International Journal of Smart Home
Vol. 9, No. 12, (2015), pp. 101-112
http://dx.doi.org/10.14257/ijsh.2015.9.12.11

An Improved DV-Hop Localization Algorithm Against Wormhole Attack in WSN

Jiuhu Zheng[1,2] and Huanyan Qian[1]

[1] School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing,210094,China
[2] School of Information Technology, Jiangsu Institute of Commerce, Nanjing,211168,China
zhjiuhu@163.com,hyqian@njust.edu.cn

Abstract

Wormhole attack is one of the most serious attacks on DV-Hop localization algorithm. Previous solutions usually require hardware support, or a higher ratio of beacon nodes and very complex mathematical operations. In this paper, we analyze the effect of the wormhole attack on DV-Hop algorithm, which mainly destroys the network topological structure and shrinks hop count between nodes and expands the localization error. We propose a modified DV-Hop method without additional hardware support against wormhole attacks. Through analyzing the characteristics of the neighboring nodes set of nodes attacked, this method detects wormhole attack, then locates nodes by using an improved DV-Hop algorithm. We show that the scheme can detect wormhole attacker adequately, and the obtained localization accuracy is even better than that of the DV-Hop method without wormhole attacks in most cases.

***Keywords**: DV-Hop, wireless sensor network, wormhole attack, positioning accuracy*

1. Introduction

Wireless sensor network (WSN) plays a huge role in many aspects due to its advantages, such as low cost, flexible easy networking, being applied to special environments [1], etc. Usually the nodes are randomly deployed without being set in advance [2], which needs to design localization algorithms. Node localization algorithms in WSN are mainly classified into two categories: range-based and range-free [3]. Though the former is better than the latter in location accuracy, the node must be outfitted with measurement distance, measurement angle, directional antenna or other hardware. The latter does not need hardware support and can meet the most the location accuracy requirements so that it is widely used. DV-Hop [4][5] algorithm is one of the most widely used algorithms in range-free, since it is a simple algorithm and has high localization accuracy.

DV-Hop algorithm has poor security. When under attack, its localization accuracy will be reduced greatly. Wormhole attack [6-7] is more serious attack method, which can damage the topology structure of WSN. When a wormhole node receives a data packet, it will transmit the information to another wormhole node through a low latency tunnel, then replay or tamper the information. The two nodes with larger distances originally are mistaken for neighbor nodes each other, and make hop between two nodes less, so it has great influence on the localization accuracy of the DV-Hop. In recent years, the research directions of optimizing DV-Hop localization algorithm mostly focus on using additional hardware support or whether the hop distance between nodes is larger than the communication radius of nodes, and mainly aim at discovering wormhole nodes. While the researches on how to reduce the impact of wormhole attacks to achieve better localization accuracy are lesser [6-13].

ISSN: 1975-4094 IJSH

For the wormhole attacks on DV-Hop, this paper proposes an improved DV-Hop localization algorithm(NSDV-Hop) based on mutual neighboring nodes set, which uses the relationship of the neighboring nodes set of attacked nodes to detect the attacked nodes by wormhole, and locates with the improved MHDV-Hop method [15]. The algorithm greatly reduces the impact of wormhole attack on DV-Hop algorithm. Even if the distances between wormhole nodes are far away, it also can achieve better positioning accuracy.

The main contributions in this paper include:

(1) Put forward the wormhole attack detection method based on the mutual neighboring node set;

(2) Take the classification processing of the attacked nodes, improve the positioning accuracy. Combined with MHDV-Hop, NSDV-Hop algorithm is proposed for resisting wormhole attack;

(3) Through the simulations, verify the effectiveness of NSDV-Hop algorithm. In most cases, compared with basic DV-Hop and basic DV-Hop witho wormhole attack, it can achieve better accuracy, basically eliminating the effect of implicit wormhole attack on DV-Hop algorithm.

The rest of the paper is organized as follows: the second section introduces the related works of the wormhole attack detection and defense, and carries on the analysis; the third part introduces the hypothesis model for NSDV-Hop to defense wormhole attacks; the fourth part introduces the NSDV-Hop algorithm; the fifth part is the simulation and the analysis; the sixth part is the conclusion.

