Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, **2015,** *9,* **1443-1448** **1443**

Open Access

An Improved DV-Hop Algorithm for Resisting Wormhole Attack

Xiaoying Yang* and Qixiang Song

College of Information Engineering, Suzhou University, Suzhou, 234000, China

Abstract: As DV-Hop algorithm estimates distance by distance vector exchanging, positioning process is vulnerable to devastate wormhole attacking. An improved DV-Hop algorithm (AWADV-Hop) which resists wormhole attack is proposed, based on the original algorithm in this paper. To solve the problem that hops and the average distance per hop is the most vulnerable to wormhole attack in DV-Hop. This paper first fixes hop value by detecting the wormhole attack. Then, according to error comparison of the average distance per hop of anchor node and the average distance per hop of the whole network, locate permission of anchor nodes are re-decided. Average distance per hop of anchor nodes with positioning permissions is weighted to be the ultimate per hop distance of unknown node. Finally, simulated by MATLAB and simulation results show that this algorithm can effectively resist wormhole attack and improve the positioning accuracy.

Keywords: DV-hop algorithm, hops, location error, malicious nodes, wireless sensor networks, wormhole attack.

1. INTRODUCTION

Node localization is the prerequisite and basis for various applications in wireless sensor networks [1]. Scholars pay high attention to DV-Hop algorithm [2] as it has many advantages, such as without ranging, directional antenna is not required and have good positioning accuracy etc.. But its security is relatively poor, extremely vulnerable to devastate wormhole attack [3]. For wormhole attack detection and prevention, many scholars have proposed ways to solve. Such as in the study of literature [4-9]. These methods can effectively resist the wormhole attack in DV-Hop algorithm to some extent, but there are still issues such as positioning accuracy is not ideal. Based on previous work, through a detailed analysis of the wormhole attack in DV-Hop algorithm, an improved DV-Hop algorithm (AWADV-Hop algorithm) is presented both to resist wormhole attack and to improve the positioning accuracy in this paper.

2. RELATED WORK

2.1. Work Principle of DV-Hop

DV-Hop algorithm is proposed by Drago Niculescu, which is divided into three phases.

The first stage: calculate the minimum number of hops between nodes.

The second stage: calculate the average distance per hop of each anchor node. The formula is shown in Eq. (1).

$$\mathrm{h}opsize_i = \frac{\sum_{i\neq j}\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{\sum_{i\neq j} hop_{ij}} \quad (1)$$

(x_i, y_i) and (x_j, y_j) are coordinate positions of node i and node j, hop_{ij} is the minimum number of hops between the two nodes. Then use $\mathrm{hop} * \mathrm{hopsize}$ to obtain estimated distance between the nodes.

The third stage: use trilateration or maximum likelihood estimation method to calculate the unknown node coordinates.

2.2. Types of Wormhole Attack

Wormhole attack establishes a link without a communication range of each other, so make two long distance nodes as two adjacent nodes, resulting in greatly reduced positioning accuracy. Karlof proposed wormhole attack in safety route [10]. Hu Y C analyzed wormhole attacks in wireless sensor networks [4]. Lazos proposed that wormhole attack risk also exists in the DV-Hop algorithm [11]. Common types wormhole attack: First, the packet is tampered, which can be an effective defended by conventional cryptography mechanism. Second, High replay attack; Third, hide-band channel attacks. This paper aims to the third kind of attacks.

2.3. Analysis of Wormhole Attack in DV-Hop

As DV-Hop algorithm involves a number of hops between two nodes, if the wormhole connected formed by a band hidden channel, then hops will be reduced. Hops between nodes thereby greatly reduce, the average distance per hop of anchor nodes will increase, which have a great influence on the position of the last acquired.

Under normal circumstances, as shown in Fig. (**1a**), $\mathrm{hop}_{AB} = 2, \mathrm{hop}_{BC} = 5, \mathrm{hopsize}_B = (40+60)/(2+5) \approx 14.3$. if node P gets the average distance per hop from node B, The distance between it and the three anchor nodes respectively is $\mathrm{d}_{PA} = 14.3\times3 = 42.9, \mathrm{d}_{PB} = 14.3\times2 = 28.6, \mathrm{d}_{PC} = 14.3\times3 = 42.9$.

