3 respectively. U_a is the conflict set. Assumed that only beacons nodes can generate the conflict sets. In **Fig. 1**, the conflict set of B_1 is $\{B_2, B_3, B_5, B_6, B_7, B_8\}$.

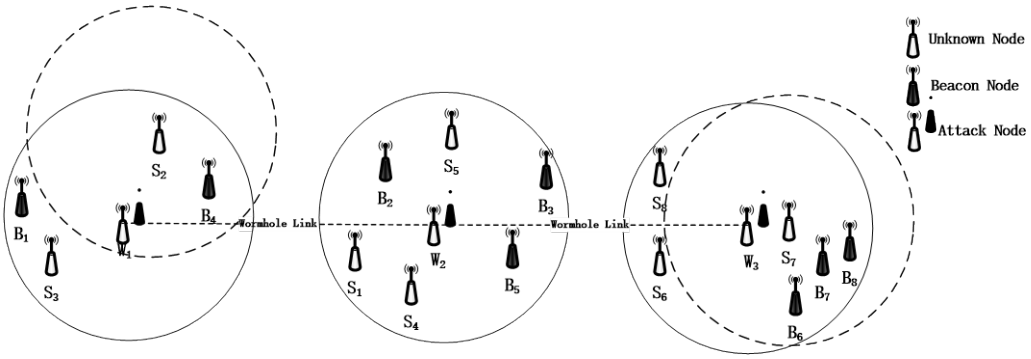


Fig. 1. The marking process of attacked nodes

Theorem 1: The beacon nodes in the same wormhole area have the same conflict set U_a.

Proof: If $\exists B_i \in U_1$, there must be $U_R(W_2) \in U_R(B_i)$ $U_R(W_3) \in U_R(B_i)$. If $U_1 \cap U_2 \cap U_3 = \varnothing$, the distances between B_i and other beacon nodes in $U_R(W_2)$ and $U_R(W_3)$ should meet $d > R$. So by the individual to the whole, $\forall B_i \subset U_1$, $U_1 \cap U_2 \cap U_3 = \varnothing$, the distances between B_i and the other beacon nodes in $U_R(W_2)$ and $U_R(W_3)$ should meet the condition of $d > R$. Similarly, $\forall B_i \in U_2$, the distances between B_i and the other beacon nodes in $U_R(W_1)$ and $U_R(W_3)$ should meet the condition of $d > R$ for $\forall B_i \in U_3$, the distances between B_i and the other beacon nodes in $U_R(W_1)$ and $U_R(W_2)$ should meet $d > R$, that is, the beacon nodes in the same wormhole area generate the same conflict set.

3.3.1 Mark the Beacon Nodes

The process to mark beacon nodes: In AMLDV-Hop algorithm, the determination of wormhole link composition and the marking process of beacon node are synchronized. The beacon nodes which have definite position can be used to distinguish different wormhole areas. It has following steps:

Step1. According to the NL, each beacon node judges whether it is the suspect beacon node.

Step2. All the suspect beacon nodes calculate the distances from the other beacon nodes whose CVR are 1 in the NL. Each suspect beacon node gets a distance set $\{d_1, d_2 ..... d_M\}$.

Step3. Each suspect beacon node compares the value of $d_i (i = 1, ..., M)$ with R. If $d_i > R$, the beacon node is under attack. Once the beacon node determines it is attacked, it saves own ID number and the target ID number of beacon node. Then the attacked beacon node generates a conflict set U_a and sends it out. This conflict set will be received by other nodes to determine whether they are attacked.

Step4. The beacon node receives U_a packet and then judges whether it belongs to U_a. If it belongs to U_a and has been judged as a suspect beacon node, which shows that the beacon node finish step 2 and step 3. If it belongs to U_a but has not been judged as a suspect beacon node, the beacon node will perform step 2 and step 3 to determine whether the suspect beacon node is actually attacked. If the beacon node is under attack, the attacked beacon node generates and broadcasts U_a packet.

Step5. According to the theorem 1, it can be concluded that the number of conflict sets generated by the attacked beacon nodes and the attack nodes are equal. If there is one wormhole link which is composed of three attack nodes in WSN, the attacked beacon nodes will generate three different conflict sets. So we can use the conflict sets to determine the composition of wormhole link.

Step6. Each attacked beacon node marks itself according to the conflict sets.

When there is MWNL in WSN, each attacked beacon node can obtain m different conflict sets. Each attacked beacon node calculates the common set in every two conflict sets. Then each attacked beacon node finds the smallest ID of beacon node in each common set. Finally, the attacked beacon node is marked with $1,2,....,m$ according to the marking principle of beacon nodes. There are three cases during the marking process.

(1)No overlapping between the different wormhole areas

Fig. 1 is the most basic spatial distribution of the wormhole attack, there is no overlapping between the different wormhole areas. In **Fig. 1**, the specific marking process is as follows.

Step1. Beacon node B_1 calculates the distances to other beacon nodes in $U_R(B_1)$. The distance set is $\{d_{B_1B_2}, d_{B_1B_3}, d_{B_1B_5}, d_{B_1B_6}, d_{B_1B_7}, d_{B_1B_8}\}$.

