A Novel Secure DV-Hop Localization Algorithm against Wormhole Attacks

Dezhi Han[1] Mengxiao Liu[1] Tien-Hsiung Weng[2] Canren Tang[1] Mario D. Marino[3] Kuan-Ching Li[2]

[1] College of Information Engineering
Shanghai Maritime University, Shanghai, China
Email: 18438622701@163.com, dzhan@shmtu.edu.cn, 201830310053@stu.shmtu.edu.cn

[2] Dept. of Computer Science and Information Engineering (CSIE), Providence University, Taiwan
E-mail: {thweng, kuancli}@pu.edu.tw

[3] School of Built Environment, Engineering and Computing, Leeds Beckett University, UK
Email: m.d.marino@leedsbeckett.ac.uk

Abstract. IoT era and its ubiquitous sensing raises serious security challenges such as wormhole attacks. Given these attacks may affect the location determination of the employed sensors, security can be seriously compromised. The most common and serious attack is the single wormhole one, which is the focus of this paper. One of the most employed algorithms to approach the sensor location determination is the Distance Vector Hop (DV-Hop) algorithm, which can stillbe seriously affected from wormhole attacks. To overcome the challenges of this algorithm, this article proposes a novel secure DV-Hop localization algorithm against wormhole attack (ANDV-Hop), where beacon nodes delegate their attacked neighboring nodes to broadcast data messages, and the intersection of communication range of these neighboring nodes does include wormhole nodes. For implicit wormhole attacks, close nodes to the wormhole node are selected in order to broadcast data messages, whilst the nodes within attack range remove beacon nodes at the other end of the link from the neighboring list. For explicit wormhole attack, the algorithm employs a trust model that calculates the comprehensive trust value which is obtained via a selection reward/punish coefficient, where the selected ones within the intersection zone are considered as rewarded, whilst the ones to be removed, classified as punished Experimental results show that the proposed algorithm improves detection success rate, reduces relative localization error and energy loss, showing effectiveness and reliability.

Keywords. Wireless sensor networks, explicit wormhole attack, implicit wormhole attack, ANDV-Hop, trust model.

I. INTRODUCTION

With the advancement of the Internet of Things (IoT), the application of Wireless Sensor Networks (WSNs) increases at a fast pace [1], such as temperature and humidity measurement, sound detection, road condition monitoring [2], environment monitoring, emergency rescue, battlefield surveillance, industrial applications, and several others [3][4]. However, there are many security threats, such as industrial network intrusion [5]. In WSNs, localization makes possible the management of complex networks, creating transparency, and ensuring speedy production, being a key technology where the location information of nodes is accurately obtained. If the monitoring data of one node location is unable to be known, practical applications are meaningless and nonsense. Therefore, localization technology is one of the key factors in achieving the type of networked production and logistics needed for the application of WSNs [6], where resource consumption of sensor nodes must also be guaranteed [7]. Sensor nodes are distributed in harsh, untrusted, infrastructure-free environments, and they are vulnerable to all kinds of network attacks, such as selective forwarding attack, Sybil attack, sinkhole attack, clone attack [8], wormhole attack, and black hole attack [9], and these attacks have a significant impact on security localization. At present, there are many encryption methods [10] and intrusion detection methods to solve network attacks; for instance, combined with blockchain technology to ensure WSNs security [11] and perform data sharing [12][13], as well as K-means algorithm [14], deep belief network [15] and MK-ELM [16] to detect attacks.

Among the above attacks, the wormhole attack is one of the most harmful attacks, changing network topology structure and reducing node positioning accuracy [17][18]. At present, Distance Vector Hop (DV-Hop) algorithm is one of the leading technologies of node localization. There are two primary schemes for localization in WSNs: range-based and non-range-based methods. The former includes TOA (Time of Arrival), TDOA (Time Difference of Arrival), AOA (Angle of Arrival), RSSI (Received Signal Strength Indication), and other positioning methods [19]. In contrast, the latter includes centroid algorithm, DV-Hop algorithm, APIT (Approximate Point-in-triangulation Test) algorithm, and others. The DV-Hop localization algorithm is the most widely used [20], with low hardware requirements. . Presently, there are several improved DV-Hop localization algorithms [21], such as enhanced 3D DV-Hop localization algorithm [22][23], improved DV-Hop and DE algorithms [24]. Unfortunately, a wormhole attack can seriously affect the performance of DV-Hop localization algorithms. A wormhole attack is an internal attack that consists of wormhole nodes and wormhole links. Wormhole attacks can be launched in different ways, called explicit and implicit wormhole attacks [25]. Both attack modes affect the DV-Hop localization algorithm, so other solutions should be adopted for different attack modes.

Nowadays, many wormhole attack solutions are only applicable to a single attack pattern, and some measures cannot solve attacks if this pattern is different from the attack pattern under assumed predicted conditions. For such, we propose ANDV-Hop in this article, and the main contributions are as follows:

(1) A newly-designed secure DV-Hop localization algorithm (ANDV-Hop) is proposed to resist wormhole attacks. Attacked beacon nodes entrust their attacked

neighboring nodes to broadcast data messages, and the intersection of communication areas of these neighboring nodes reduces the range of wormhole nodes.

(2) ANDV-Hop is a novel algorithm proposed and implemented for defending against implicit and explicit wormhole attacks. The former makes nodes close to wormhole nodes in intersection-range broadcasting data messages, deleting beacon nodes at another end of wormhole link from the neighbor list, so these nodes within the communication range of two wormhole nodes are disconnected. In the latter, an explicit wormhole attack is eliminated by establishing a trust model and calculating the nodes' comprehensive trust value in the intersection range. This article focuses on improving the efficiency of a single wormhole attack and investigating the coexistence of multiple attacks, as further discussed.

(3) This algorithm method reduces the energy consumption of other nodes and facilitates subsequent processing of the wormhole attack on localization.

The remainder of this article is organized as follows: Section II introduces related work, Section III is problem description, and Section IV presents the proposed ANDV-Hop security localization method. Section V presents results and analysis of the simulation and experimental testing, and finally, concluding remarks and future directions in section VI.

II. RELATED WORK

A number of researches on localization algorithms against wormhole attacks in WSNs have been proposed, and shown in Table 1 literature overview of the wormhole attach research solutions on DV-Hop localization algorithm, where solutions, advantages and disadvantages are included.

In [26], Li *et al.* proposed a secure DV-Hop localization algorithm against wormhole attack (AWDV-Hop) that compares neighboring nodes' real and theoretical numbers to discover suspicious beacon nodes, since attacked beacon nodes and unknown nodes are labeled. In this way, this method reduced localization error, though it removed the nodes in overlapping regions, causing waste of resources. To overcome such an issue, label-based localization algorithm (LBDV-Hop) was proposed [27], where marked nodes remove the nodes differently from their label in neighboring list, eliminating the effect of wormhole attacks. Unlike the labeling method [26], LBDV-Hop has incorporated more details such as uneven node distribution; however, these techniques result in significant errors when detecting nodes and reducing node connectivity. Compared to LBDV-Hop [27] and to AWDV-Hop [26], the proposed ANDV-Hop can reduce the range of wormhole nodes and does not need to remove them so that the connectivity of nodes will not change.

A real-time intrusion detection system for RPL routing protocol wormhole attack was proposed in [28], whereas the received signal strength indicator identifies attacking nodes that can detect wormhole attacks in lower-density sensor networks. However, it is unsuitable for high-density sensor networks, leading to low efficiency. Alternatively, given its narrower range of wormhole nodes, ANDV-Hop can approach much denser networks. Furthermore, Luo *et al.* detected wormhole attacks through a simple and localized trusted neighboring discovery protocol [29], where each node is considered a suspicious node according to the neighboring ratio value and the size of the neighboring ratio threshold. However, the method relied heavily on the threshold of the neighboring ratio, so detection success may decrease when the node changes dynamically. Since nodes change dynamically, ANDV-Hop is lesser affected by the detection rates.

Tamilarasi *et al.* proposed a safe path selection method based on Ad-hoc on-demand multipath distance vector (AOMDV) routing protocol [30], focusing on identifying wormhole links using detection and feedback packets from the source node to verify the target node. In addition, the source node selected optimal path from non-attack path through particle swarm optimization algorithm, which improved the security. If there are more wormhole links, the nodes will consume energy significantly, while malicious attack nodes are hidden inside the network, their location and wormhole links cannot be determined by normal nodes. Conversely, a wormhole node is included in ANDV-Hop, so the range of wormhole nodes is reduced. In [31], Ping *et al.* proposed a safe neighboring discovery algorithm to identify false neighbors by hop count difference and remove false neighbors from the node neighboring list, reducing the impact of wormhole attacks. That is, if the network extension structure is sparse, it cannot eliminate false neighbors, and thus, to eliminate false neighbors, nodes are placed close to wormhole nodes in the intersection-range broadcast data messages in ANDV-Hop. Beacon nodes are deleted from the neighbor list in the wormhole link, thus allowing nodes within the communication range of two wormhole nodes to be disconnected.