1874-110X/15 2015 Bentham Open

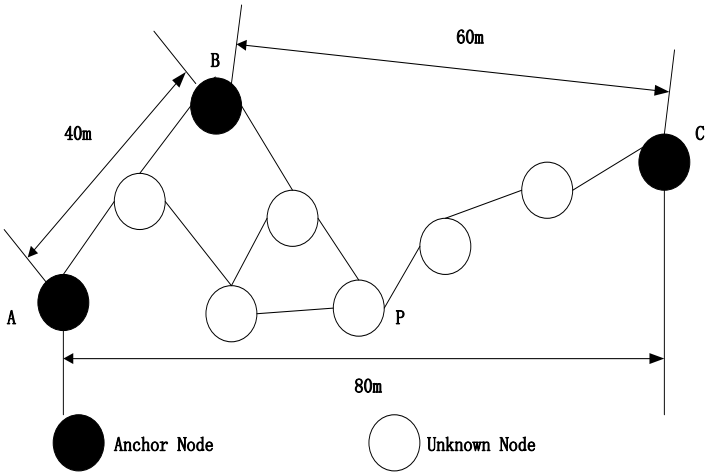

Fig. (1a). Normal DV-hop.

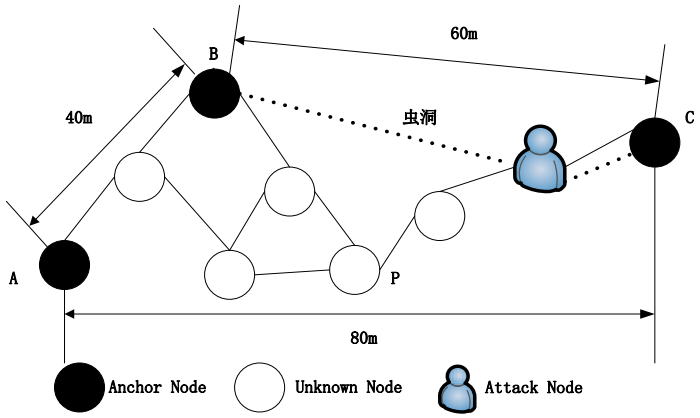

Fig. (1b). DV-Hop suffering wormhole attack.

Under the wormhole attack case, shown in Fig. (**1b**), $\mathrm{hop}_{AB} = 2, \mathrm{hop}_{BC} = 1, \mathrm{hopsize}_B = (40 + 60)/(2 + 1) \approx 33.3$, if node P gets the average distance per hop from node B, The distance between it and the three anchor nodes respectively is $d_{PA} = 33.3\times3 = 99.9, d_{PB} = 33.3\times2 = 66.6, d_{PC} = 33.3\times3 = 99.9$. It can be seen that, when there is wormhole attack in DV-Hop algorithm, it will significantly reduce the number of hops between nodes. The average distance per hop of the anchor node will increase, leading to a sharp increase in position error, which even cannot be located.

3. AWADV-HOP ALGORITHM RESISTS WORMHOLE ATTACK

For wormhole attack in DV-Hop algorithm, hops and jump distance is improved in the paper to effectively resist the wormhole attack and achieve safe location for nodes.

3.1. The Improvement of AWADV-Hop Algorithm

(1) Limit the maximum number of hops. When the network topology is irregular, the error of actual distance per hop increases with the number of hops becomes larger, deviation between the estimated distance of per hop and the actual distance of per hop is growing. Thus limiting the maximum number of spread hop (Mh)of data packets can both reduce network traffic and can reduce errors of distance per hop. According to the network size, proportion of the anchor node in the network as well as the network connectivity to set Mh value [12-14]. To ensure within the range Mh, there are anchor nodes around unknown nodes, Mh=4 is set in the paper.