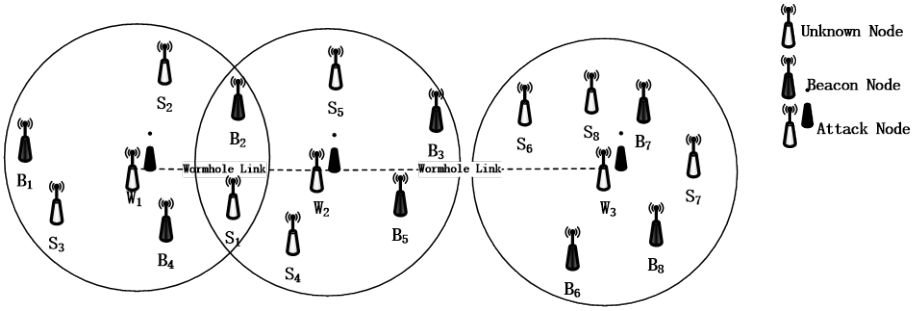
Step2. The beacon node B_1 compares the values of $d_i\ (i=1,....,M)$ with R. The results will be $d_{B_1B_2} > R$, $d_{B_1B_3} > R$, $d_{B_1B_5} > R$, $d_{B_1B_6} > R$, $d_{B_1B_7} > R$, $d_{B_1B_8} > R$. It indicates that the communication radius of the beacon node B_1 is greater than R and the beacon node B_1 is under attack. Then the beacon node B_1 generates conflict set U_a as $\{B_2, B_3, B_5, B_6, B_7, B_8\}$. Finally, the beacon node B_1 sends the U_a packet to other nodes.

Step3. After receiving the U_a packet sent by node B_1, the nodes B_2, B_3, B_5, B_6, B_7 and B_8 calculate the distances to other beacon nodes whose CVR are 1. Each of them generates a distance set $\{d_1, d_2, \ldots, d_M\}$ respectively and compares the values of $d_i\ (i=1,....,M)$ with R. Finally, the conflict set U_a of the beacon nodes B_2, B_3 and B_5 is $\{B_1, B_4, B_6, B_7, B_8\}$, the conflict set U_a of the beacon nodes B_6, B_7 and B_8 is $\{B_1, B_4, B_2, B_3, B_5\}$.Each of them sends the U_a packet to other nodes. When node B_4 received the U_a packets sent by the beacon nodes B_2, B_3, B_5, B_6, B_7 and B_8, the beacon node B_4 belongs to U_a but has not been judged as a suspect beacon node. The node B_4 will re-determines itself as a suspect beacon node. Then it carries out the Step2 and generates the conflict set U_a as $\{B_2, B_3, B_5, B_6, B_7, B_8\}$. When the beacon nodes B_2, B_3, B_5, B_6, B_7 and B_8 received the U_a packet sent by node B_4, the beacon nodes B_2, B_3, B_5, B_6, B_7 and B_8 have been judged as the attacked nodes, according to the previous steps, there is no need to carry out other steps. When this process is finished, all the attacked beacon nodes are found.

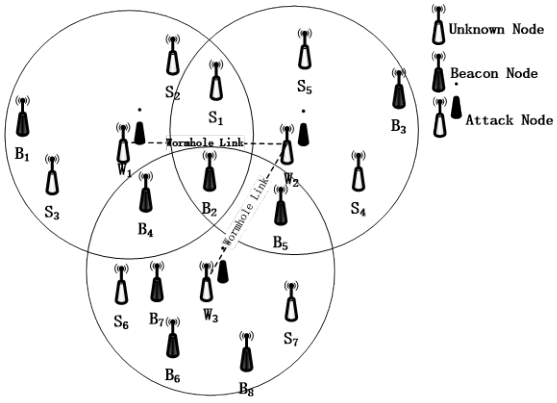
Step4. The attacked beacon nodes can obtain three sets of U_a, the conflict set U_a of beacon node B_1 and B_4 is $\{B_2, B_3, B_5, B_6, B_7, B_8\}$, the conflict set U_a of beacon node B_2, B_3 and B_5 is $\{B_1, B_4, B_6, B_7, B_8\}$, the conflict set U_a of beacon node B_6, B_7 and B_8 is $\{B_1, B_2, B_3, B_4, B_5\}$. Each attacked beacon node calculates the common set in every two conflict sets. The result is that the common set between the beacon nodes B_1, B_4 and the beacon

nodes B_2, B_3, B_5 is $\{B_6, B_7, B_8\}$, the common set between the beacon nodes B_1, B_4 and the beacon nodes B_6, B_7, B_8 is $\{B_2, B_3, B_5\}$, the common set between the beacon nodes B_2, B_3, B_5 and the beacon nodes B_6, B_7, B_8 is $\{B_1, B_4\}$. Then each of the attacked beacon nodes finds the smallest ID of beacon node in each common set. The result is that the smallest ID of beacon node in $\{B_6, B_7, B_8\}$, $\{B_2, B_3, B_5\}$, and $\{B_1, B_4\}$ are B_6, B_2, and B_1 respectively. According to the principle of progressive marking, the beacon nodes B_1, B_4 mark themselves with 1, the beacon nodes B_2, B_3, B_5 mark themselves with 2, the beacon nodes B_6, B_7, B_8 mark themselves with 3.

(2)The overlapping of two or three different wormhole areas



(a) case 1



(b) case 2

Fig. 2. The overlapping between different wormhole areas

In **Fig. 2(a)**, we consider that any two different wormhole areas overlap with each other and the third wormhole area does not overlap with other two wormhole areas. The distance between the attack node W_1 and the attack node W_2 should meet the condition of $0 < d_{W_1W_2} < 2R$, which leads to $B_2 \in (U_1 \cap U_2)$. In this case, according to the marking principle of beacon nodes, the node B_2 marks itself as same as node B_1 which is the smallest ID beacon node in all conflict sets received by B_2. This scheme can be applied to any two of the wormhole areas which are overlapping with each other. The scheme finds the smallest

ID beacon node from the U_a firstly. Then the marking of the beacon node which is in the overlapping area is same as the marking of the smallest ID beacon node.

In **Fig. 2(b)**, three different wormhole areas overlap with each other. The distances between attack nodes W_1, W_2 and W_3 should meet the following condition.

$$\begin{cases} 0 < d_{W_1W_2} < 2R \\ 0 < d_{W_1W_3} < 2R \\ 0 < d_{W_2W_3} < 2R \end{cases} \tag{7}$$

The attack nodes W_1, W_2 and W_3 are close to each other, which leads to $B_2 \in (U_1 \cap U_2 \cap U_3)$. In this case, the marking principle of beacon nodes is the same as the case in **Fig. 2 (a)**, that is, the beacon node B_2 mark itself the same as the smallest ID beacon node when the beacon node B_2 exists in three conflict sets U_a at the same time. In **Fig. 2(b)**, the beacon node B_2 marked with 1

3.3.2 Mark the Unknown Nodes

The unknown nodes take the marked beacon nodes as references to determine the wormhole areas that the unknown nodes belong. Then the unknown nodes are marked with $1,2,....,m$. The unknown nodes that are marked unsuccessfully mark themselves according to the marked unknown nodes. Those who still fail to be marked are semi-isolated. According to the **Fig. 1**, theorem 2 and theorem 3 can be obtained.