TABLE 1. EXISTING SOLUTIONS

PAPER	SOLUTION	ADVANTAGE	DISADVANTAGE
[3]	This method inserted an active game to prevent infection into the basic DV-Hop scheme.	It could detect and prevent wormhole attacks without requiring additional hardware.	It had less to say about how to deal with wormhole nodes.
[26]	This method disconnected beacon nodes with different markers that were subject to wormhole attacks.	It effectively reduced positioning errors.	It removed some nodes from the network, resulting in wasting resources.
[27]	The method removed nodes attacked by wormholes from the network by creating conflict sets.	It verified the correctness of theories and reduced the impact of wormhole attacks on DV-Hop.	Hibernating nodes consume a lot of energy and waste resources.
[28]	The paper identified wormhole attack nodes by using received signal strength indicators.	It could detect wormhole attacks to some extent.	It requires additional hardware, and the detection rate decreases when the network scale is large.
[29]	The paper detected different wormholes through a trusted neighbor discovery protocol.	It was able to detect different types of wormholes.	It was highly dependent on the neighbor ratio threshold.
[30]	It detected the wormhole attack path and used a particle swarm optimization algorithm to select the optimal path.	It effectively improved network energy and efficiency.	If the wormhole node's ID is unknown, the wormhole link cannot be identified.
[31]	It was detected according to the difference of path hops between nodes, and the false links were filtered by the	It reduced the impact of wormhole attacks and improved the location of nodes.	Hidden wormhole nodes and wormhole links cannot be found.

search and discovery algorithm.

This article proposes different security localization methods according to different wormhole attack modes. For explicit wormhole attack, malicious nodes will be removed from the network after determining the wormhole node's ID according to the trust model, while suspicious node pairs are removed if detected under wormhole attack from each other's neighboring list in implicit wormhole attack. The proposed method can resist wormhole attacks in different ways, improving detection efficiency and reducing localization errors, as depicted in Section IV.

Next, we focus on detailing the modeling of wormhole attacks with the DV-Hop localization algorithm.

III. PROBLEM DESCRIPTION

Splitting the problem into three parts, and described as follows: (A) evaluating the impact of the wormhole attack on DV-Hop, (B) how this algorithm is deployed, and (C) how it is detected.

A. Impact of Wormhole Attack on DV-Hop Localization Algorithm

(1) DV-Hop Positioning Process

The DV-Hop localization algorithm is distributed localization method through distance vector routing and GPS (Global Positioning System) localization. The main advantages are simplicity and high localization accuracy, and the basic idea is as follows [32][33]:

Step 1. Each beacon node initiates flooding, including location information and hops count, unknown nodes calculate the number of hops to each beacon node and save the minimum number of hops.

Step 2. Similarly, each beacon node counts the number of hops and location coordinates to other beacon nodes. Average distance per hop is estimated according to Equation (1), and beacon nodes broadcast average hop distance group to the network, unknown nodes calculate the distance to beacon nodes according to average hop distance and hop count, assuming the unknown node is S_k, and its distance to S_k is calculated by Equation (2).

Where d_i denotes hop distance, d_{kj} is the distance from S_k to B_j, (x_i, y_i) and (x_j, y_j) are the coordinates of the beacon nodes B_i, B_j respectively, C_{ij} is the minimum hop number between B_i and B_j, and C_{kj} is the hop number between S_k and B_j.

$$d_i = \frac{\sum_{i \neq j} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum_{i \neq j} C_{ij}} \qquad (1)$$

$$d_{kj} = C_{kj} \times d_i \qquad (2)$$

Step 3. Unknown nodes obtain the distances of three and more beacon nodes, and then coordinate positions can be estimated based on a trilateral measure or the maximum likelihood estimation method via least squares. Next, turn our attention to wormhole attack mode modeling.

(2) Wormhole attack mode

Wormhole nodes attract much traffic, causing the surrounding nodes to consume more energy, and thus reducing the network survival cycle. Furthermore, the establishment of wormhole links disrupts the routing mechanism of distance information between nodes and leads to the failure of route discovery protocols. As previously stated, wormhole attacks were classified into explicit and implicit wormhole attacks according to whether the ID of the wormhole node was visible [25]. Fig.1 mainly shows that the node path is divided into normal path and abnormal path through wormhole link, different wormhole attack patterns are illustrated in Fig.1 and explained as follows:

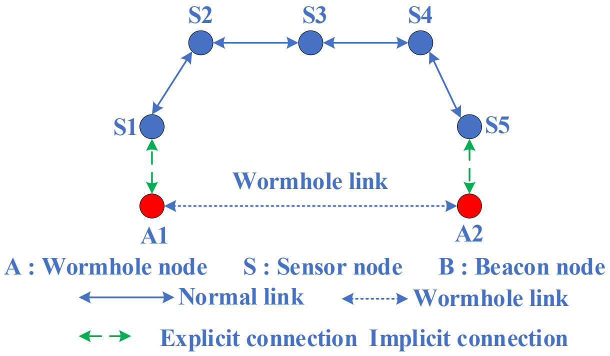


Fig.1. Distinguish wormhole attack patterns.

1) *Explicit Wormhole Attack*: Attack node disguises itself as a normal node, and its ID is visible to the network, but the wormhole link is invisible. When the wormhole node sends data packet, it will add its identity information to data packet to prove its identity. According to Fig.1, the normal path from node S1 to S5 is S1→S2→S3→S4→S5, and abnormal path is S1→A1→A2→S5. There are 4 hops from S1 to S4 under the normal path while 3 hops under the wormhole link. Based on the shortest path first algorithm, S1 has the shortest hop count under wormhole link. Therefore, S1 will choose the wormhole link as the route, reducing the hop count between S1 and S5.

2) *Implicit Wormhole Attack*: Wormhole node hides in the network, it cannot establish contact with any other nodes, and its ID is invisible to other nodes. In this attack mode, neither the equipment used by the wormhole node nor the wormhole link is a part of the network. Furthermore, routing protocols do nothing to limit this type of attack. The path through the wormhole link is S1→S5 in Fig.1. S1 mistakenly believes that S5 is neighboring node, so S1 and S5 establish neighboring relationship. The false neighboring relationship causes wrong routing information, and normal nodes send packets through the wrong route [29].

From the previously mentioned analysis, both attack modes would change the hop information and lead to positioning errors. Now, analyzing the impact of wormhole attacks on the positioning algorithm process depicted in Fig.2. Connections of different colors between nodes in Fig.2 represent different paths from node S to B. There are three paths from unknown node S to beacon node B, respectively (1)S→A1→A2→B, (2)S→A2→A1→B, and (3)S→B. Comparing the size of three path hops, if the hop count in (3) is the smallest, wormhole node will not interfere with hop count from S to

B. However, if the number of hops in (1) or (2) is the smallest, the hop count calculated through wormhole link will be used, affecting the first step of the DV-Hop localization algorithm.

Similarly, the number of hops from one beacon node to other beacon nodes will also be affected, affecting the DV-Hop localization algorithm's second step and leading to significant error while calculating the average hop distance. Therefore, a wormhole attack impacts the DV-Hop localization process, so a wormhole attack must be solved if the localization accuracy improves.

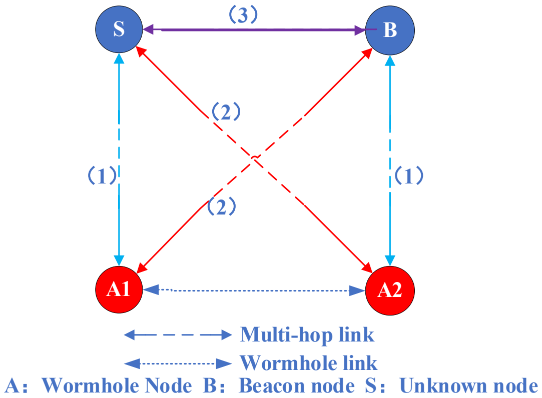


Fig.2. Influence of wormhole attack on DV-Hop localization.

B. Network Deployment

It is assumed that there are three types of nodes in WSNs, namely sensor node (S), wormhole node (A), and beacon node (B), which are randomly distributed in the network. Among them, the beacon node knows location information and initiates flood to surrounding nodes, and the position information of the sensor node is unknown. All nodes conform to the Poisson distribution and assuming that the communication radius (R) of nodes is the same, there is no attack of data packet loss and multiple attack modes coexisting, and the Poisson distribution satisfied by nodes is shown in Equation (3).

$$P(N(S)=k)=\frac{(\rho s)^k}{k!}e^{-\rho s}(k=0,1,2,\dots) \qquad (3)$$

Where P is the probability of occurrence, N(S) denotes the number of sensor nodes whose node communication area is S, ρ signifies sensor node density.

C. Wormhole Attack Detection

Beacon nodes are used to detect wormhole attack, and wormhole attack is detected according to the following three characteristics in WSNs[34]:

(1)Restricted single-hop communication range: the nodes cannot directly communicate with nodes outside the single-hop communication range,

(2)No repetitional characteristics of data packets: the nodes can only receive data packets sent from neighboring nodes once in the communication process and cannot repeatedly receive data messages from the same node.

(3)Packet self-exclusion: the nodes cannot receive data messages sent by themselves.