(2) Hops improvements. In wireless sensor networks, the communication distance between nodes can't be greater than the maximum communication radius R, Thus use Eq. (2) to detect whether there is an wormhole attack between anchor nodes.

$$\frac{\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{\mathrm{hop}_{ij}} > R \tag{2}$$

If the Eq. (2) is tenable, there exists wormhole attack between nodes i and j. Then, directly use Eq. (3) to calculate the value of hop_{ij}' to replace hop_{ij}.

$$\mathrm{hop}_{ij}' = \left\lceil \frac{\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{R} \right\rceil + 1 \tag{3}$$

As shown in Fig. (**1b**), assuming the communication radius of each node are R = 20m. For anchor node B which

suffers wormhole attack, $\mathrm{hop_{BC}} = \lceil 60/20 \rceil + 1 = 4$ place$\mathrm{hop_{BC}} = 1$, thus, $\mathrm{hopsize_B} = (40 + 60)/(2 + 4) \approx 16.7$, which is relatively close to the average distance per hop without attack.

As for the unknown node, then use received hops of two anchor node hopA, hopB to determine whether there is wormhole attack by Eq. (4).

$$\frac{\sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}}{(hop_{A+} hop_B)} > R \tag{4}$$

If path of the two anchor nodes which through the node does not exist attack, then use the hops of the two nodes to detect hops from other anchor nodes. Once hopC which is attacked by the wormhole is detected, then use hopA and hopB , which are no wormhole attack, correct hop value by Eq. (5).

$$\mathrm{hop_c} = \left[\left(\left\lfloor \frac{\sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}}{R} \right\rfloor + 1\right) + \left(1 + \left\lfloor \frac{\sqrt{(x_A - x_C)^2 + (y_A - y_C)^2}}{R} \right\rfloor - \mathrm{hop_C}\right)\right] /2 \tag{5}$$

As shown in Fig. (**1b**), Eq. (5) to correct $\mathrm{hop_{PC}} = \frac{\left[\left(\left\lfloor \frac{60}{20} \right\rfloor + 1\right) + \left(1 + \left\lfloor \frac{80}{20} \right\rfloor - 3\right)\right]}{2} = 3$, which is the same as the hop which was not attacked, which effective against the impact of the wormhole attack on the hop count.

(3) Remove malicious nodes by distance per hop. Correcting the number of hops, to a certain extent, is effective against the wormhole attack, but there are still malicious nodes which cause distance per hop calculation error. Therefore, this paper further removes malicious nodes by distance per hop to reduce the impact of the wormhole attack on the location error.

Using hops which have been corrected to calculate average distance per hop (hopsize) of each anchor node by Eq. (1). As a correction, hopsize is broadcast in the network.

Unknown nodes collect all the correction information of anchor nodes within its communication range to establish the correction value set$(\mathrm{hopsize_1}, \cdots \mathrm{hopsize_m})$. Using Eq. (6) to calculate the average distance per hop(avghs) of the whole network. Then calculate error ε of average distance per hop (hopsize) of each anchor node and the average distance per hop(avghs) of the whole network.The formula is shown in Eq. (7). Setting upper limits ε_l and lower limits ε_h of the error. By determining the relationship between the error ε and the upper limit and lower limit is to correct the average distance per hop and location permissions of each anchor node.

$$\mathrm{avghs} = (\mathrm{hopsize_1} + \cdots + \mathrm{hopsize_m})/\mathrm{m} \tag{6}$$

$$\varepsilon_\mathrm{i} = |\mathrm{hopsize_i} - \mathrm{avghs}| \tag{7}$$

If$\varepsilon_i \le \varepsilon_l$, the anchor node is joined in positioning anchor node set. If $\varepsilon_l < \varepsilon_i \le \varepsilon_h$, using avghs replace their average distance per hop, then joins in positioning anchor node set. If $\varepsilon_i > \varepsilon_h$, the node may be malicious node, deprive locate permission of the node. Eventually forming the set of nodes for positioning $(1, \cdots, \mathrm{n})$. Different anchor nodes have different located affects on the unknown node. therefore, give a weight to each node in accordance with the Eq. (8). Calculate average distance per hop of the unknown nodes by Eq. (9).