2. Related Works

The wormhole attack is usually composed of two malicious nodes that cooperate together to launch attacks. A malicious node will transmit information received to another malicious node via a private tunnel. Although the two malicious nodes are perhaps far apart, but there is only one hop distance. The wormhole attack can reduce the hop count. Many shortest paths between nodes will pass through the private tunnel, and the wormhole node will tamper with the packets or make node location errors greatly increased.

The wormhole attack is divided into hidden wormhole attack and exposed wormhole attack [6]. As for the hidden wormhole attack, the attacker often does not modify after receiving data packet of node A in general. The tunnel will transmit the data packet to another attack node in distant end to replay. When node B receives the replayed data packet, it will mistake that node A is its neighboring node. Hidden wormhole attackers generally do not appear in the routing table. As for exposed wormhole attack, after an attacker receiving the data packet of node A, it will transmit it to another attacker in distant end, then this attacker transmits the information with its header file to node B. The attackers appear in the routing table. Aiming at the wormhole attack, many scholars have proposed different solutions [6-13].

Literatures [6] and [7] have proposed a wormhole attack detection and defense mechanism of packet leash, and put forward two kinds of leash: geography leash and time leash. Geography leash requires the node to know its position in advance and should be synchronized with the clock. Obtaining the position of node and synchronizing the clock need the additional hardware support, such as using GPS positioning to obtain the position information of each node, the cost is more expensive. Time leash requires strict time synchronization, since the distance between the nodes are short in general, time synchronization requires to reach to the nanosecond-level precision. Affected by the environmental factors, it is difficult for WSN to achieve this. This detection method can be used to hidden wormhole attack. Literatures [7] applies Hash tree into time leash and puts forward an optimized TIK method.

Literature [8] puts forward a wormhole attack detection method based on the directional antenna, the node periodically sends the message to confirm all the neighbors in the direction indicated by the directional antenna. All the nodes share the directional information to prevent the malicious node disguising as the neighbor node. Even it does not require positioning and time synchronization, it needs directional antenna. When many nodes attack, it cannot detect all the wormhole nodes.

Literatures [9] and [10] have proposed a wormhole detection mechanism. When the calculated hop size of a node is greater than the communication radius, the nodes are considered to be under the wormhole attack. Usually the hop size is much smaller than the communication radius R, it is about 0.7R. Even if under attack, the node’s hop size becomes larger, and it may not be more than R, that the attacker could not be detected.

Literature [11] puts forward a program to conduct data investigation on wormhole node, it can be applied to two types of wormhole attack detection. It detects the wormhole attack through the monitoring and analysis on several important factors, such as the processing time of intermediate node and the modified frequency of neighbor list, etc. This program is complicated, there are many other factors affect the detection effect.

Literature [12] puts forward a wormhole attack detection method based on the signal processing technology, it proposes that transfers the receiving time data into “signal” and sends it out consciously, analyzes it at the destination node and then uses fast Fourier transform to transfer that signal to the frequency domain and conduct analysis to detect wormhole attack. That method needs to have the signal recognition and processing function, which has high requirement on the nodes.

Literature [13] puts forward a safe positioning mechanism to defend the wormhole attack based on the label during the localization process of DV-Hop, the communication mechanism is more complex. It includes three phases: beacon node label, node label and safe positioning based on DV-Hop. It identifies the wormhole attack based on the self-exclusion of node, label mechanism of beacon node, the uniqueness of data packet and other properties. If the data packet received by node violates the three properties above, it is thought to be attacked by the wormhole node and is marked.

Literature [14] puts forward the PDWA wormhole attack detection algorithm based on the only pre-order node, it uses the feature that wormhole node is usually set as the only pre-order node to conduct wormhole node detection, the algorithm is simple and can fully detect the wormhole node. This algorithm is applicable to the exposed wormhole attack.