Wormhole attack is detected according to specific actions. Fig.3 shows that beacon nodes and unknown nodes can detect attacked nodes according to the above three rules at different positions within the wormhole node range. There is at least one beacon node in the communication range R of two wormhole nodes, and wormhole attacks can be detected, according to (1). In Fig.3,$B1 \in D_R(A_1)$, $B2 \in D_R(A_2)$, B1 and B2 are not within each other's communication range. Whenever there is a wormhole attack, data packet is sent by B1 and received by B2 through the wormhole link, B1 and B2 are nodes with known positions. The distance calculated is over R, which violates (1). $S1 \in D_R(A_1)$, $S2 \in D_R(A_2)$, S1 and S2 are in the communication range of each other, data packet is sent by S1 and received directly by S2. It is also received by A1 and forwarded to A2, and A2 broadcasts the data to neighboring nodes. Eventually, S2 receives data messages from S1 twice, and then the (2) is violated. For the (3), $S3 \in A1$ and $S3 \in A2$, A1 forwards packets sent by S3 to A2, A2 broadcasts data information to neighboring nodes, S3 will receive packets sent by itself, violating this property.

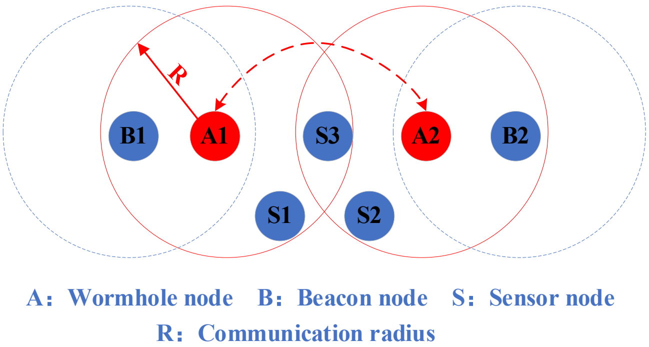


Fig.3. Detecting Wormhole Attack in WSN.

Based on the above analysis, there is one beacon node in the range of two attacking nodes, wormhole attack can be detected to calculate the theoretical detection success rates[27]. Assuming that A represents no beacon node in the range A1, B represents no beacon node in the range A2, and events A and B are independent of each other. Beacon nodes also belong to the Poisson distribution, where ρ_B represents the density of beacon nodes, P_{r_s} is the success rate of detection, and P_{r_f} is the failure rate of detection, with $P_{r_s} + P_{r_f} = 1$. When there is no beacon node within the attack node, $P(A) = P(B) = e^{-\rho_B s}$, and P_{r_f} is calculated by Equation (4).

According to Equation (4), wormhole attacks' theoretical detection success rate can be obtained as per Equation (5).

$$\begin{gathered} P_{r_f} = P(A \cup B) = P(A) + P(B) - P(AB) \\ P(A) + P(B) - P(A)P(B) \qquad (4) \\ 2e^{-\rho_B s} - (e^{-\rho_B s})^2 \end{gathered}$$

$$P_{r_s} = 1 - P_{r_f} = 1 - 2e^{-\rho_B s} + e^{-2\rho_B s} \qquad (5)$$

Next, we discuss the proposed algorithm ANDV-Hop.

IV. SECURE ANDV-HOP LOCALIZATION ALGORITHM

Different safe and effective localization methods for different wormhole attack patterns are proposed. Based on the previously described three parts of the problem's specification, it determines which beacon nodes suffer wormhole attacks and then eliminates the impact of wormhole nodes on the DV-Hop localization algorithm according to different attack methods.

A. Implicit Wormhole Attack Security Localization Algorithm

If there is an implicit wormhole attack, the wormhole node cannot be deleted from the network since its ID cannot be determined. For this reason, this paper mainly shrinks the location of the wormhole node, selects some nodes close to the wormhole node to send data messages, and finally deletes the attacked nodes from the mutual routing table at both ends of the wormhole link. Therefore, the first step of the DV-Hop algorithm can be executed correctly. The IDs of A1 and A2 in Fig.4 are unknown, indicating a way of implicit wormhole attack, the basic process is described and discussed next.

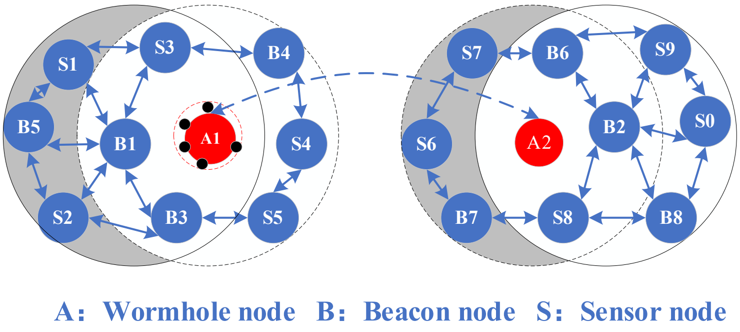


Fig.4. Secure localization of implicit wormhole attack.

As depicted in Fig.4, B1 and B2 are the ones that will suffer wormhole attacks according to the above three characteristics and mistakenly consider each other to be a neighboring node. After the detection is completed, B1 entrusts its neighboring nodes to broadcast data messages and determines which neighboring nodes are in the scope of attack node A1, that is, if B2 receives data messages from S3, S3 is in the range of A1, and if B2 cannot receive data messages broadcast by S1, then S1 is not in the range of A1. If the wormhole link is short, three characteristics must also be used to determine whether the neighboring nodes are within the A1 range.

The intersection of neighboring nodes delegated in the attack node range must contain A1, as shown in the red area of Fig.4, the more attacked nodes the delegated suffers, the smaller the intersection area will be, narrowing the range where wormhole nodes are. Since all nodes have the same communication radius, the nodes' communication range almost coincides with the attacking node in the intersection region. The node close to the attacking node (the node with the highest repetition rate of the same neighbors) is selected to broadcast data messages in the red region. The process mainly deletes B2 from the neighbor list, so most of the nodes in the communication range of A1 will remove B2 from their routing table. Other beacon nodes also perform similarly so that the nodes under attack at both ends of the wormhole link will remove beacon nodes that are not in an attack range from the neighbor list, thus eliminating the influence of wormhole nodes on the localization algorithm. The specific algorithm is described as algorithm 1, and input beacon nodes are represented by B1, B2, the total number of nodes by n and the neighbor node set of B1(such as S3, B3), outputs the nodes attacked by wormhole node A1, and delete B2 from the neighbor list. And its complexity is $O(n)$. The complexity will increase when the nodes are dense, though the accuracy improved.

Algorithm 1: Implicit Wormhole Attack Security Localization Scheme

```
Input: Beacon nodes $B_1$,$B_2$; n: the neighbor set of node $B_1$
Output: Remove $B_2$ from the list of nodes within the attack range of $A_1$
Let $B_1$ delegates its neighbor nodes n to send a message
for each node $n_i$ in n do
    if $B_2$ receives messages or against three characteristics then
        $n_i$ in the wormhole range
          put $n_i$ in S
    end if
end for
if $n_i \cap n_j \cap \ldots \cap n_s \neq \emptyset$ then
    Intersection $setA_1 = n_i \cap n_j \cap \ldots \cap n_s$
end if
In $setA_1$, select the node id with a high repetition rate in the neighbor list to form
    the set ID
for each $id_i$ in ID do
    $id_i$ removes $B_2$ from the list and broadcasts it to the neighbor node
end for
```

B. Explicit Wormhole Attack Security Localization Algorithm

If there is an explicit wormhole attack, the solution is different from an implicit wormhole attack. Because the ID of the attack node is visible in WSNs, it establishes contact with nodes in the communication range, and the nodes under attack save the ID of the attack node. Therefore, this article proposes a trust mechanism model to remove wormhole nodes from the network, Fig.5 is a way of explicit wormhole attack, the following part of Fig.5 is to implement the trust model for narrowing the range of nodes details follow next.

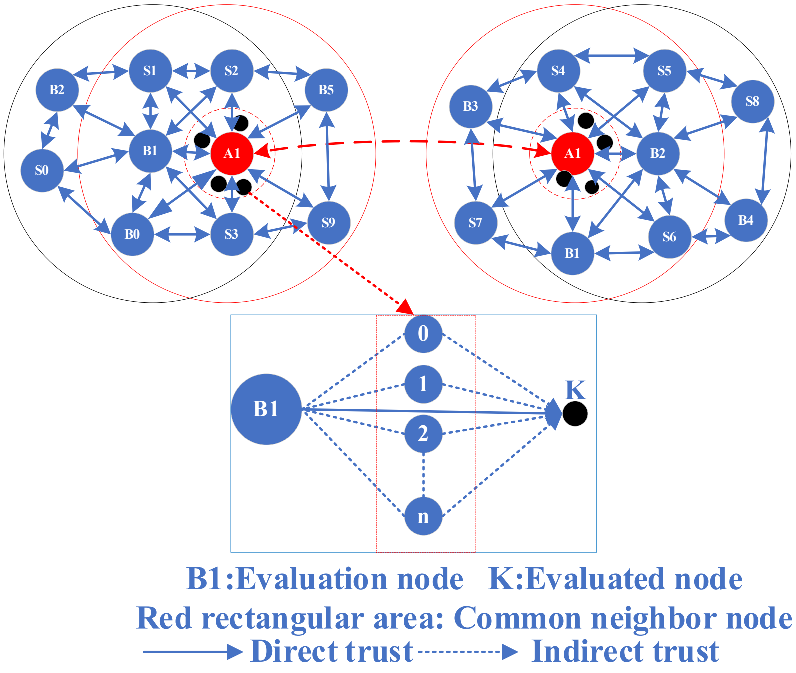

B2
S1
S2
B5
S0
B1
A1
B0
S3
S9
B3
S4
S5
S8
A1
B2
S7
B1
S6
B4
0
1
2
n
B1
K
B1:Evaluation node K:Evaluated node
Red rectangular area: Common neighbor node
Direct trust
Indirect trust

Fig.5. Secure localization of explicit wormhole attack.