$$\mathrm{w_i} = \frac{1/\mathrm{hop_i}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} 1/\mathrm{hop_i}} \tag{8}$$

$$\mathrm{hop} = \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{w_i} \times \mathrm{hopsize_i} \tag{9}$$

3.2. Positioning Process of AWADV-Hop Algorithm

Based on the above analysis, positioning process of AWADV-Hop algorithm which resists wormhole attack is described as below.

The first stage: Each anchor nodes broadcast data packets $\{\mathrm{id_i}, \mathrm{x_i}, \mathrm{y_i}, \mathrm{hop_i}, \mathrm{Mh}\}$ which contain the node label, coordinates positions. The minimum number of hops and restrictions on the maximum number of network hops to the network. The minimum number of hops is initialized to 0 and Mh = 5. After receiving this packet, $\mathrm{hop_i}$=$\mathrm{hop_i}$+1 in each neighbor node, judge whether $\mathrm{hop_i}$ is greater than Mh, if it is, the packet is discarded, otherwise it forwards the packet. If the node is an anchor node, using the data packet information to judge whether there is wormhole attack by Eq. (2). If there is wormhole attack, hop is corrected by using Eq. (3). Then the packet is saved into data sheet. Otherwise, the packet is saved directly. The unknown node uses Eq. (4) to detect the impact of the wormhole and Eq. (5) is used to correct the number of hops which is attacked if there is wormhole.

The second stage: After completion of the first stage, each anchor node uses Eq. (1) to calculate the average distance per hop. Then the data packet $\{\mathrm{id_i}, \mathrm{hopsize_i}, \mathrm{Mh}\}$ is broadcasted to the network, Mh is initialized to 0. When the node receives the data packet, makes $\mathrm{Mh} \leftarrow \mathrm{Mh} + 1$, then forwards it. When Mh> 5, the packet is discarded. Unknown node receives set of average distance per hop $(\mathrm{hopsize_1}, \cdots \mathrm{hopsize_m})$ of all-anchor nodes within communication range. It then calculates the average distance per hop of the whole network and the error ε of the average distance per hop of anchor nodes and the average per hop of the whole network. Reassign positioning permissions of the anchor node by judge ε, revoke positioning permissions of anchor nodes which exists wormhole attack. Correct the average distance per hop of part of the anchor nodes and generate a new set of anchor nodes. Using Eq. (9) to obtain final average distance per hop of unknown node, the estimated distance between nodes is obtained by hops multiplied by the average distance per hop.

The third stage: the same as the DV-Hop algorithm.

4. SIMULATION

In order to verify the positioning performance and validity of resisting wormhole attack of AWADV-Hop localization algorithm, MATLAB7.0 simulation platform is used to simulate AWADV-Hop localization algorithm and DV-Hop localization algorithm. The performance of the proposed algorithm is measured in two ways which are the average location error and traffic. The average location error is defined as [15-20]:

$$\mathrm{Aerr} = \frac{\sqrt{(x_t - x_e)^2 + (y_t - y_e)^2}}{\mathrm{R}} \times 100\% \tag{10}$$

where (x_t, y_t), (x_t, y_t), R respectively, is the true coordinate position and the estimation coordinate position of node and its communication radius.

The experimental area is 300m × 300m of randomly deployed 500 sensor nodes. Initialize the network node distribution which is shown in Fig. (**2**). The maximum propagation network hops is set to 5. According to the literature [10], when the values of error ε of the average distance per hop of anchor nodes and the average distance per hop of the whole network in [0.08avghs, 0.2avghs] range, not only can remove the malicious nodes, but also can ensure positioning accuracy requirements of the algorithm [21, 22]. Therefore, this paper set upper limit ε_l and lower limit ε_h value of 0.08avghs and 0.2avghs. Wormhole link length is 50m.