3. Hypothesis

Hide wormhole attack is a common and effective method for attacking DV-HOP algorithm. NSDV-Hop algorithm detects the hidden wormhole attack based on the neighboring nodes set. It overcomes the problem that hidden wormhole attack and defense method mainly depends on the hardware support and hop size being greater than the node communication radius. As shown in Figure 1, when two wormhole nodes attack, the attacker's neighboring nodes(S_1,S_2,S_3,S_4) would think another attacker’s neighboring nodes (S_5,S_6,S_7,S_8) are their neighboring nodes, forming a set of neighboring nodes ｛S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8｝. In the case of no additional hardware support, NSDV-Hop uses of neighboring nodes set to detect the wormhole attack and finds out the attacked node, then it improves localization accurate.

In order to illustrate NSDV-HOP, set h_{AB} as the minimum hops between node A and node B, and the definition is provided as follows:

Definition 1. *Preorder node* [15] (PN), if any node A, B, X, $\exists h_{AB}=1$ and $h_{BX}=h_{AX}-1$, thus node B is the preorder node from node A to node X, marked as: $B \in P_X(A)$.

Definition 2. *Neighboring nodes set* (S_N), the neighboring nodes set of node A is: the nodes set that is one hop far away from node A, marked as S_N (A), as shown in formula (1).

$$\forall B \in S_N(A) \Rightarrow h_{AB} = 1 \qquad (1)$$

Definition 3. *Attacked nodes set*（S_W）, the neighboring nodes sets of a pair of wormhole attacker M and N are S_N(M) and S_N（N）, the set of attacked nodes（S_W）is shown in formula (2).

$$S_W = S_N(M) \cup S_N(N) \qquad (2)$$

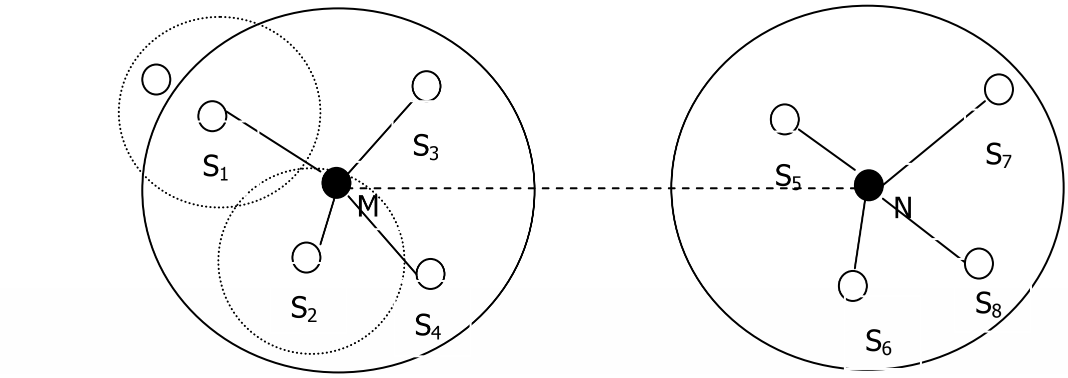


Figure 1. Schematic Diagram of the Ends of the Neighboring Node under Wormhole Attack

As shown in Figure 1, S_W is {S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8}. When attacked by many wormholes, many S_W will appear, marked as S_W (i).

Definition 4. *Mutual neighboring nodes set*（S_M）, when judge S_W, assume a node's neighboring nodes includes itself, that is to say, the neighboring nodes of node A includes node A. S_M meets the formula (3).

$$\forall A \in S_M \Rightarrow S_N(A) \cap S_M = S_M \qquad (3)$$

Definition 5. *Fully attacked node*（N_F）: If the set of neighbor nodes S_N (A) is a true subset of attacked nodes set S_W, marked as: $S_N(A) \subseteq S_W$,thus node A is called as the fully attacked node. As shown in Figure 1, node S_2 is N_F.

Definition 6. *Part attacked node*（N_P）: If the set of neighboring nodes S_N (A) is not a subset of the set of attacked nodes S_W, marked as: $S_N(A) \not\subset S_W$,thus node A is called as part attacked node. As shown in Figure 1, node S_1 is N_P.

4. NSDV-Hop System Model

In this section, we have described the main ideas of NSDV-Hop positioning algorithm, including three stages:

a. find out the attacked nodes set $S_{W;}$

b. classify the S_W nodes for processing;

c. locate with the MHDV-Hop algorithm.