As the implicit wormhole attack, let beacon nodes under wormhole attack delegate their neighboring nodes to send packets, the intersection of neighboring nodes under attack must include wormhole node, because the ID of wormhole node is known. According to the trust model, beacon node calculates direct, indirect, and comprehensive trust values for the nodes in the intersection range: the more neighbor nodes, the more accurate the calculated trust value.

As depicted in Fig. 5, and taking beacon node B1 as an example, the red dotted circle is the intersection containing A1. Next, B1 calculates the direct trust value for the node K in the range, and its neighbor nodes calculate direct trust value then send feedback to B1, so it calculates indirect trust value based on these values, and finally, B1 calculates trust value according to direct and indirect trust values. A1 only forwards data messages, but it does not reply to confirmation messages. In addition, the trust mechanism model sets reward and punishment coefficients, so the trust value of A1 must decrease continuously. Other beacon nodes attacked by wormholes also perform similarly.

TABLE II. DIFFERENTIATION OF TRUST DEGREE

TRUST VALUE	TRUST DEGREE
[-1,0.5)	Complete distrust
[0.5,0.6)	Distrust
[0.6,0.8)	Trust
[0.8,1)	More trust
1	Full trust

Each beacon node broadcasts the ID with the smallest trust value, the IDs of nodes with the lowest trust value are removed from the WSNs in the end. Algorithm 2 is a description of the entire process, input beacon nodes are represented by B1, B2, the total number of nodes by n and the neighbor node set of B1(such as S1, S2, S3, B0), output is to delete wormhole nodes A1 and A2 from the network. If the intersection of neighbor nodes contains k nodes, its complexity is $O(nk)$. Similarly, when the nodes are dense, complexity will be increase, but accuracy will be improved. The trust threshold is set as 0.6, and the initial trust value is 0.5. The calculation process of trust value is based on the trust mechanism model [35], and the degree of trust will be distinguished according to trust value. When the trust value exceeds a threshold, the greater the trust value is, the higher the trust degree will be, as depicted in Table II.

Algorithm 2: Explicit Wormhole Attack Security Localization Scheme

```
Input: Beacon nodes $B_1$,$B_2$; n : the neighbor set of node $B_1$
Output: Remove two malicious nodes from WSN
Let $B_1$ delegates its neighbor nodes n to send a message
for each node $n_i$ in n do
    if $B_2$ receives messages or against three characteristics then
        $n_i$ in the wormhole range
         put $n_i$ in S
    end if
end for
if $n_i \cap n_j \cap \ldots \cap n_s \neq \emptyset$ then
    Intersection $setA_1 = n_i \cap n_j \cap \ldots \cap n_s$
end if
for each node $k_i$ in $setA_1$ do
    $B_1$ calculates $DT_{B1ki}$ and $w_{B1ki}^{DT}$($DT_{B1ki}$: Direct trust value;$w_{B1ki}^{DT}$: Direct trust weight) for $k_i$
    for each node $O_i$ in S do
        $O_i$ calculates $DT_{Oiki}$ and $w_{Oiki}^{DT}$ for $k_i$
        Sending $DT_{Oiki}$ and $w_{Oiki}^{DT}$ to $B_1$
    end for
end for
$B_1$ calculates $IT_{B1ki}$ and $w_{B1ki}^{IT}$ according to $DT_{Oiki}$ and $w_{Oiki}^{DT}$($IT_{B1ki}$: Indirect trust value;$w_{B1ki}^{IT}$: Indirect trust weight)
for each node $k_i$ in $setA_1$ do
    $B_1$ calculates $\pi_{B1ki}$ for $k_i$
    Initialize min=0.5
    if $\pi_{B1ki} < 0.5$ then
        min=$\pi_{B1ki}$
    end if
end for
if Get two IDs with the lowest trust value in min then
    Remove two nodes from the network
end if
```

(1) Trust mechanism model

The trust mechanism model is upgraded and adapted strictly following the trust model proposed in [35], the reward and punishment coefficients are used to update trust value. In addition, the number N of interactions between nodes in the time interval T is no higher than 50, because when N comes to 50, the adequacy is close to 100%. The number of successful interactions is represented by S, and the number of failed interactions represented by F, and S+F=N. The trust model includes the calculation of direct trust value, indirect trust value, and comprehensive trust value. The calculation process is described in combination with Fig.5.

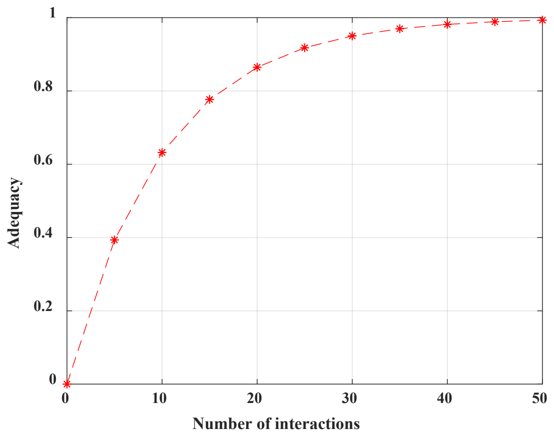


Fig.6. The functional relation between N and f.

1) *Direct trust value*: The calculation of direct trust value includes direct trust value and its weight. First of all, the paper has to consider the number of interactions between nodes in T. N has a direct impact on the update of trust value, if N is different, the number of S and F is different, updated trust value is also different. Furthermore, the number of interactions also affects the weight of direct trust value. Assuming that the number of interactions between node B1 and K is N (0N≤50) in T, direct trust value is calculated by Equation (6), where DT_{B1K} denotes the direct trust value of beacon node B1 to K, DT'_{B1K} denotes the direct trust value before update, α is reward coefficient, if all 50 interactions are successful, trust value will reach 1, so set to 0.01, and β is penalty coefficient, if all 50 interactions are failed, trust value will reach -1, and punishment degree must be higher than reward degree, so β set to -0.03. With increased interaction times, its complexity will increase, but the more reliable the trust value will be. Therefore, the higher the trust value of a node, the higher its credibility.

$$DT_{B1K} = S * \alpha + F * \beta + DT'_{B1K} \qquad (6)$$

The weight of direct trust value can measure the reliability of direct trust value, which is related to the adequacy of interactions between nodes. Adequacy is similar to the number of interactions, and the number of interactions in time T is also an essential factor in weight calculation. Equation (7) is the relationship between interaction times and adequacy, f is adequacy, and the value of μ is 10[35]. By normalization, the adequacy value can be kept within [0,1], while the exponential function is shown in Fig.6. With the increase of interaction times, the increased speed of adequacy changes from fast to slow.

$$f = 1 - e^{\frac{-N}{\mu}} \qquad (7)$$

The weight of direct trust value can be calculated, as shown in Equation (8), denoting the direct trust weight of beacon node B1 to K by ω_{B1K}^{DT}.

$$\omega_{B1K}^{DT} = \frac{1}{2} * (f + 1) \qquad (8)$$

2) *Indirect trust value*: Common neighboring nodes of B1 and K calculate direct trust value for the target node K and feed these trust values to B1, B1 calculates indirect trust value and indirect trust weight based on these feedback for the node K. Indirect trust value is denoted by IT_{B1K}. When a node has more neighbors, the degree of indirect trust will continue to improve.

Assuming that common neighbouring nodes of B1 and K are in red rectangle region, as depicted in Fig.5. These direct trust values of common neighbouring nodes to K are denoted as $\{DT_{1K}, DT_{2K}, DT_{3K}, \cdots, DT_{nK}\}$, and their direct trust weights are written to be $\{\omega_{1K}^{DT}, \omega_{2K}^{DT}, \omega_{3K}^{DT}, \cdots, \omega_{nK}^{DT}\}$. The sum of direct trust values of B1 to all common neighboring nodes is calculated, and the ratio of the trust value of each common neighboring node to the sum of these trust values is calculated. Next, the direct trust value of common neighboring nodes to K is multiplied by the corresponding ratio and summed, so the indirect trust value of node B1 to K is obtained, as shown in Equation (9), $\sum_{m=1}^{n} DT_{B1m}$ represents the sum of direct trust values of node B1 to common neighboring nodes, and $\frac{DT_{B1m}}{\sum_{m=1}^{n} DT_{B1m}}$ is the proportion of each direct trust value to the sum of total trust values.

$$IT_{B1K} = \sum_{m=1}^{n} \frac{DT_{B1m}}{\sum_{m=1}^{n} DT_{B1m}} * DT_{mK} \qquad (9)$$

The indirect trust weight of node B1 to K is ω_{B1K}^{IT}, and the calculation as shown

Equation (10). Similarly, $\sum_{m=1}^{n}\omega_{B1m}^{DT}$ is the sum of direct trust weights of node B1 to common neighboring nodes, and $\frac{\omega_{B1m}^{DT}}{\sum_{m=1}^{n}\omega_{B1m}^{DT}}$ denotes the proportion of each weight in the sum of its weights. Each proportion is multiplied by the direct trust weight of common neighboring nodes to K. The final sum is the indirect trust weight of node B1 to K.