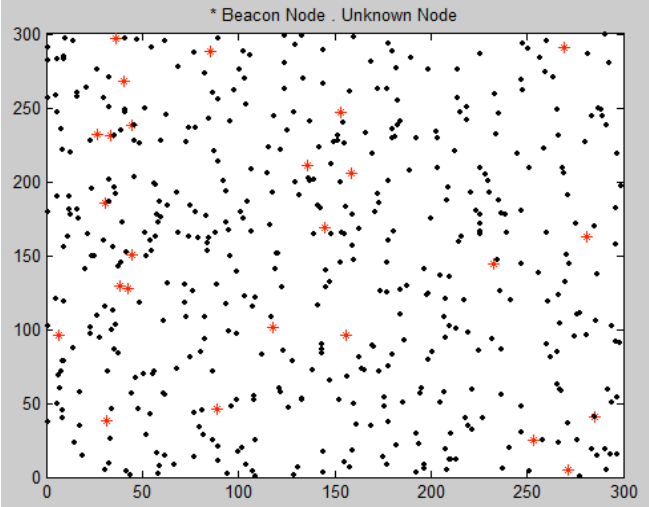

Fig. (2). Distribution network.

4.1. Simulation 1

Proportion of anchor nodes from 5% to 50%, communication radius of node is 20m, no wormhole attack, wormhole link number is 10, comparison of the average location error of two algorithms. The simulation results are shown in Figs. (**3** and **4**).

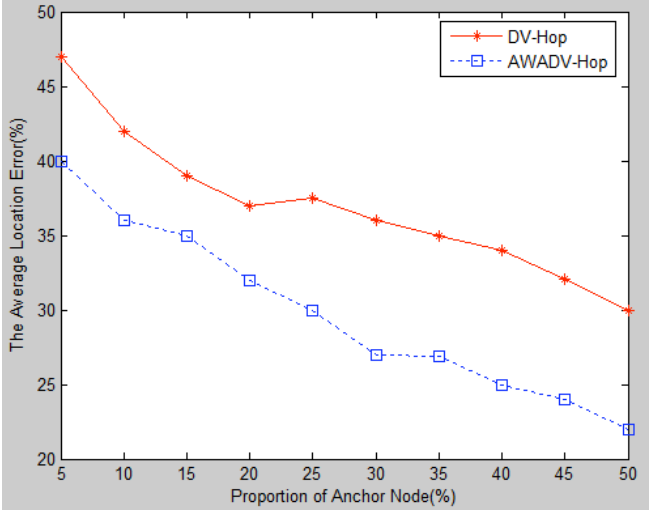

Fig. (3). The average location error without wormhole attack.

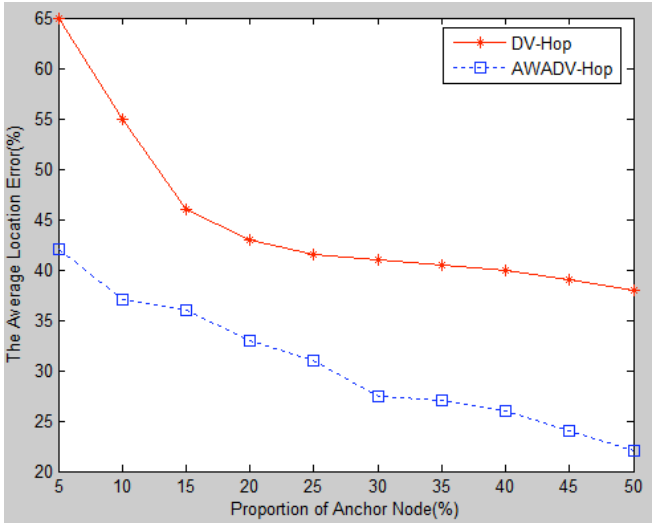

Fig. (4). The average location error with wormhole attack.