Theorem 2: The attacked unknown node which can communicate with all the attacked beacon nodes except the beacon nodes in U_i must be in the set U_i.

Proof: If $\exists S_j \in U_3$, according to the requirements of the theorem 2, there must be $\exists S_j \in (U_1 \cup U_2 \cup \ldots U_3)$ and $U_R(W_1) \in U_R(S_j)$, $U_R(W_2) \in U_R(S_j)$, $U_R(W_3) \notin U_R(S_j)$. When $S_j \in U_1$, according to the property of wormhole attack, there must be $U_R(W_2) \in U_R(S_j), U_R(W_3) \in U_R(S_j)$, it is contrary to the condition of $U_R(W_3) \notin U_R(S_j)$. When $S_j \in U_2$, there must be $U_R(W_1) \in U_R(S_j), U_R(W_3) \in U_R(S_j)$, it is contrary to the condition of $U_R(W_3) \notin U_R(S_j)$. When $S_j \in U_3$, there must be $U_R(W_1) \in U_R(S_j)$, $U_R(W_2) \in U_R(S_j)$, due to the limitation of communication radius, $U_R(W_3) \notin U_R(S_j)$ can be satisfied. Such as the unknown node S_2 which can communicate with all the beacon nodes B_2, B_3 B_5 in U_2 and all the beacon nodes B_6, B_7, B_8 in U_3, it fails to communicate with the beacon nodes in U_1, there must be $S_2 \notin U_2$, $S_2 \notin U_3$, $S_2 \in U_1$.

Theorem 3: If the unknown node cannot communicate with all the beacon nodes of at least $m-1$ wormhole areas, the unknown node is a normal node.

Proof: Consume that m=3, according to the property of wormhole attack, if $\exists S_j \in U_1$, there must be $U_R(W_2) \in U_R(S_j), U_R(W_3) \in U_R(S_j)$, it indicates that the unknown node S_j can communicate with all the beacon nodes of at least two wormhole areas. Similarly, if $\exists S_j \in U_2$,

there must be $U_R(W_1) \in U_R(S_j), U_R(W_3) \in U_R(S_j)$, it will get the same result as well as the condition of $\exists S_j \in U_3$.

Based on the theorems above, the attacked unknown nodes mark themselves by the principle of two-round marking. In the first-round marking, the marking process is as follows.

(1) If all the beacon nodes marked with 2 and 3 belong to set $U_R(S_j)$ and simultaneously satisfy $U_R(S_j)$ does not contain all the beacon nodes marked with 1, S_j is marked as 1.

(2) If all the beacon nodes marked with 1 and 3 belong to set $U_R(S_j)$ and simultaneously satisfy $U_R(S_j)$ does not contain all the beacon nodes marked with 2, S_j is marked as 2.

(3) If all the beacon nodes marked with 1 and 2 belong to set $U_R(S_j)$ and simultaneously satisfy $U_R(S_j)$ does not contain all the beacon nodes marked with 3, S_j is marked as 3.

(4) If all the beacon nodes marked with 1, 2 and 3 belong to set $U_R(S_j)$, S_j will end the first-round marking and wait for the second-round marking. In the second-round marking, the unknown node S_j will take the marked unknown nodes as references to mark itself. If the unknown node S_j still fails to mark itself, it is semi-isolated.

(5) In other cases, according to the theorem 3, the unknown node S_j is normal.

The unknown node will wait for the second-round marking after it fails to be marked in the first-round marking. Two cases will cause the unknown node fail to be marked.

(1) The uneven distribution of beacon nodes

In **Fig. 1**, because of the uneven distribution of beacon nodes, the unknown node S_7 meet the condition of $\{U_R(S_7) | (U_R(W_1) \cup U_R(W_2) \cup U_R(W_3)) \in U_R(S_7)\}$, the unknown node S_7 fails to be marked in the first round. The specific marking process of second-round marking is as follows.

Step1. In **Fig. 1**, according to the marking principle of beacon nodes, the beacon nodes B_1, B_4 are marked with 1, the beacon nodes B_2, B_3, B_5 are marked with 2, the beacon nodes B_6, B_7, B_8 are marked with 3. According to the marking principle of unknown nodes, in the first-round marking, the unknown nodes S_2, S_3 are marked with 1, the unknown nodes S_1, S_4 S_5 are marked with 2, the unknown nodes S_6, S_8 are marked with 3.The unknown node S_7 is waiting for the second-round marking.

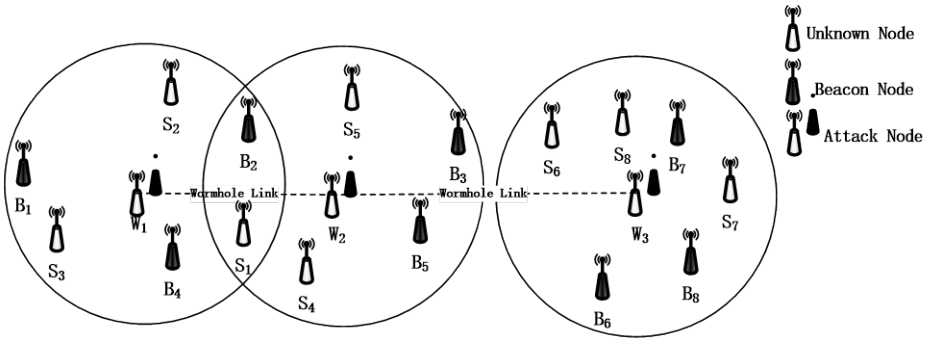
Step2. The unknown nodes that are marked successfully send their marking information to other nodes. When the unknown node received the marking information, it will determine whether it has received two or more conflict sets U_a (If the wormhole link is composed of m attack nodes, the attacked unknown nodes must receive at least $m-1$ conflict sets U_a). If the unknown node has received two or more conflict sets, it will forward the marking information to other nodes. This ensures that all the attacked unknown nodes in different wormhole areas can receive the marking information of other attacked unknown nodes, providing more references for the attacked unknown node that fails to be marked in the first-round marking. In **Fig. 1**, the unknown nodes S_2, S_3 are marked with 1 and send the marking information to other nodes. The unknown nodes S_1, S_4, S_5, S_6, S_7, S_8 receive and