4.1 Find out the Attacked Node Set S_W

When a pair of wormhole attackers M and N begin to attack, the nodes within their communication radius will be affected. Choose from M to N channel as the shortest path, then the neighbor nodes of M and N become the mutual neighboring nodes set S_M. When we defend against wormhole attack, first find the S_M under attacks, and conduct processing. Since it may be under multi pairs of wormhole attackers, there may be multiple mutual neighboring nodes sets, respectively expressed as S_M(i) (i=1, 2, 3,…), and union of them is S_W. Because DV-Hop algorithm usually requires the average connectivity more than 16 in WSN. Suppose node A is a attacked node, $S_N(A)$ contains sets of the two attackers' neighboring nodes and the neighboring nodes set of its own . In order to reduce the computational complexity, when solve the attacked nodes set, set the minimum node number (N_{min}) of the attacked nodes set. If the number of neighboring nodes of a node is less than N_{min}, the node is not considered as an attacked node. The value of N_{min} is too large to detect all attacked nodes. While N_{min} is too small, the amount of calculation will be increased. Through the experimental analysis, set N_{min}=30.

The main procedures of finding S_W are as follows:

a. Record the neighboring nodes set $S_N(i)$ of each node, including the increased neighboring nodes due to wormhole attacks.

b. Supposed k is the number of wormhole node pairs(In general two wormhole nodes which communicate each other through a tunnel are a pair of wormhole nodes), and set k=0. Calculate the length of $S_N(i)$ of each node, which is recorded in the array L_N, as shown in the formula (4).

$$L_N[\mathrm{i}] = length(\mathrm{S}_{\mathrm{N}}(i)) \tag{4}$$

c. Sort L_N in descending order, and store the node ID of each node which satisfies $L_N[i] \geq N_{min}$ into the set S_{ID} in proper order.

d. Calculate n, m, and $S_{max,}$ as shown in the formulas (5), (6) and (7).

$$n = length(S_{ID}) \tag{5}$$

$$m = \mathrm{S}_{\mathrm{ID}}(1) \tag{6}$$

$$S_{max} = S_N(m) \tag{7}$$

e. Calculate the mutual neighboring nodes set S_M of node m, carry out the following codes:

```
$S_{temp}=\Phi$;
for j=2:n
   $S_{\cap}=S_{max}\cap S_N(S_{ID}(j))$;
   if length($S_{\cap}$) $\geqslant N_{min}$
      $S_{temp}=S_{\cap}$;
   end
end
if $S_{temp}\neq\Phi$
    $S_{ID}=S_{ID}-S_{temp}$
    k=k+1;
    $S_M(k)=S_{temp}$
else
    $S_{ID}=S_{ID}-\{i\}$
end
```

f. If $S_{ID} \neq \Phi$, return d.

In case of not being attacked, the circumstance that more than 30 nodes are SM rarely occurs, so the calculated S_M (i) is the set of attacked nodes.

The computational formula of S_W is shown as the formula (8).

$$S_W = \bigcup_{i=1}^{k} S_M(\mathrm{i}) \tag{8}$$

4.2. Classify the Nodes of S_W for Processing

After finding S_W, it should be processed. If all the nodes in S_W are removed, a greater cavity will be generated in the communication radius of wormhole node, and hops between its surrounding nodes will increase, which will greatly increase the localization error. The nodes in S_W can be divided into the attacked beacon node, entirely attacked node N_F and partially attacked node N_P according to their different characteristics. Then they are processed according to classification, so as to reduce the impact of this cavity attacked.