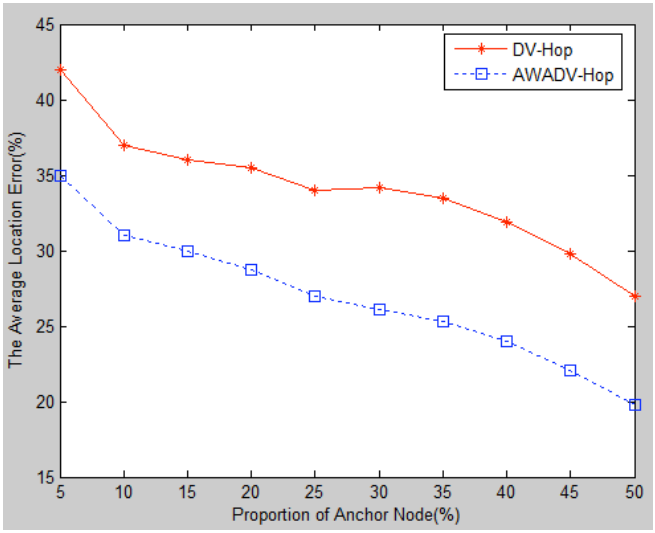

Fig. (5). The average location error without wormhole attack.

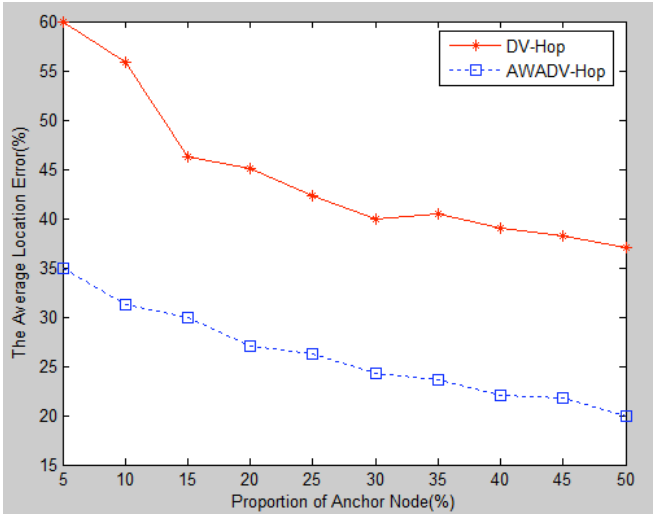

Fig. (6). The average location error with wormhole attack.

Proportion of anchor nodes from 5% to 50%, communication radius of node is 40m, no wormhole attack, wormhole link number is 10. Comparison of the average location error

of two algorithms. The simulation results are shown in Figs. (**5** and **6**).

As can be seen from the simulation results which are shown in Figs. (**3-6**), in the case of non-attack, with an increase in the proportion of beacon nodes, connectivity of the network continuously increases. The number of the nodes involved in the positioning beacon increases. The positioning accuracy increases accordingly. Thus positioning errors of DV-Hop algorithm and AWADV-Hop algorithm are reduced, because average distance per hop of unknown nodes is weighted in AWADV-Hop algorithm. Thus it is closer to the actual distance of each hop. Positioning error is smaller than DV-Hop algorithm and has more stable and smooth curves.

In the situation with the wormhole attack, DV-Hop algorithm has no way to resist, thus localization error of node is far greater than the normal level. When wormhole attack occurs, the number of hops is corrected and the average distance per hop of wormhole anchor node is instead by the average distance per hop of the whole network in AWADV-Hop algorithm. In addition, remove positioning permissions of wormhole anchor node with larger error and the average distance per hop of unknown node is weighted. Thus it is more close to the actual distance of each hop, and thus improves the positioning accuracy of the algorithm. The error is close to the normal level, and the curve is not volatile. All of these prove that AWADV-Hop algorithm has high stability and strong anti-attack capability in the face of a wormhole attack.

4.2. Simulation 2

The ratio of anchor node is 20%. The communication radius is 20m and wormhole link count is incremented sequentially from 5 to 50. Compare the traffic of the two algorithms. The simulation result is shown in Fig. (**7**).