forward the marking information to other nodes. Other attacked unknown nodes in different wormhole areas will take the same steps. This ensures that all the attacked unknown nodes can obtain marking information from other attacked unknown nodes that has been marked.

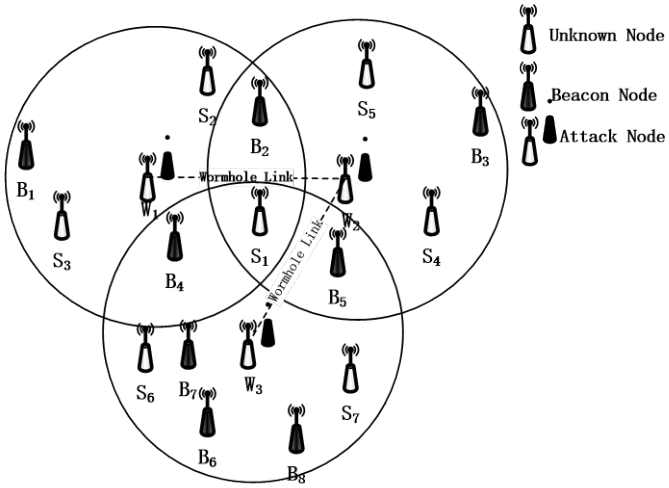
Step3. After Step2, the unknown node S_7 receives all the marking information from attacked unknown nodes. The unknown node S_7 saves the marking information and marks itself through its NL. For the unknown node S_7, the unknown nodes S_6, S_8 which have been marked before can be used as references. The NL of unknown node S_7 does not contain the unknown nodes S_6 and S_8, according to the theorem 2, the unknown node S_7 and the unknown nodes S_6 and S_8 are in the same wormhole area, the unknown node S_7 mark itself with 3.

(2) The overlapping of two or three different wormhole areas

In case 1 and case 2, the unknown nodes in overlapping areas can communicate with all the attacked nodes, which leads to that the unknown nodes in overlapping areas cannot be marked in the first-round marking and the second-round marking. In both cases, the unknown nodes are semi-isolated, that is, when the unknown nodes can communicate with all the attacked nodes in different wormhole areas, the unknown nodes disconnected from other nodes that are marked before. In **Fig. 3(a)**, the process is as follows.



(a) case 1



(b) case 2

Fig. 3. The overlapping between different wormhole areas

Step1. According to the marking principle, the beacon nodes B_1, B_2, B_4, and the unknown nodes S_2, S_3 are marked with 1, the beacon nodes B_3, B_5 ,and the unknown nodes S_4, S_5 are marked with 2, the beacon nodes B_6, B_7, B_8 ,and the unknown nodes S_6, S_7 ,and S_8 are marked with 3. The unknown node S_1 cannot be marked in the first-round marking, and then S_1 will wait for the second-round marking.

Step2. The unknown nodes S_2, S_3, S_4, S_5, S_6, S_7, S_8 send the marking information to other nodes. After receiving the marking information, the nodes forward the marking information again to ensure that the unknown node S_1 can receive all the marking information from the attacked unknown nodes. (The specific process can refer to Step2 of the marking process of unknown node S_7 in **Fig. 1.**

Step3. The unknown node S_1 receives all the marking information from the attacked unknown nodes. The unknown node S_1 searches the NL and finds that it can communicate with the unknown nodes S_2, S_3, S_4, S_5, S_6, S_7, S_8, which leads to that the unknown node S_1 cannot be marked in the second-round marking.

Step4. In the next round, the nodes marked with 1, 2, and 3 disconnect from each other. The unknown node S_1 is semi-isolated and disconnects from all the marked nodes. The unknown node S_1 will keep communication with other normal nodes within its communication radius. As long as there is one normal node within the communication radius of node S_1, it can use the beacon nodes beyond the wormhole areas to locate itself successfully. The unknown node S_1 can obtain other data packets of beacon nodes by the normal nodes and calculate its own coordinate. However, if there is no normal node within the communication radius of the unknown node S_1, the unknown node S_1 is considered as missing-judged which will be removed from the network.

In **Fig. 3 (b)**, the unknown node S_1 solves this problem in the same way as above. However, in the case 2, the unknown node S_1 is more likely to become missing-judged than that in the case 1.The reason is that the unknown node S_1 in case 2 is close to the centre of the wormhole areas. It is high probability that there is no normal node in the communication radius of node S_1.

3.4 Analysis of Error Source and Special Cases

Due to the characteristics of MWNL, there are many cases that will increase the localization error, such as the case of **Fig. 3(a)**. The following case also has a great influence on localization error.

Because the nodes are not evenly deployed, the unknown node S_1 meets the condition of $\left\{U_R(S_1) \mid U_R(W_3) \notin U_R(S_1), \left(U_R(W_1) \cup U_R(W_2)\right) \in U_R(S_1)\right\}$ in **Fig. 4**. In this case, the unknown node S_1 misjudges itself as an attacked node and determines that it is in the set U_3. When the node S_1 is corrected, it will disconnect from the nodes in the set U_1 and U_2. But the unknown node S_1 can communicate with other nodes which are normal. Although the localization error increases to some extent, it still obtains the enough localization information to locate itself.