3) *Comprehensive trust value*: Based on direct trust value DT_{B1K}, direct trust weight ω_{B1K}^{DT}, indirect trust value IT_{B1K}, and indirect trust weight ω_{B1K}^{IT}, the comprehensive trust value of B1 to K can calculated. σ represents normalized direct trust weight, and is calculated in Equation (11). $1-\sigma$ represents normalized indirect trust weight, and Π_{B1K} is comprehensive trust value, the calculation is given as per Equation (12).

$$\omega_{B1K}^{IT} = \sum_{m=1}^{n}\left(\frac{\omega_{B1m}^{DT}}{\sum_{m=1}^{n}\omega_{B1m}^{DT}} * \omega_{mK}^{DT}\right) \qquad (10)$$

$$\sigma = \frac{\omega_{B1K}^{DT}}{\omega_{B1K}^{DT}+\omega_{B1K}^{IT}} \qquad (11)$$

$$\Pi_{B1K} = \sigma * DT_{B1K} + (1-\sigma) * IT_{B1K} \qquad (12)$$

4) *Trust value update process*: According to Equation (6), direct trust value can be updated in each cycle. Since the number of interaction successes and interaction failures in each cycle is different, the trust value in the previous cycle is updated in combination with the penalty coefficient and reward coefficient. In addition, according to Equation (7), direct trust weight can also be updated. The corresponding direct trust weight varies with the number of interactions. So both indirect trust value and indirect trust weight will be updated according to Equations (9) and (10). Therefore, the final comprehensive trust value is updated trust value according to Equations (11) and (12). The trust value in the future cycle is calculated according to the trust value in each past cycle. The future Nth trust value is the average value of previous (N-1)th trust value, which makes future trust value more scientific and persuasive, rather than depending on trust value in a cycle.

V. EXPERIMENTAL RESULTS AND ANALYSIS

A. Experimental environment

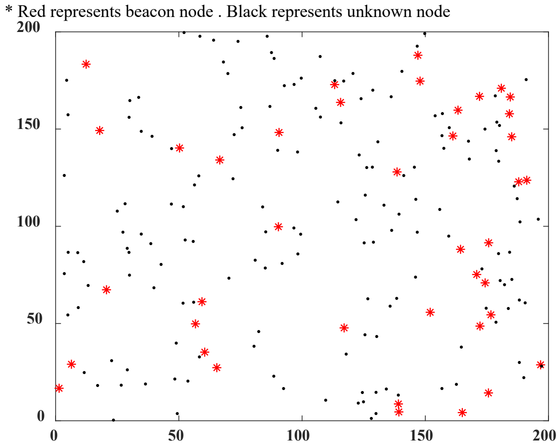


Fig.7. Node distribution diagram.

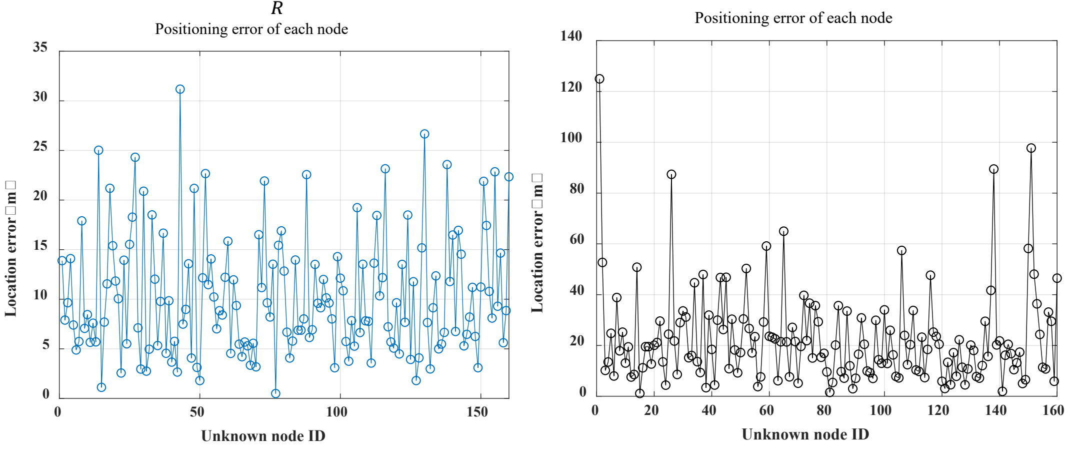
Experiments are conducted in a personal computer composed of one Intel Core i7-8700 @ 3.20GHz processor, 8G memory, and Windows 10 Operating System installed. The ANDV-HOP localization algorithm is implemented and simulated using MATLAB 2018B software. Under the same conditions, simulations and experiments are compared with schemes presented in [26][27]. Therefore, for comparison purposes, this article uses similar parameters as the ones proposed the literature by Li et al. [26], where the network is composed of 200 nodes that are randomly distributed in an area of $200 \times 200m^2$. A pair of wormhole nodes are present in the network, the node communication radius R is 30m, and L denotes the wormhole link length. The diagram of node distribution is shown in Fig.7, where "red" dots represent beacon nodes and "black" dots are unknown nodes. The node distribution in Fig.7 shows that the range of all beacon nodes can cover the whole range, which means that the wormhole detection algorithm can effectively detect attacked nodes.

B. Analysis of localization error and node connectivity

Assuming that the ratio of beacon nodes is 0.2, the localization error analysis of unknown nodes under wormhole attack is shown in Fig.8. Fig.8(a) is localization error without wormhole attack, whereas Fig.8(b) is localization error under wormhole attack. The errors in Fig.8(a) are 5 15, and those in Fig.8(b) are concentrated 10 20. Through accurate calculation, if there is no wormhole attack, the average localization error is 11.2828, and the accuracy is 37.61%; if there is a wormhole attack, the average localization error is 21.5003, and its accuracy is 71.67%. From the data, wormhole attack has a significant impact on the DV-Hop localization algorithm. The average localization error is calculated in Equation (13), and the accuracy (relative localization error) is calculated in Equation (14), where (x_i, y_i) is actual coordinate, (x_j, y_j) is the estimated value of coordinate, and n is the number of unknown nodes.

$$E = \frac{\sum_{i=1}^{n} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{n} \tag{13}$$

$$A = \frac{E}{R}$$



$$(14)$$

(a) (b)

Fig.8.(a) Positioning error without attack. (b) Positioning error with attack.

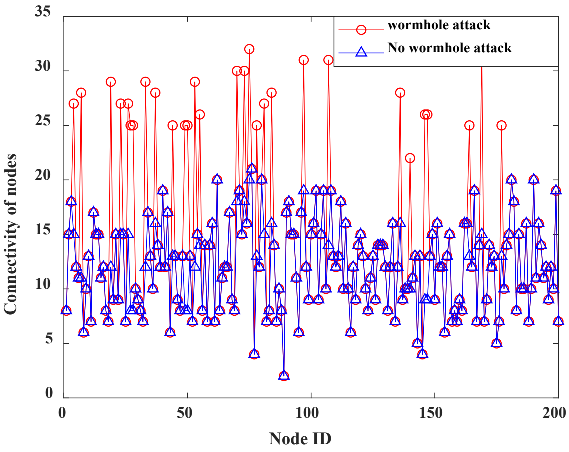


Fig. 9. Influence of wormhole attack on node connectivity.

Due to the existence of wormhole attacks, the connectivity degree of nodes(number of neighbor nodes) is close to double[26], connectivity can reflect that some nodes are abnormal. Fig.9 shows the influence of wormhole attack on the connectivity degree of nodes, and the connectivity degree of nodes attacked by wormhole is higher than that without wormhole attack, the highlighted red mark in Fig.9 indicates the connectivity of the attacked node. Therefore, the wormhole attack significantly impacts the extension structure of a normal network, affecting DV-Hop localization performance.

C. Analysis of detection success rate

The wormhole link length directly affects the success rate of detection. In order to verify the reliability of the detection method, assuming that the ratio of beacon nodes is 0.2[27], Fig.10 shows the influence of link length to communication radius (L/R) on the success rate of wormhole detection, the value of L/R represents the distance between wormhole nodes, which can affect the environment of nodes. From the curve changes shown in this figure, when L/R<2, the detection success rate of the detection method used is higher than that of AMDV-Hop, so the detection effect of ANDV-Hop is better than that of AMDV-Hop, because the range of wormhole nodes has intersection. When L/R≥2, the detection success rate of the two wormhole attacks coincides, indicating that the detection effect of the two is the same, because both do not need to eliminate nodes. Therefore, under a certain proportion of beacon nodes, the link length will impact the success rate of wormhole attack detection due to the random distribution of nodes in the network, and the effectiveness and correctness of the detection algorithm are also verified.