The discriminated method of V_F and V_P is shown as the formula (9).

$$S_N(\mathrm{i}) - \mathrm{S}_W \begin{cases} = \Phi & i \in N_F \\ \neq \Phi & i \in N_P \end{cases} \tag{9}$$

The following respectively processes three types of nodes.

a. Attacked beacon node

Assume the set of beacon nodes attacked is NB. It is harmful that a node in NB continues to localize for other unknown node. So it should be deleted. The process mode of node i on the NB in Formula (10).

$$S_N(\mathrm{i}) = S_N(\mathrm{i}) - N_B \tag{10}$$

b. Entirely attacked node (N_F)

All neighboring nodes of NF are attacked, all nodes which can be with the help of location are not credible, which should be deleted. The process mode of any node i on the node NF is showed in Formula (11).

$$S_N(\mathrm{i}) = S_N(\mathrm{i}) - N_F \tag{11}$$

c. Partially attacked node (NP)

Partial neighboring nodes of N_P are not attacked and positioning by relying on those nodes. Set the non-attack neighboring nodes set is S_P (i). N_P node processing is as follows:

ⅰ. Delete S_W in the neighboring nodes table of any node i, as shown in Formula (12).

$$\forall i \in N_P, \mathrm{S}_\mathrm{N}(\mathrm{i}) = \mathrm{S}_\mathrm{N}(\mathrm{i}) - \mathrm{S}_W \tag{12}$$

ⅱ. Any node i, j$\in N_P$, k is a node without attacked, if h (i, k) = 1 and h (j, k) = 1, it is considered that i and j are real neighboring nodes. Set h (i, j) = 1.

4.3. Locate with the MHDV-Hop Method

After the treatment in section 4.2, obtain the new neighboring nodes set $S_N(i)$ of each node. It is set that a node is one hop from its neighboring nodes. Then apply the MHDV-Hop method to positioning. Use the neighboring nodes table from section 4.1 and section 4.2 to calculate the number of hops and average hop size between nodes (calculation method is the same as DV-Hop), then correct them. Assume node a is any beacon node and node i is any unknown node. The preorder nodes set from node i to node a is denoted as P_a (i), and the number of the preorder node from node i to node a is denoted as N_a (i).

Modified MHDV-Hop algorithm is described as follows [15]:

a. Calculate the number of the preorder nodes from any nodes to any beacon node: traverse all the nodes, record the preorder nodes from node i to the beacon node a in $P_a(i)$, and count $N_a(i)$ of each node i (if N_a (i) > 7, set N_a (i) =7). Sort by the beacon node $N_a(i)$ and ID in ascending order. Successively calculate the correction coefficients from node i to beacon node a in this order.

b. Calculate e the correction coefficient E_{last} from node i to the beacon node a. Take K value of 7. Use the formula (13) to calculate E_{last} from the unknown node i to the beacon node a.

$$E_{last} = \begin{cases} \frac{2}{K}\left(\left\lceil \frac{K}{2} \right\rceil - N_a(i)\right), & N_a(i) < K \\ \frac{2}{K}\left(\left\lceil \frac{K}{2} \right\rceil - K\right), & N_a(i) \geq K \end{cases} \tag{13}$$

c. n is the hop count from the unknown node i to the beacon node a. Set n=1, use the formula (14) to calculate the correction coefficient $E_a(i)$ from the node i to the beacon node a. Set the correction coefficient E_a (i) of unknown node i away from beacon node a for one-hop as 0, and $E_0 = 0$.

$$E_a(i) = \begin{cases} 0, & N_a(i) = 0 \\ E_{last} + E_{n-1}, & N_a(i) > 0 \end{cases} \tag{14}$$

d. Set n=n+1, and calculate the average correction coefficients E_{n-1} of all preorder node hops to the beacon node a using the formula (15).

$$E_{n-1} = \frac{1}{N_a(i)} \sum E_a(j),\ j \in P_a(i) \tag{15}$$

e. Then calculate the correction coefficient $E_a(i)$ with the formula (14).

f. If there is any other unknown node away from beacon node a for n hops, calculate its correction factor E_a (i) away from beacon node a according to ⑤-⑥;

g. If there are other beacon nodes, repeat ②-⑥.

h. Calculate the distance from each node to the beacon node. The calculation method of $HopSize_a$ of beacon node a is the same as that of the DV-Hop method. The hop count from the unknown node i to the beacon node a is denoted as h_{ia}. The distance between the unknown node i and the beacon node a is denoted as d_{ia}. That unknown node i is the first to receive $HopSize_a$ denoted as $HopSize_i$. Calculate d_{ia} as shown in formula (16).

$$d_{ia} = HopSize_i \times (h_{ia} + E_a(i) / \mathrm{h}_{ia}) \tag{16}$$

i. Subsequently calculate the distance from each unknown node to each beacon node by the method of ⑧.

j. Use maximum likelihood method to calculate the position of each unknown node.