For the special cases, in **Fig. 1,** due to the uneven distribution of nodes which are within the communication radius of the attack node W_3, the unknown node S_7 meets the condition of $\{U_R(S_7) | (U_R(W_1) \cup U_R(W_2) \cup U_R(W_3)) \in U_R(S_7)\}$. According to the marking principle, the unknown node S_7 cannot be marked in the first-round marking and second-round marking. S_7 is semi-isolated and tries to communicate with other normal nodes. But S_7 is close to the attack node W_3, there may be no normal node within the communication radius of node S_7. S_7 is considered as missing-judged and it will be removed from the network. The closer the unknown node S_7 is to the attack node W_3, the more likely it is to become missing-judged.

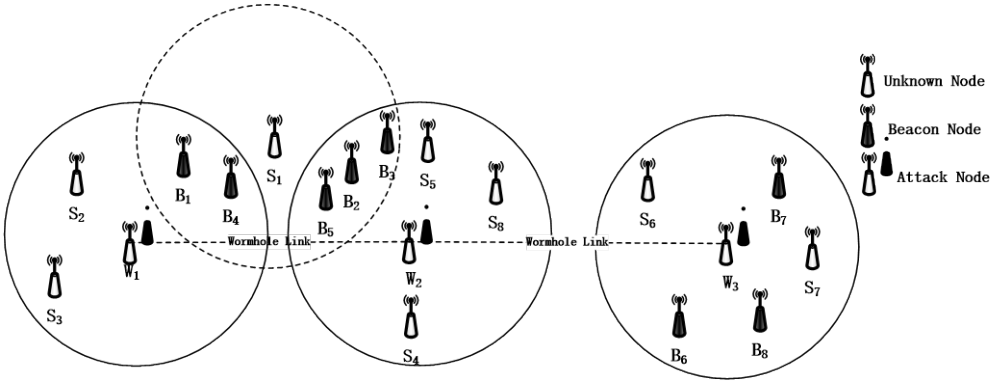


Fig. 4. The analysis of error source

4. Simulation Results and Analysis

In order to verify the effectiveness of the proposed AMLDV-Hop algorithm, we performed various simulation experiments. The simulation conditions are as follows:

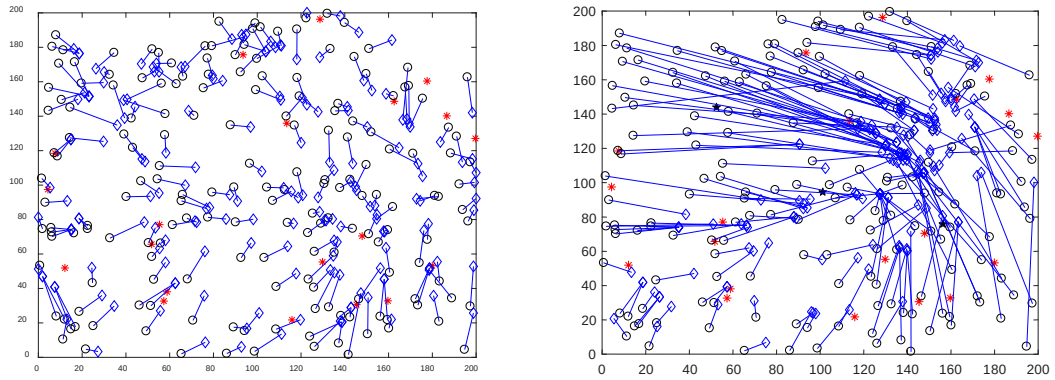
Number of nodes: 200, distribution area: $200 \times 200 m^2$, communicate radius: 30m, wormhole link composition: three attack nodes form one link, the suspect node determination coefficient G: 1.51.

Fig. 5 compares the localization error between the network with wormhole attack and the network without wormhole attack. The beacon nodes ratio is 0.1. The red symbol "*", the black symbol "★" and the blue symbol "○" represent the actual position of the beacon nodes, the attack nodes and the unknown nodes respectively. And we use blue symbol "◇" to represent the estimated position of unknown nodes. Actually, the localization error can be expressed by the lines between "○" and "◇". The longer the line between"○" and "◇", the larger the error is. **Fig. 5(a)** shows the localization error for the unknown nodes under the normal conditions, the localization error is 0.394. However, the localization error increases rapidly to 2.15 in **Fig. 5(b)** which shows the localization error for the unknown nodes with wormhole attack. It indicates that the wormhole attack has a significant negative impact on average localization error of the unknown nodes.

The average localization error E is defined as:

$$E = \frac{\sqrt{\left(x_i - x_i'\right)^2 + \left(y_i - y_i'\right)^2}}{R} \tag{10}$$

where, (x_i, y_i) is the actual coordinate value, (x_i', y_i') is the estimated coordinate value.



(a)Normal condition (b) Under attack

Fig. 5. The localization error comparison

Fig. 6 shows the influence of wormhole attack on the number of neighbor nodes. As can be seen from the figure, the attacked nodes usually have more neighbor nodes than the normal nodes. When there is one wormhole link that is composed of three attack nodes in the network, the number of neighbors of the attacked nodes is roughly three times as large as before.