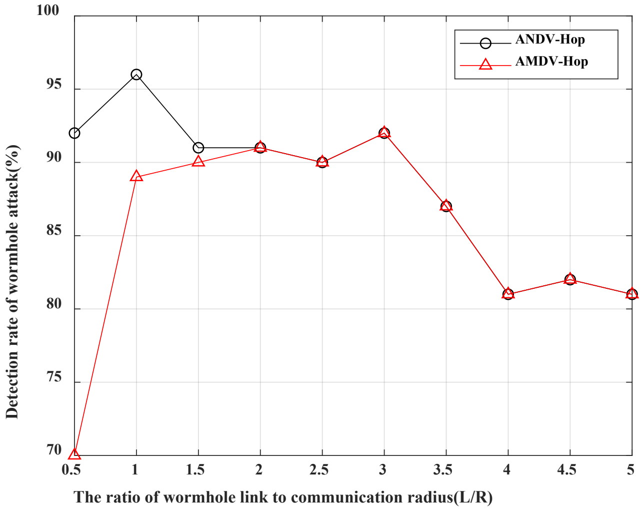


Fig.10. Influence of L/R on the success rate of wormhole attack detection.

This article mainly detects wormhole attacks by beacon nodes, so the proportion of beacon nodes directly affects the success rate of wormhole attack detection. From Fig.11, the detection success rates increase with the number of beacon nodes. By comparing the detection algorithm of the AMDV-Hop localization and the ANDV-Hop localization algorithm, it is noticeable that the detection method used is significantly higher. When the ratio of beacon nodes reaches 0.3, the detection success rate reaches more than 90%. The more significant the proportion of beacon nodes, the higher the positioning accuracy, when the ratio of beacon nodes comes 0.4, the used detection method coincides with the success rate of theoretical detection, in which the theoretical detection probability is calculated by Equation (5), and the reliability of the used method is verified by experiments.

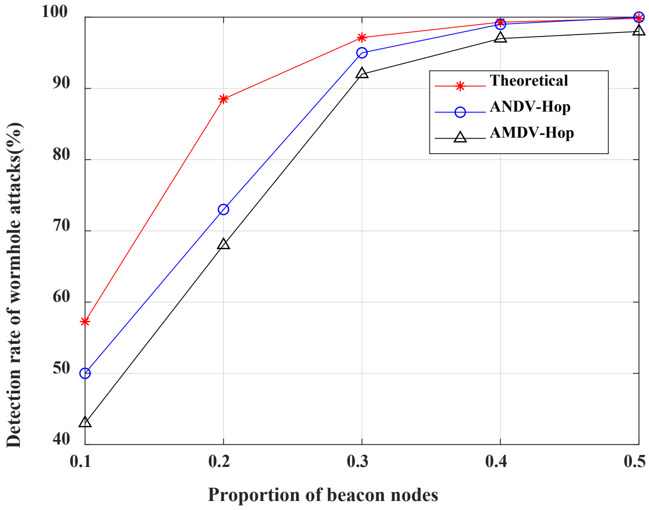


Fig. 11. Effect of beacon node ratio on the success rate of wormhole detection.

D. Analysis of implicit wormhole results

Fig.12 represents the effect of the ratio of wormhole link length to communication radius (L/R) on the relative localization error, L/R affects the detection efficiency and the positioning accuracy of unknown nodes. Because each node is generated randomly, one generation is not representative, so each value of L/R is iterated 500 times during the experimental simulation[26], and the average value is calculated to enhance data reliability and improve the localization accuracy. In Fig.12, the relative positioning error of the ANDV-Hop is lower than that of the AWDV-Hop and the LBDV-Hop, because ANDV-Hop does not eliminate nodes and has the least impact on the total hop of nodes, so the positioning error is smaller than others. The experiments verify the solution's effectiveness to the proposed implicit wormhole attack.

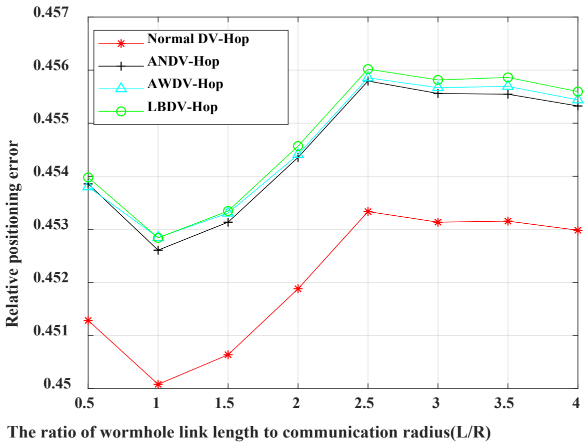
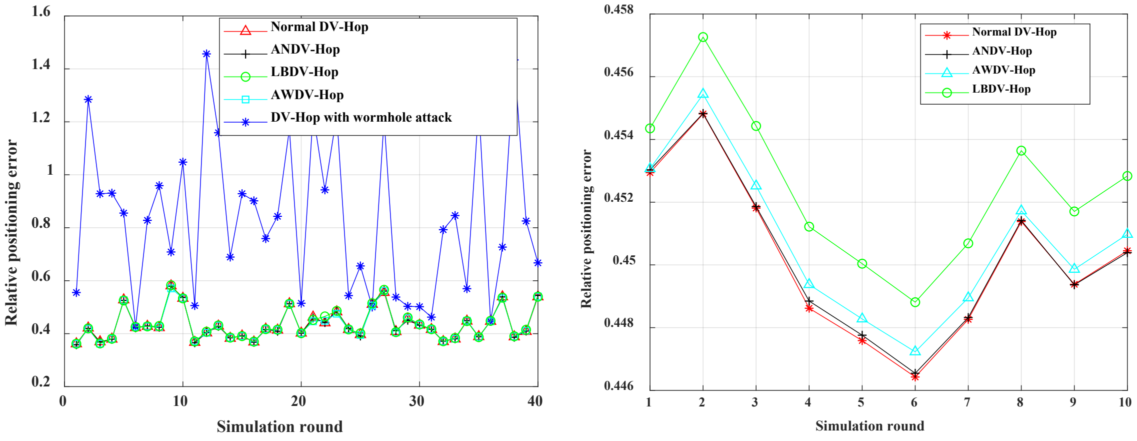


Fig.12. Effect of L/R on relative positioning error

As nodes are randomly distributed in the network, nodes are randomly generated during the simulation to change the positioning error. Fig.13 shows the effect of the number of simulations on the relative localization error to verify the correctness and reliability of the scheme proposed. To improve the accuracy, the ratio of beacon nodes is 0.2, there are ten simulations in total, and each iteration is 40. Calculating the average of the iteration times of each simulation. Fig.13(a) shows the variation of the associated localization error for 40 iterations, from which it can be seen that the ANDV-Hop localization scheme proposed overlaps with the normal DV-Hop, LBDV-Hop, and AWDV-Hop, and all of them are lower than the relative localization error with wormhole attack. Fig.13(b) verifies the characteristics of random distribution of nodes, and the relative localization error of the proposed scheme is closer to that of a wormhole-free attack. Fig.13 shows that when the number of interactions between nodes in the network is more, the relative positioning error of the method proposed in this paper is closer to the free-attack network.



(a) (b)

Fig.13. Influence of iteration number on relative positioning error.

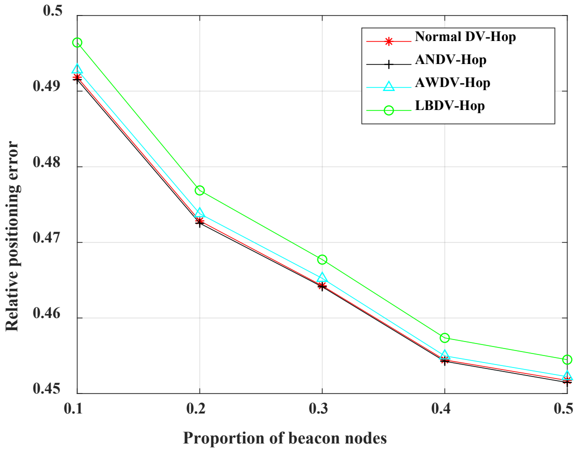


Fig.14. Influence of beacon node ratio on relative positioning error.

The two essential parameters in the DV-Hop localization algorithm are the number of hops and the average hop distance, the ratio of beacon nodes directly affects the variation of hops and the calculation of average hop distance, when the number of beacon nodes increases, localization accuracy will theoretically improve, and localization error will decrease. Fig.14 shows the influence of the beacon node's proportion on relative positioning error. When the number of beacon nodes increases, the ANDV-Hop scheme proposed and the wormhole-free DV-Hop, AWDV-Hop, and LBDV-Hop show a downward trend. In addition, the localization error of the ANDV-Hop localization scheme proposed largely overlaps with that of the wormhole-free localization scheme and is lower than that of both AWDV-Hop and LBDV-Hop. The experimental results verify the theoretical conjecture and demonstrate the scheme's feasibility.