5. Analysis of Simulation Results

In this section, we uses MATLAB to conduct simulation experiment and compares and analyzes the localization accuracy of DV-Hop method not attacked by the wormhole, DV-Hop method attacked by the wormhole and NSDV-Hop method attacked by the wormhole.

5.1. Simulation Settings

The nodes are randomly distributed in the rectangular region with the size of 1000m*1000m. The communication radius R of unknown nodes and beacon nodes is 100m. The communication radius R_w of the wormhole attacker satisfies $R \leqslant R_w \leqslant 1.5R$. The distance D_w between a pair of wormhole attack nodes satisfies $D_w \geqslant 3R$. N_W, the number of wormhole attackers is 2. The total number N of the unknown nodes and the beacon nodes is 700. And the beacon node ratio $P_B = N_B/N = 10\%$ (N_B is the number of beacon nodes). Under the above conditions, make simulation experiments through changing some parameters. In order to eliminate the errors generated randomly, the simulation result is the average value of 100 results under the same conditions.

The computing method of the average localization error (E_A) is indicated as the formula (17).

$$E_A = \frac{\sqrt{(X_E - X_i)^2 - (Y_E - Y_j)^2}}{R} \tag{17}$$

Where (X_i,Y_i) is the actual location of the node; (X_E,Y_E) is the calculated position of the unknown node; R is the communication radius of unknown node. Use the average localization error to express the localization accuracy.

5.2. Simulation Results and Analysis

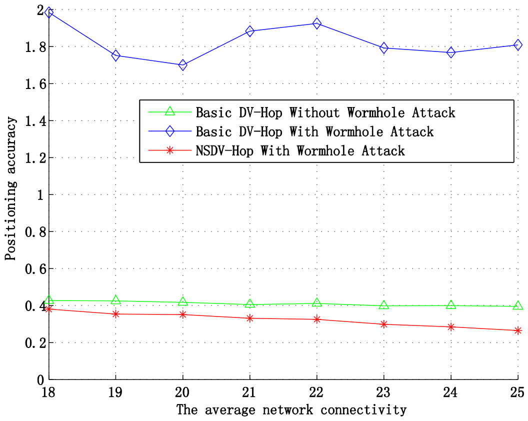


Figure 2. Localization Error for Varying Average Network Connectivity (rb=10%, Nw=2)

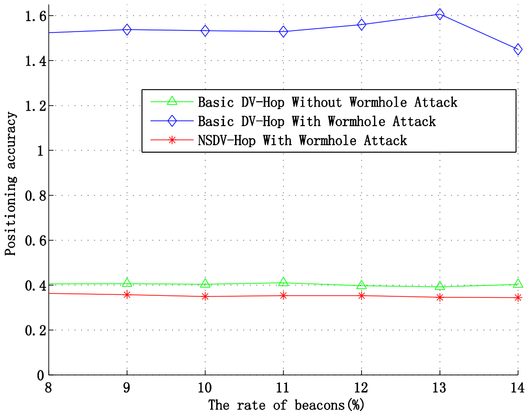


Figure 3. Localization Error for Varying Beacon Rate(N=700, Nw=2)

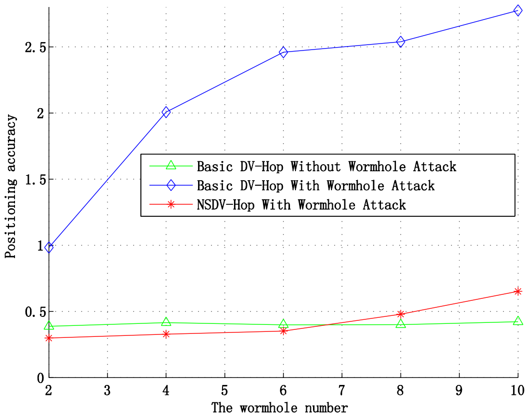


Figure 4. Localization Error for Varying Number of Wormhole Node (N=700, PB=15%)