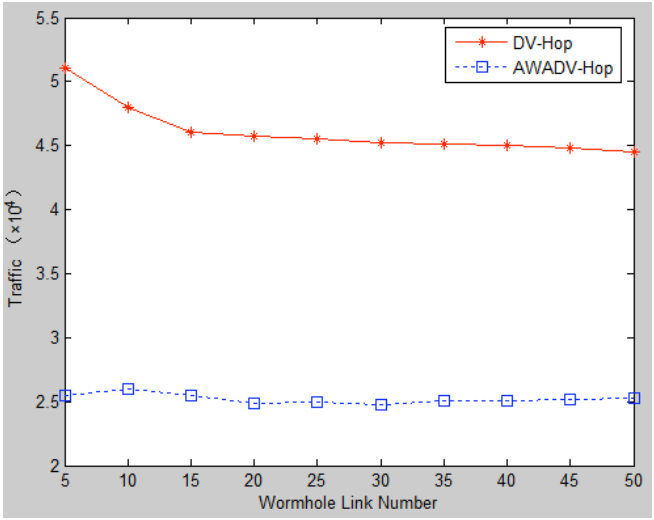

Fig. (7). Comparison of traffic of wormhole link with changing.

Traffic is counted by node broadcast information. The node broadcast for each time, the traffic is increased by one. As can be seen from Fig. 7, in the circumstances that the ratio of anchor nodes and node communication radius is certain, with the increase in the number wormhole link, traffic volume which DV-Hop algorithm and AWADV-Hop algorithm need is decreasing constantly. AWADV-Hop algorithm limits the maximum number of hops of data packet broadcasting, reduces the probability of packet delivery may occur during conflict or collision, which greatly reduces the traffic brought by resending data packets, so in the same conditions next, the traffic is much smaller than the DV-Hop algorithm.

CONCLUSION

For the problem that DV-Hop algorithm is vulnerable to the wormhole attack, the number of hops is used to detect wormhole attacks and attacked hops are corrected in this paper. Positioning permission of malicious anchor nodes are excluded through the error of the average distance per hop of anchor nodes and the average distance per hop of the whole network in the second stage of positioning. Then correct the larger error of the average distance per hop of anchor nodes. Finally, the average distance per hop of unknown nodes are weighted. Simulation results show that AWADV-HOP algorithm can effectively resist the wormhole attack and AWADV-HOP algorithm accuracy has been greatly improved and has better stability. The future work is to make DV-Hop algorithm wormhole attack has better resistance and a higher positioning accuracy to meet the needs of positioning.

CONFLICT OF INTEREST

Financial contributions and any potential conflict of interest must be clearly acknowledged under the heading ‘Conflict of Interest’. Authors must list the source(s) of funding for the study. This should be done for each author.

ACKNOWLEDGEMENTS

The study of our work is supported in part by Young Talents Fund Project in Anhui Province of China (No. 2013SQRL083ZD), Anhui University Provincial Natural Science Research Project (No.KJ2014A247) and Open platform topics of Suzhou University of China (No. 2012YKF38, No.2011YKF10).

REFERENCES

[1] W. Xinsheng, Z. Yanjin, and L. H. Tao, “Improved study based on DV-hop localization algorithm”, *Computer Science*, vol. 38, no. 2, pp. 76-78, 2011.

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

[3] C. Xiaomei, Y. Bo, and C. Guihai, “Safety analysis of sensor network node positioning system” *Journal of Software* vol. 19, no. 4, pp. 879-887, 2008.

[4] Y. C. Hu, A. Perrig, and D. B. Johnson, “Wormhole aRacks inwireless net-works”, *IEEE Joumal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370-380, 2006.

[5] L. Buttyrn, L. Dora, and I. Vajda, “Statistical wormhole detection in sensor networks”, *Lecture Notes in Computer Science*, vol. 3813, pp. 128-141, 2005.