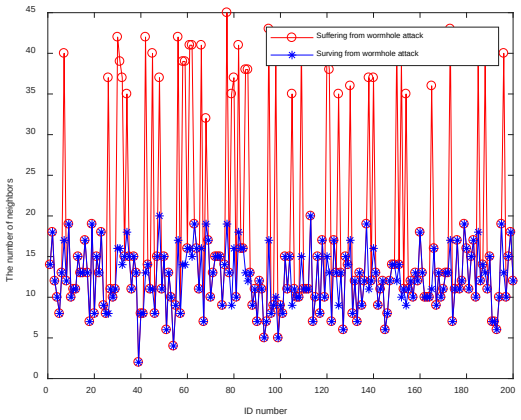
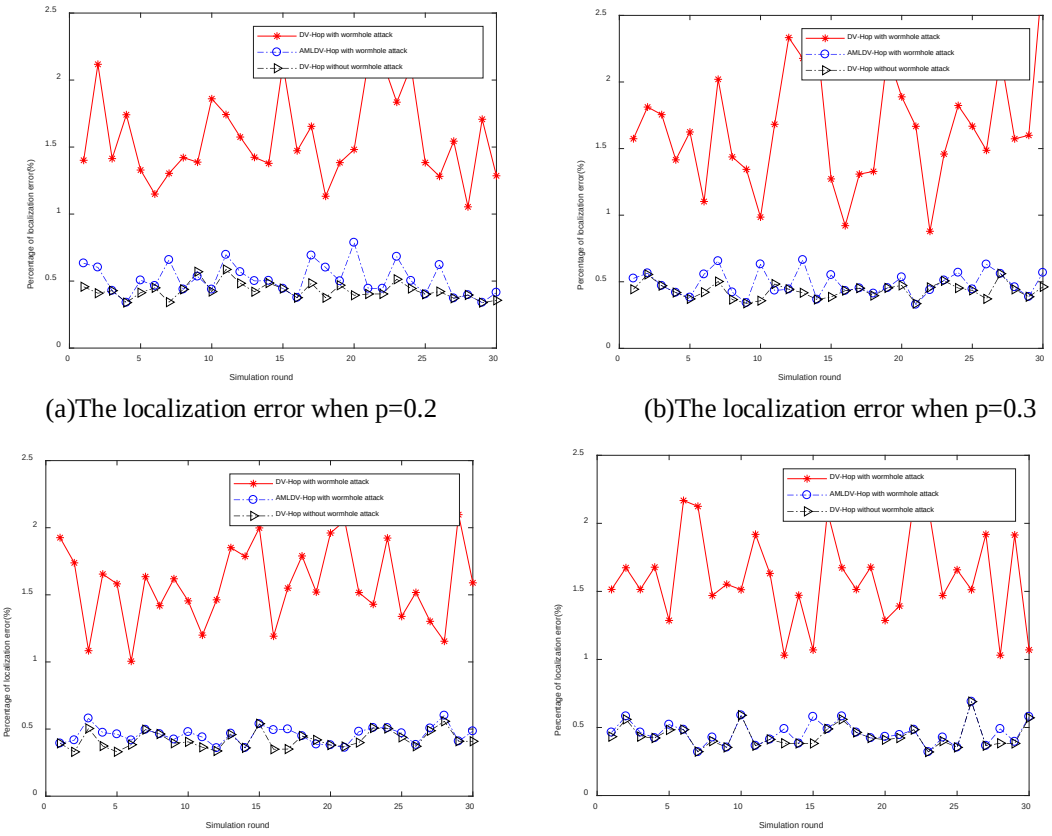


Fig. 6. The influence of wormhole attack on the number of neighbor nodes

In **Fig. 7**, we compare the localization error of DV-Hop without wormhole attack, DV-Hop with wormhole attack and AMLDV-Hop with wormhole attack. We also adjust the beacon nodes rates (represented by P) to observe the performance of AMLDV-Hop algorithm. When P is increased from 0.2 to 0.5, the localization error of AMLDV-Hop algorithm is about 105.4%, 116.9%, 112.2%, and 114.4% lower than DV-Hop with the wormhole attack. Compared with the DV-Hop without the wormhole attack, the localization error of AWLDV-Hop algorithm is only increased by about 8.29%, 5.50%, 3.84%and 2.23%. It indicates that the AWLDV-Hop algorithm can resist wormhole attack effectively and higher beacon node ratio means better performance. In practice, due to the misjudgments of the nodes, it will cause the localization error of the AMLDV-Hop a bit greater than the original DV-Hop error, but it still can meet the requirement of node localization.

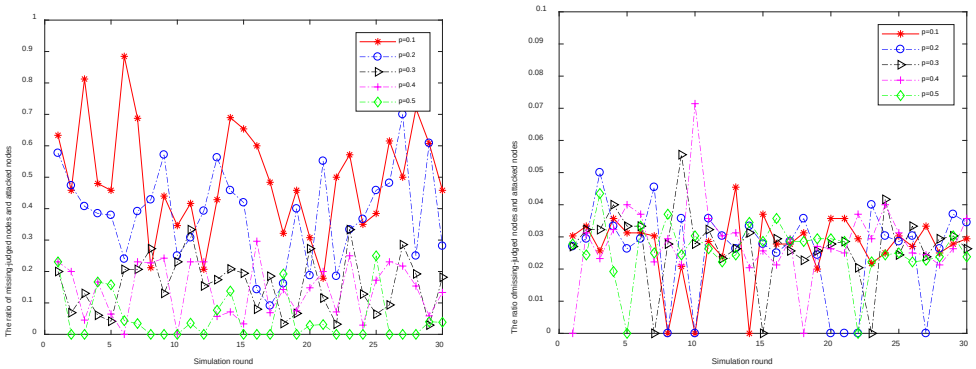


(a)The localization error when p=0.2 (b)The localization error when p=0.3

(c)The localization error when p=0.4 (d)The localization error when p=0.5

Fig. 7. The average localization error for different algorithms under different beacon node rates

Fig. 8 shows the associate between different P and the rate of missing-judged nodes. The low rate means better algorithm performance. It represents more unknown nodes can mark themselves successfully and to be corrected. **Fig. 8(a)** shows that there is more relation between the increase of P and the rate of missing-judged nodes in AWDV-Hop algorithm. With the increase of P, the rate of missing-judged nodes gradually decreases. When P increases from 0.1 to 0.5, the ratio of missing-judged nodes is decreased from 49.4% to 5.9%. So when there are fewer beacon nodes in the wormhole areas, the rate of missing-judged nodes will increase evidently. **Fig. 8(b)** shows that there is less relation between the increase of P and the rate of missing-judged nodes in AMLDV-Hop algorithm. The attacked unknown nodes take the marked beacon nodes as references in the first-round marking. If any attacked unknown nodes fail to be marked in the first-round marking, they will take the marked unknown nodes that are marked in the first-round marking as references in the second-round marking to mark them. So more attacked unknown nodes are marked. The number of missing-judged nodes has more relation with the distribution of nodes and has less relation with P. When P increases from 0.1 to 0.5, the average ratio of missing-judged nodes is about 2.669%, 2.569%, 2.706%, 2.836%, and 2.586% respectively.