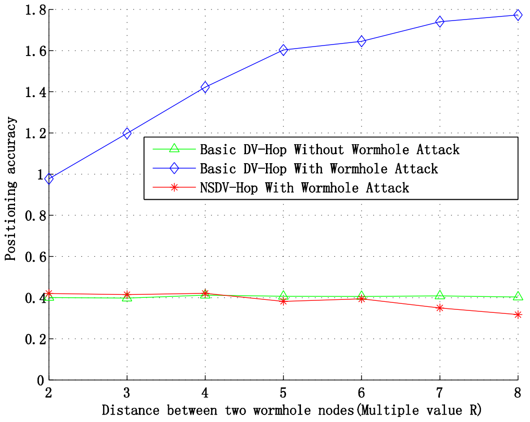


Figure 5. Localization Error for Varying DW(NW=2,PB=15%)

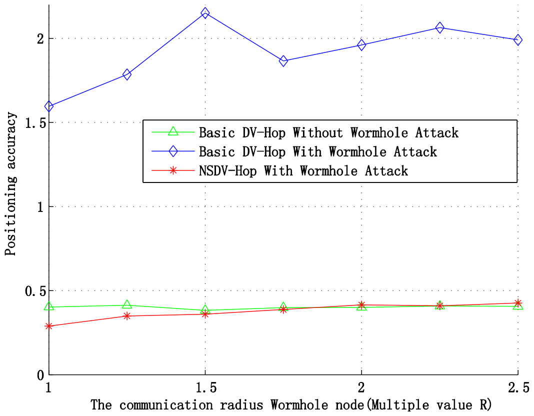


Figure 6. Localization error for Varying RW(NW=2,PB=15%)

As shown in Figure 2, the simulation results show when the average connectivity is more than 18, the DV-Hop localization error attacked by the wormhole is more than 1.5R, and after applying the NSDV-Hop method, location accuracy is better than DV-Hop algorithm accuracy not attacked by the wormhole, and with the increase in the average network connectivity, the localization accuracy increases.

As shown in Figure 3, the simulation results show that using the NSDV-Hop localization algorithm can overcome the influence of the wormhole attack under the condition of P_B changing, the location accuracy is better than DV-Hop algorithm not attacked by the wormhole, and with the increase in P_B, the location accuracy increases.

As shown in Figure 4, the simulation results show when there are various pairs of wormholes attacking nodes, the method NSDV-Hop also have a good effect. Under the experimental condition, when there are more than 6 wormhole nodes, the localization accuracy will decrease. In practical applications, with the increase in the area and the density of nodes, when there are more than 6 wormhole nodes, it will have very high localization accuracy.

As shown in Figure. 5, the simulation results show that the distance between wormhole attackers does not make NSDV-Hop algorithm fail. The longer the distance between wormhole attackers is, the better the localization accuracy will be.

As shown in Figure 6, the simulation results show that NSDV-Hop can achieve better results under different R_W circumstances. When $R_W \leq 2.5R$, it still can achieve similar localization accuracy to DV-Hop which is not attacked by the wormhole.

Through the above simulation data, it fully indicates NSDV-Hop algorithm is applicable to different parameters, and its localization accuracy in most occasions is better than DV-Hop not attacked, and the effect of using NSDV-Hop method to resist the wormhole attack is very good.

6. Conclusions and Future Work

In this paper, we analyzes the serious impact of wormhole attack on DV-Hop localization algorithm in WSN. In order to solve the problem of localization accuracy under wormhole attack, we proposes a NSDV-Hop algorithm based on neighboring nodes set to detect and defend against wormhole attack. The simulation results show that the NSDV-Hop algorithm can obtain satisfactory results in the change of the total number of nodes, the beacon node ratio, the number of wormhole nodes, the distance between the attackers and the communication radius of the wormhole nodes, etc. . It indicates that the NSDV-Hop algorithm is effective against the wormhole attack. In future work, we will extend to the detection and prevention of all forms of wormhole attacks and design the algorithm with better localization accuracy against wormhole attack.