E. Analysis of explicit wormhole results

Explicit wormhole attack localization can eliminate the attacking nodes through trust model mechanism and eradicate the impact of wormhole attack on the DV-Hop localization algorithm. Both AWDV-Hop and LBDV-Hop localization schemes do not remove the wormhole nodes from the network but mark the beacon and unknown nodes directly. Fig.15 shows the change of node connectivity when 0<L<2R. Since AWDV-Hop and LBDV-Hop remove some nodes from the network or neighboring list, both change the number of neighboring nodes for some nodes, causing waste of resources, and affecting node localization performance. From Fig.15, the node connectivity degree of the scheme proposed is higher than that of the two schemes.This is because the proposed method does not need to eliminate normal nodes. Nodes not labelled in the figure have the same node connectivity degree, illustrating the reliability and effectiveness of the approach.

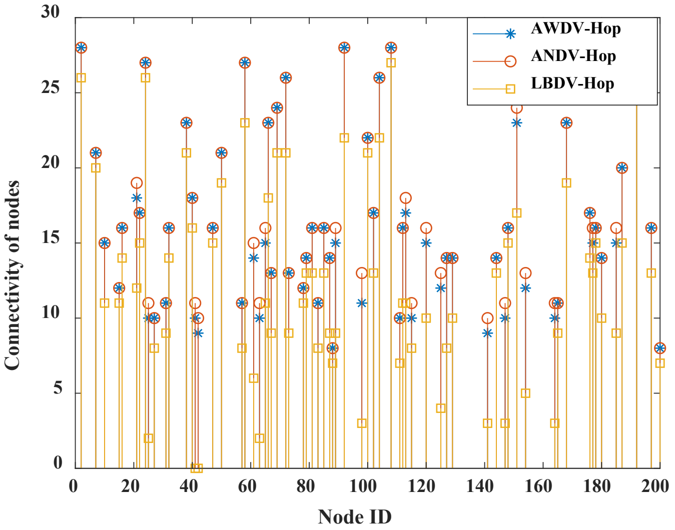


Fig. 15. Node connectivity with an intersection.

The change of node connectivity means that the node layout changes, so the sum of minimum hops between nodes will also change. Fig.16 represents the effect of wormhole link length on the total hops communicated between nodes in the network, where ITH indicates the total hops added to the communication between nodes, and the changed hops directly affect the performance and accuracy of the DV-Hop localization algorithm. The total hops of ANDV-Hop proposed are lower than AWDV-Hop and LBDV-Hop in Fig.16. Since AWDV-Hop and LBDV-Hop delete some nodes, or their ordinary neighbors are deleted, some nodes have to find other paths, so their hop numbers increase. Moreover, the ANDV-Hop proposed has the most negligible influence on ITH, ensuring the accuracy of the DV-Hop positioning algorithm.

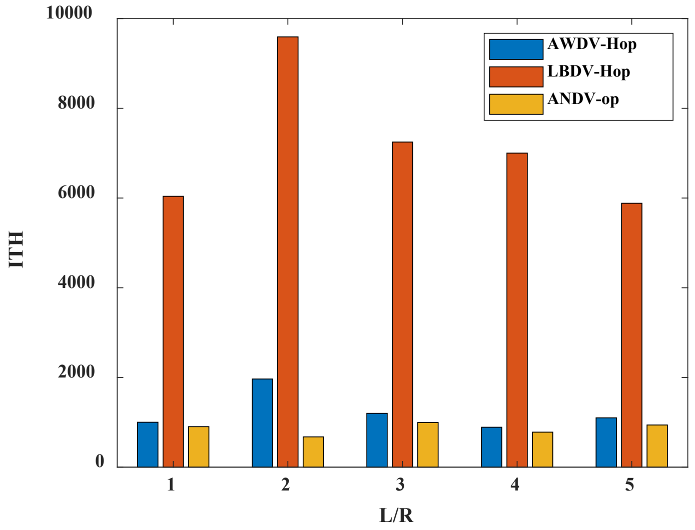
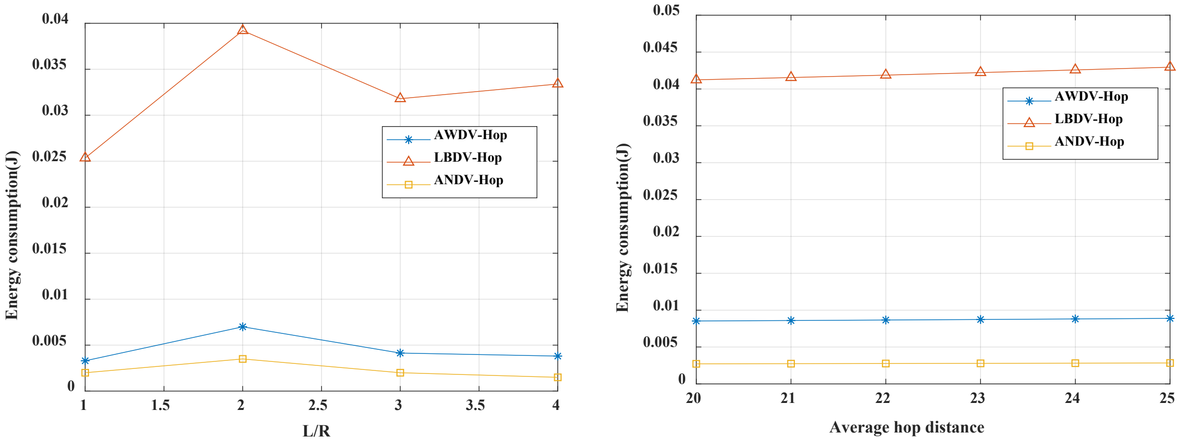

10000
8000
6000
4000
2000
0
ITH
1
2
3
4
5
L/R
AWDV-Hop
LBDV-Hop
ANDV-op

Fig. 16. Effect of link length on the total number of node communication hops.



(a) (b)

Fig.17 Effects of link length(a) and average hop diatance(b) on energy consumption.

Distributed wireless sensor networks communicate through channels, and sensor nodes will consume energy in the process of communication or calculation. Since nodes are limited by battery energy, so it must consider the energy consumption of nodes. Equation (15) gives the energy consumed by transmitting μ bit data over a distance of d meters. Different energy loss models are used according to the size of transmission distance[36]. When d is large, the Free-space Path Loss model is selected, while the Multipath Fading model is selected when d is small. The value of d depends on the distance threshold d_0, where E_e represents the energy consumed by the sensor module to receive 1 bit of data, ε_f and ε_a represent the energy consumed by the two models to enlarge the signal, and the real energy consumed by calculation is E_r. According to [36], assuming that initial energy is 150J, the message accounts for 10 bytes. The specific values of the parameters are shown in Table III. According to Equation(15), the difference between L/R and average hop distance affect energy consumption. Fig.17(a) shows the effect of link length on energy, and Fig.17(b) shows the impact of average hop distance on energy. Observing Fig.16, the total number of hops (ITH) of the proposed ANDV-Hop is the smallest, and from Fig.17, it is known that the energy consumption of the ANDV-Hop is significantly lower than that of AWDV-Hop and LBDV-Hop, further verifying the rationality and reliability of the approach.

$$E_r = \begin{cases} \mu E_e + \mu \varepsilon_f d^2 d < d_0 \\ \mu E_e + \mu \varepsilon_a d^4 d > d_0 \end{cases} \tag{15}$$

TABLE III. CORRESPONDING VALUES OF PARAMETERS

PARAMETERS	VALUES
E_e	5×10^{-8}J/bit
μ	80bit
E	150J
ε_f	1×10^{-11}J/(bit·m^2)

ε_a	1.3×10^{-15}J/(bit·m^4)

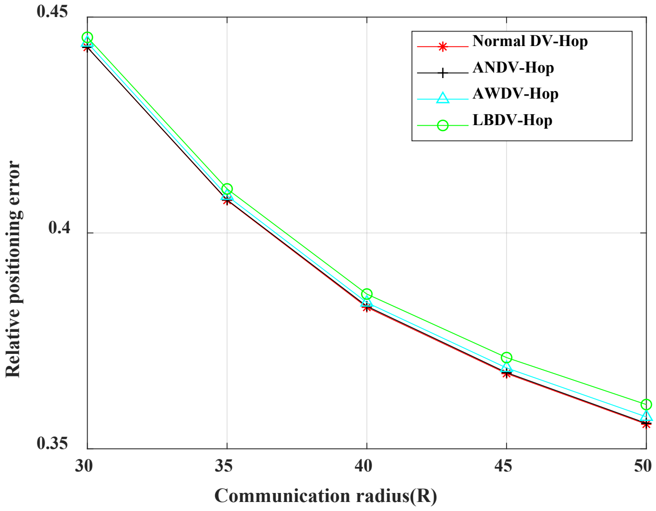


Fig.18. Effect of communication radius on relative positioning error.

Fig.18 shows the influence of node communication radius on positioning error. From Fig.18, as the communication radius of the node changes, the relative positioning error decreases with the increase of the communication radius. As the number of beacon nodes in the communication area increases with the increase of the radius, the localization error is reduced. In addition, the relative localization error of the proposed approach is close to the standard DV-Hop algorithm and lower than AWDV-Hop and LBDV-Hop.