(a)The results of AWDV-Hop algorithm (b)The results of AMLDV-Hop algorithm

Fig. 8. The influence of beacon node rate on the rate of missing-judged nodes

Fig. 9 shows the comparison on the localization error among different algorithms with different P. We do numbers of simulations under the condition of different P to exclude special cases. Compared with the DV-Hop with wormhole attack, LBDV-Hop, NDDV-Hop, and AWDV-Hop, the localization error of AMLDV-Hop algorithm is reduced by about 112.3%, 10.2%, 41.7%, and 6.9% respectively.

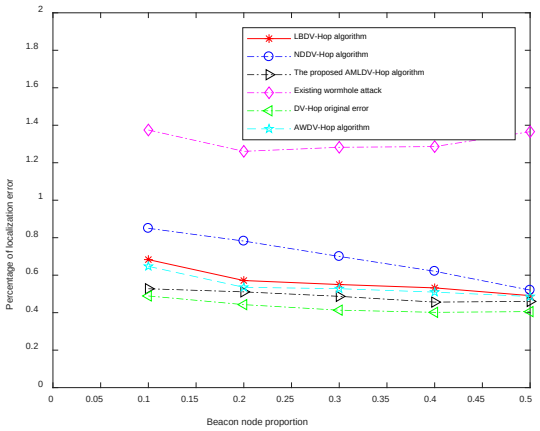


Fig. 9. The localization error among different algorithms with different beacon node rates

5. Conclusion

This paper proposes the AMLDV-Hop algorithm for the shortcomings of research status on wormhole attack. It applies to DWNL and MWNL a represent n represent d can effectively eliminate the negative impact of wormhole attack. Firstly, in the flooding phase, all the nodes create NL to obtain information about their neighbor nodes. Then the nodes make preliminary judgment based on the number of neighbors to determine whether they are attacked. The node that meets the conditions considers itself as a suspect beacon node. After calculating, the attacked beacon nodes are found and marked with $1,2,....,m$. The unknown nodes take the marked beacon nodes as references and mark themselves with $1,2,....,m$ in the first-round marking. If the unknown nodes fail to be marked in the first-round marking, they will take the marked unknown nodes as references to mark themselves in the second-round marking. The unknown nodes that still fail to be marked are semi-isolated. The nodes which have marked

with different numbers will no longer receive information from each other. Compared with LBDV-Hop algorithm, NDDV-Hop algorithm, DV-Hop with wormhole attack, and AWDV-Hop algorithm, the localization error of AMLDV-Hop algorithm is reduced by about 10.2%, 41.7%, 112.3% and 6.9% respectively. The proposed algorithm can detect multiple-wormhole attack in WSN. It uses the NL to reduce the computation complexity. It has high fault-tolerance ability. Once one beacon node is determined as the attacked beacon node, the algorithm can find the remaining attacked nodes by distance calculating. Besides, the proposed AMLDV-Hop algorithm also has better corrective effects without additional hardware. It should be noted that, although we only apply the scheme of MWNL detection to the DV-Hop algorithm, it can be applied to any network, in which NL can be obtained and have enough beacon nodes. The limitation of the proposed algorithm is that the nodes within the wormhole areas need to receive and transmit the U_a packets frequently. It will cause extra uneven energy consumption, which is harmful for the network lifetime.

Acknowledgements

This work was supported by National Natural Science Foundation of China (No.61501106), Science and Technology Foundation of Jilin Province (No.20180101039JC and No.JJKH20170102KJ), and Science and Technology Foundation of Jilin City (No.201831775).

References

[1] Jianpo Li, Xinxin Zhong and Chun Xu, "Review of dynamic node localization algorithm for wireless sensor networks," *Journal of Northeast Dianli University*, vol. 35, no. 1, pp. 52-58, January, 2015. Ariticle(CrossRef Link) .

[2] Kaur Ravneet and Malhotra Jyoteesh, "Comparitive analysis of DV-hop and APIT localization techniques in WSN," *International Journal of Future Generation Communication and Networking*, vol. 9, no. 8, pp. 327-344, March, 2016. Article (CrossRef Link) .

[3] Zhijun Teng, Miaomiao Xu and Li Zhang, "Nodes deployment in wireless sensor networks based on improved reliability virtual force algorithm," *Journal of Northeast Dianli University*, vol. 36, no. 2, pp. 86-89, February, 2016. Article (CrossRef Link) .

[4] Tsitsiroudi Niki, Sarigiannidis Panagiotis and Karapistoli Eirini, "EyeSim: A mobile application for visual-Assisted wormhole attack detection in IoT-enabled WSNs," in *Proc. of 9th Int. IFIP Wireless and Mobile Networking Conference*, pp. 103-109, July 11-13, 2016. Article (CrossRef Link) .

[5] Singh Parminder and Kaur Damandeep, "An approach to improve the performance of WSN during wormhole attack using promiscuous mode," *International Journal of Computer Applications*, vol. 73, no. 20, pp. 26-29. July, 2014.

[6] Khandare Pravin, Sharma Yogesh and Sakhare S.R, "Countermeasures for selective forwarding and wormhole attack in WSN," in *Proc. of Int. Inventive Systems and Control*, pp. 1-7, January 19-20, 2017. Article (CrossRef Link) .