[6] Z. Q. Ming, and H. Yong, “Simulation and approach todefend of wormhole attack in DV-Hop algorithm”, *Computer Engineering and Applications*, vol. 46, no. 14, pp. 88-90, 2010.

[7] L. Zhen, L. Zhen-Yang, and Z. Xiao-Hong, “Effective defense method for wormhole attack”, *Computer Systems and Applications*, vol. 21, no. 7, pp. 203-207, 2012.

[8] Y. Xiang, L. Chaoze, and W. Wei, "DV-HOP secure positioning algorithm for wormhole attack resistance", *Computer Applications and Software*, vol. 30, no. 5, pp. 188-192, 2013.

[9] L. Caixia, and H. Tinglei, "Research on improved DV-hop algorithm in WSN against wormhole attack", *Chinese Journal of Sensors and Actuators*, vol. 24, no. 10, pp. 221-225, 2011.

[10] C. Karlof, and D. Wagner, "Secure Routing in sensor networks: Attacks andcountermeasures", In: *1st IEEE International Workshop on Sensor Network Protocol and Applications*, ANCHORAGE, AC, USA, 2003.

[11] L. Lazos, and R. Poovendran, "SeRLoc: Secure range independent localization for wireless sensor networks", In: *Proceedings of ACM Workshop on Wireless Security (ACM Wise ′ 04)*, Philadelphia, PA, 2004.

[12] Z. Yan-hang, Q. Zhi-hong, S. Xiao-hang, and C. Chao, "PSO localization algorithm for WSN nodes based on modifying average hop distances", *Journal on Communications*, vol. 34, no. 9, pp. 105-114, 2013.

[13] W. Junfeng, C. Honglong, W. Lou, and Z. Wang, "Label-based DV-hop localization against wormhole attacks in wireless sensor networks", In: *IEEE 5th International Conference on Networking, Architecture and Storage (NAS)*, MACAU, 2010.

[14] H. Chen, W. Lou, and Z. Wang, "A consistency-based secure localization scheme against wormhole attacks in WSNs", In: *Proceedings of the International Conference on Wireless Algorithms, Systems and Applications (WASA)*, Bosten, MA, USA, 2009.

[15] H. Chen, W. Lou, X. Sun, and Z. Wang. "A secure localization approach against wormhole attacks using distance consistency", In: *Eurasip Journal on Wireless Communications and Networking, Special Issue on Wireless Network Algorithms, Systems, and Applications*, 2009.

[16] H. Chen, W. Lou, and Z. Wang, "Conflicting-set-based wormhole attack resistant localization in wireless sensor networks", In: *Proceedings of 6th International Conference on Ubiquitous Intelligence and Computing (UIC)*, 2009.

[17] D. Dezun, L. Mo, and Y. Liu, "Connectivity-based wormhole detection in ubiquitous sensor networks", *Journal of information science and engineering*, vol. 27, pp. 65-78, 2011.

[18] D. Dezun, L. Mo, and L. Yunhao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks", *IEEE/ACM Transactions on Networking*, vol. 19, no. 6, pp. 1787-1796, 2011.

[19] J. Wu, H. Chen, W. Lou, and Z. Wang, "Label-based DV-Hop localization against wormhole attacks in wireless sensor networks", In: *Proceedings of 2010 IEEE International Conference on Networking, Architecture and Storage*, 2010.

[20] D. Dong, M. Li, Y. Liu, and X. -Y. Li, "Topological detection on wormholes in wireless ad hoc and sensor networks", In: *Proceedings of International Conference on Network Protocols*, 2009.

[21] K. –L. Hui, W. Hui, and W. T. Yue, "Information security outsourcing with system interdependency and mandatory security requirement", *Journal of Management Information Systems*, vol. 29, no. 3, pp. 117-155, 2012.

[22] G. Liu, and L. J. Hong, "Kernel estimation of the greeks for options with discontinuous payoffs", *Operations Research* vol. 59, no. 1, pp. 96-108, 2011.

Received: February 17, 2015 Revised: May 21, 2015 Accepted: June 09, 2015