VI. CONCLUSIONS AND FUTURE WORK

In this article, we propose a novel secure DV-Hop localization algorithm (ANDV-Hop) against the wormhole attack, aimed at (1) wormhole attack detection: the existence of wormhole attack can be detected according to three characteristics, from which attacked nodes can be estimated. Experiments show that the success rate for detecting the used method is higher than that of the AWDV-HOP positioning approach. As the ratio of beacon nodes reaches 0.4, it is the same as the theoretical success rate for detection, indicating the feasibility of the used method, (2)the ANDV-Hop security localization method: both implicit and explicit wormhole attacks use the beacon nodes under attack to delegate their neighboring nodes to send data messages, if the other end of the wormhole link receives data messages or neighboring nodes violate one of the three characteristics, and it can decide which neighboring nodes are in the attack range of the wormhole node, the intersection of the communication area of these neighboring nodes must contain wormhole node, narrowing the range where the wormhole node is located.

The nodes in the intersection region close to the wormhole nodes are selected to broadcast messages for the implicit wormhole attack. The process is to inform other nodes to delete beacon nodes at the other end of the link from the neighboring list so that the nodes in the scope of two wormhole nodes are separated from each other. For the explicit wormhole attack, the trust model is used to calculate the comprehensive trust value of nodes in the intersection range, and punishment and reward coefficients are set in the trust model. The wormhole node only forwards messages but does not reply to confirmation messages, and its trust value will decrease continuously, so the two nodes will be deleted from the network. Experimental results show that the relative positioning error of ANDV-Hop is less than AWDV-Hop and LBDV-Hop with lower energy consumption.

Next, the article will further study the impact of wormhole attacks on the DV-Hop localization algorithm process. Due to the complexity of the sensor network environment, there may be different communication ranges of each node and multiple wormhole links in the network, which will have a more significant impact on the localization algorithm. Furthermore, combining more complex scenarios and considering multiple attack modes in future investigations via a possible modification of the localization algorithm proposed here, node communication, identification, and coverage /interference among the different attacks. In addition, this article will consider the impact of node mobility on the location algorithm.

Conflicts of interest/Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Availability of data and material

Data available upon request to the authors.

Code availability

The source code of the implementations used to compute the present results can be obtained by contacting corresponding authors.

Acknowledgement

This research is supported by the National Natural Science Foundation of China under Grant 61873160 and Grant 61672338, Natural Science Foundation of Shanghai under Grant 21ZR1426500.

REFERENCES

[1] M. Cui, D. Han, J. Wang, K. -C. Li and C. -C. Chang, "ARFV: An Efficient Shared Data Auditing Scheme Supporting Revocation for Fog-Assisted Vehicular Ad-Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15815-15827, Dec. 2020, DOI: 10.1109/TVT.2020.3036631.

[2] M. Cui, D. Han and J. Wang, "An Efficient and Safe Road Condition Monitoring Authentication Scheme Based on Fog Computing," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9076-9084, Oct. 2019, DOI: 10.1109/JIOT.2019.2927497.

[3] N. Labraoui, M. Aliouat, and M. Gueroui, "Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks", Transactions on Emerging

Telecommunications Technologies, 23(4), p. 303-316, June 2012.

[4] W. Liang, W. Huang, J. Long et al., "Deep Reinforcement Learning for Resource Protection and Real-time Detection in IoT Environment", in IEEE Internet of Things Journal, 7(7), p. 6392 - 6401, IEEE, 2020.

[5] W. Liang, K. Li, J. Long et al., "An Industrial Network Intrusion Detection Algorithm Based on Multifeature Data Clustering Optimization Model", IEEE Transactions on Industrial Informatics, 16(3), p. 2063-2071, 2020.

[6] J. Chen, S. Wang, M. Ouyang et al., "Iterative Positioning Algorithm for Indoor Node Based on Distance Correction in WSNs", Sensors, 19(22), 4871, MDPI, Nov 2019.

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

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

[9] G. Farjamnia, Y. Gasimov, and C. Kazimov, "Review of the techniques against the wormhole attacks on wireless sensor networks", Wireless Personal Communications, 105, p. 1561–1584, 2019.

[10] D. Han, N. Pan, K. Li, "A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection", IEEE Transactions on Dependable and Secure Computing, 19(1)，p.316-327, IEEE, 2022.

[11] T. H. Kim, R. Goyat, M. K. Rai, G. Kumar, and R. Thomas, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks", IEEE Access, 99, p. 1–1, 2019.

[12] L. Xiao, D. Han, X. Meng et al., "A Secure Framework for Data Sharing in Private Blockchain-Based WBANs", IEEE Access, 8, 153956-153968, IEEE, 2020.

[13] D. Han, Y. Zhu, D. Li, W. Liang, A. Souri and K. -C. Li, "A Blockchain-based auditable access control system for private data in service-centric IoT environments," in IEEE Transactions on Industrial Informatics, 18(3), p.3530-3540，IEEE，2020.

[14] J. Xu, D. Han et al., "A K-means algorithm based on characteristics of density applied to network intrusion detection", Computer Science and Information Systems, 17(2), 665-687,COMSIS, 2020.

[15] Tian, Q., Han, D., Li, KC. et al. "An intrusion detection approach based on improved deep belief network". Appl Intell 50, 3162–3178 (2020).

[16] Zhang, W., Han, D., Li, KC. et al. "Wireless sensor network intrusion detection system based on MK-ELM". Soft Comput 24, 12361–12374 (2020).

[17] R. K. Dwivedi, P. Sharma, and R. Kumar, "Detection and prevention analysis of wormhole attack in wireless sensor network", in 2018 8th International Conference on Cloud Computing, Data Science and Engineering (Confluence), 2018.

[18] R. Verma, R. Sharma, and U. Singh, "New approach through detection and prevention of wormhole attack in manet", p. 526–531, 2017.

[19] C. Ji, "Research on Location Algorithm of Non-ranging Nodes in Wireless Sensor Networks", PhD thesis, Jiangxi University of Science and Technology, 2015.

[20] G. Liu, Z. Qian, and X. Wang, "An improved DV-Hop localization algorithm based

on hop distances correction", Communications, China, 2019.

[21] M. Ghafour, S. H. Kamel, and Y. Abouelseoud, "Improved DV-Hop based on squirrel search algorithm for localization in wireless sensor networks", Wireless Networks, 27, p. 2743–2759, 2021.

[22] A. Kaushik, D. K. Lobiyal, and S. Kumar, "Improved 3-dimensional DV-Hop localization algorithm based on information of nearby nodes", Wireless Networks, 27, p. 1801–1819, 2021.

[23] X. Huang, D. Han, M. Cui, G. Lin, and X. Yin, "Three-Dimensional localization algorithm based on improved a and DV-Hop algorithms in wireless sensor network", Sensors, 21, (2), p. 448, 2021.

[24] D. Han, Y. Yu, K. C. Li, and R. Mello, "Enhancing the sensor node localization algorithm based on improved DV-Hop and DE algorithms in wireless sensor networks", Sensors, 20(2), 343, 2020.

[25] C. Kairen, "Research on Wormhole Detecting Scheme Based on Hierarchy Structure in WSN", PhD thesis, Liaoning University, China, 2018.

[26] J. Li, D. Wang, and Y. Wang, "Security DV-Hop localization algorithm against wormhole attack in wireless sensor network", IET Wireless Sensor Systems, 8, (2), p. 68–75, 2017.

[27] 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, 16, Part A, p. 22–35, 2015.

[28] S. Deshmukh-Bhosale and S. S. Sonavane, "A realtime intrusion detection system for wormhole attack in the RPL based Internet of Things", Procedia Manufacturing, 32, p. 840–847, 2019.

[29] X, Luo, Y, Chen, Miao, Li, Qian, Luo, Kang, and Xue, "CREDND: A novel secure neighbor discovery algorithm for wormhole attack", IEEE Access, 7, p. 18194-18205, 2019.

[30] N. Tamilarasi and S. G. Santhi, "Detection of wormhole attack and secure path selection in wireless sensor network", Wireless Personal Communications, 114, p. 329–345, 2020.

[31] D. Ping and Z. Hongjiang, "A DV-Hop localization algorithm for wormhole resistance in wireless sensor networks", Journal of Southwest Jiaotong University, 50, 1, p. 51–57, 2015.

[32] J. Li and D. Wang, "The security DV-Hop algorithm against multiple-wormhole node link in WSN", KSII Transactions on Internet and Information Systems, 13, 4, p. 2223–2242, 2019.

[33] X. Zhu, K. Li, J. Zhang et al., "Distributed Reliable and Efficient Transmission Task Assignment for WSNs", Sensors, 19(22), 5028, MDPI, Nov 2019.

[34] D. Zhengfei, "Research on attackresistant secure localization algorithm for wireless sensor networks", PhD thesis, Southwest Jiaotong University, 2018.

[35] F. Yahui, "Research on trust model of wireless sensor network based on recommendation and risk control", PhD thesis, South China University of Technology, 2020.

[36] C. Tang, D. Han, and J. Wang, "A low resource consumption clone detection

method for multi base station wireless sensor networks", IEEE Access, 8, p. 128349-128361, 2020.