[7] Bendjima Mostefa and Feham Mohammed, "Wormhole attack detection in wireless sensor networks," in *Proc. of SAI Computing Conference*, pp.1319-1326, July 13-15, 2016. Article (CrossRef Link) .

[8] Ranu Shukla, Rekha Jain and P.D Vyavahare, "Combating against Wormhole Attack in Trust and Energy Aware Secure Routing Protocol (TESRP) in Wireless Sensor Network," in *Proc. of Int. Recent Innovations in Signal Processing and Embedded Systems*, pp. 555-561, October 27-29, 2017. Article (CrossRef Link) .

[9] Zhijun Teng and Xiaoxu, Zhang, "The layout optimization of WSN based on inertia weight shuffled frog leaping algorithm," *Journal of Northeast Dianli University*, vol. 35, no. 6, pp. 66-69, June, 2015. Article (CrossRef Link) .
[10] Naidu Swarna Mahesh and Himaja Vemuri Bhavani, "Handling wormhole attacks in WSNs using location based approach," *in Proc. of 1st Int. Advances in Intelligent Systems and Computing*, pp. 43-51, December 01, 2016. Article (CrossRef Link) .
[11] Subha.s and Sankar U.Gowri, "Message authentication and wormhole detection mechanism in wireless sensor network," in *Proc. of 9th Int. Intelligent System and Control*, pp. 25-28, January 9-10, 2015. Article (CrossRef Link) .
[12] Sharma Mayank Kumar and Joshi Brijendra Kumar, "A mitigation technique for high transmission power based wormhole in wireless sensor networks," in *Proc. of Int. ICT in Business, Industry, Government*, pp. 722-723, November 18-19, 2016. Article (CrossRef Link) .
[13] Jayashree Padmanabhan and Venkatesh Manickavasagam, "Scalable and distributed detection analysis on wormhole links in wireless sensor networks for networked systems," *IEEE Access*, vol. 6, pp. 1753-1763, December, 2017. Article (CrossRef Link) .
[14] Arai Massayuki,"Reliability improvement of multi-path routing for wireless sensor networks and its application to wormhole attack avoidance," in *Proc. of 12th Int. Ubiquitous Intelligence and Computing*, pp.711-722, August 10-14, 2015. Article (CrossRef Link) .
[15] Ping Deng and Hongjiang Zhang, "A DV-Hop localization algorithm against wormhole attacks in WSN," *Journal of Southwest Jiaotong University*, vol. 50, no. 1, pp. 51-57, February, 2015.
[16] Honglong Chen and Zhibo Wang, "Secure localization scheme against wormhole attack for wireless sensor networks," *Journal on Communication*, vol. 36, no. 3, pp.723-732, March, 2015.
[17] Honglong Chen, Wei Lou and Zhi Wang, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, no. PA, pp. 22-35, January, 2015. Article (CrossRef Link) .
[18] Hongbin Wang, "The secure localization algorithm of SDV-Hop in wireless sensor networks," *Telecomunication, Computing, Electronics and Control*, vol. 14, no. 3, pp. 65-74, 2016. Article (CrossRef Link) .
[19] Neha Agrawal and Nitin Mishra, "RTT based Wormhole Detection using NS-3," in *Proc. of 6th Int. Computational Intelligence and Communication Networks*, pp.861-866, 14-16 Nov., 2014. Article (CrossRef Link) .
[20] Amish Parmar and Vaghela V.B, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol," in *Proc. of 7th Int. Communication,Computing and Virtualization*, pp. 700-707, 2016. Article (CrossRef Link) .
[21] Kumar Gulsham, Rai Mritunjay Kumar and Saha Rahul, "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, December, 2017. Article (CrossRef Link) .
[22] Bharat Bhushan and Dr. G. Sahoo, "Detection and defense mechanisms against wormhole attacks in wireless sensor networks" in *Proc. of Int. Advance in Computing and Automation (Fall)*, pp. 1-5, September 15-16, 2017. Article (CrossRef Link) .
[23] Ronghua Hu and Xiaomei Dong, "Senleash: A restricted defense mechanism against wormhole attacks in wireless sensor network," *Journal on Communications*, vol. 34, no. 10, pp. 65-75, November 12, 2013. Article (CrossRef Link) .
[24] Omar Cheikhrouhou, Ghulam M. Bhatti and Roobaea Alroobaea, "A hybrid DV-Hop algorithm using RSSI for localization in large-scale wireless sensor networks," *Journal of Sensors*, vol. 18, no. 1469, pp. 1-14, May, 2018. Article (CrossRef Link) .
[25] Bhagat Swati and Panse Trishna, "A detection and prevention of wormhole attack in homogeneous wireless sensor network," in *Proc. of Int. ICT in Business, Industry, and Government*, pp.1-6, 18-19 Nov., 2016. Article (CrossRef Link) .
[26] Xiang Yang, "DV-Hop secure positioning algorithm for wormhole attack resistance," *Computer Applications and Software*, vol. 30, no. 5, pp.188-192, May, 2013.

[27] Jianpo Li, Xinxin Zhong and Chun Xu, "Review of statical node localization algorithm for wireless sensor networks," *Journal of Northeast Dianli University*, vol. 35, no. 2, pp.73-82, February, 2015. Article (CrossRef Link) .
[28] Jianpo Li, Dong Wang and Yanjiao Wang, "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network," *IET Wireless Sensor Systems*, vol. 8, no. 2, pp.68-75, 2018. Article (CrossRef Link) .

Jianpo Li was born in China in 1980. He received his B.S., M.S., and Ph.D. from the Department of Communication Engineering, Jilin University, China, in 2002, 2005, and 2008, respectively. In 2008, he joined the School of Computer Science, Northeast Electric Power University, where he is currently a professor. His research interests are wireless sensor network and intelligent signal processing.

Dong Wang was born in China in 1992. He received his B.S. from the School of Information Engineering, Northeast Electric Power University. He is currently pursuing his M.S. in Northeast Electric Power University. His main research interest is wireless sensor network.