References

[1] J. T. Wang, “A Study of Attacks Security Mechanisms in Wireless Sensor Network”, Proceedings of IEEE CCIS, **(2012)**.

[2] X. Y. Zhao, “The Security Problem in Wireless Sensor Networks”, Proceedings of IEEE CCIS, **(2012)**.

[3] T. He, C. Huang, B. M. Blum, J. A. Stanovic and T. Abedlzaher, “Range-free localization for larger scale sensor networks”, Proc 9th Annual Int’1 Conf on Mobile Computing and Networking (MobiCom), **(2003)**; San Diego,CA.

[2] K. Chen, Y. Zhou and J. H. He, “A Localization Scheme for Underwater Wireless Sensor Networks”, International Journal of Advanced Science and Technology, vol. 4, **(2009)**, pp. 9-16.

[4] D. Niculescu and B. Nath, “DV based positioning in ad hoc networks”, Journal of Telecommunication Systems, vol. 22, no. 1-4, **(2003)**, pp. 267-280

[5] H. Y. Chen and K. R. Sezaki, “An Improved DV-Hop Localization Algorithm with Reduced Node Location Error for Wireless Sensor Networks”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E91-A, **(2008)**, pp. 2232-2236.

[6] Y. Hu, A. Perrig and D. Johnson, “Packet leashes: A defense against wormhole attacks in wireless networks”, Twenty-Sencond Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM), **(2003)**; San Francisco, USA.

[7] Y. Hu, A. Perrig and D. B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, **(2006)**, pp.370-380.

[8] K. Kumar, M. A. Waheed and K. K. Basappa, “TCPL: A Defense against wormhole attacks in wireless sensor networks”, International Conference on Modeling, Optimization, and Computing (ICMOS), AIP Publishing, **(2010)**.

[9] L. Hu and D. Evans. "Using Directional Antennas to Prevent Wormhole Attacks", Proc. 11th Network and Distributed System Security Symposium (NDSS), **(2004)**.

[10] H. Ronghui, M. Guoqing and F. Lan, "WRL: a wormhole-resistent localization scheme based on DV-hop for wireless sensor networks", Proceedings of the 14th WSEAS international conference on Computers: part of the 14th WSEAS CSCC multiconference-Volume I, World Scientific and Engineering Academy and Society (WSEAS), **(2010)**.

[11] B. Triki, S. Rekhis and N. Boudriga, "Digital investigation of wormhole attacks in wireless sensor networks", Network Computing and Applications, NCA, Eighth IEEE International Symposium, IEEE, **(2009)**.

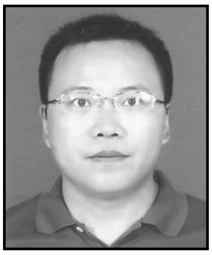
[12] R. Song, P. C Mason and M. Li, "Enhancement of frequency-based wormhole attack detection", Military Communications Conference, MILCOM, IEEE, **(2011)**.

[13] J. Wu, H. Chen and W, Lou, "Label-based DV-HOP localization against wormhole attacks in wireless sensor networks", Networking, Architecture and Storage (NAS), IEEE Fifth International Conference, IEEE, **(2010)**.

[14] J. H. Zheng, H. Y. Qian, J. G. Chen and J. Xu, "Unique-previous-node-based DV-Hop Localization Against Wormhole Attack for Wireless Sensor Networks", Journal of Information and Computational Science, vol. 12, no. 6, **(2015)**, pp. 2417–2428.

[15] J. H. Zheng, H. Y. Qian, D. M. Gao and X. Y. Yan, "Improved DV-Hop Positioning Algorithm Based on Modifying Hop Counts", Computer Science, vol. 40, no. 1, **(2013)**, pp.63-67

Authors



Jiuhu Zheng, male, he is a PhD student of school of computer science and engineering in Nanjing University of Science and Technology, lecturer, received the Master Degree in Software Engineering from Nanjing University in 2004. He engaged in the research wireless sensor networks and network security. He is a member of the China Computer Federation.

Huanyuan Qian, male, he is a professor of Nanjing University of Science and Technology, the executive director of Jiangsu Province Computer Users Association. He engaged in the research computer networks and information security.