Dealing with Wormhole Attacks in Wireless Sensor Networks Through Discovering Separate Routes Between Nodes

Farzad Rezaei
Department of Computer Engineering, College of Technical and Engineering, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran.
farzad_65sh@yahoo.com

Abdolhamid Zahedi
Department of Electrical Engineering
Kermanshah University of Technology
Kermanshah, Iran
Zahedi@Kut.ac.ir

***Abstract*—One of the most common attacks against Wireless Sensor Networks is the wormhole attack. In this attack, the enemy deploys two malicious nodes in two different areas of the network and establishes a high-speed dedicated channel between these two. This will cause the normal nodes in two different areas wrongly think that they are two-hop neighbors. Therefore, this attack will greatly affect the routing algorithms. In this paper, a new distributed algorithm is provided to deal with the wormhole attack. The main idea of the proposed algorithm is to discover separate routes between pairs of two-hop neighboring nodes. The proposed algorithm was implemented and evaluated in terms of true and false detection rate by performing a series of experiments and the results were compared with the base algorithm. The test results showed that the proposed algorithm has desirable efficacy.**

Keywords-wireless sensor networks; security; wormhole attack

I. INTRODUCTION

Today, wireless sensor networks have an increasing application in military, environment, urban services, discoveries and monitoring fields. Since, sensor nodes have very limited computational, memory and radio capabilities, and according to the application of such networks in critical regions especially military, establishing security in such networks is very essential and has attracted the attention of many researchers [1-3]. One of the most dangerous known attacks against such networks is wormhole attack [4]. In this attack, as shown in Figure 1, the enemy deploys two malicious nodes in the network and establishes a high-speed dedicated communication channel between these two nodes. These two nodes receive messages from a part of network from a low latency link and relay them in another part of the network. Thus, this attack greatly affects the routing algorithms [5].

Many algorithms have been provided to cope with this attack in wireless sensor networks until now. In [5], an algorithm is proposed based on probability distribution of the number of neighboring nodes called WAPN to cope with wormhole attacks. This algorithm requires no special hardware and simply attempt to identify the wormhole attack according to the number of neighbors. One of the well-known algorithms benefiting from beacon nodes to detect the wormhole attack is provided in [6]. In this algorithm, in addition to the conventional sensors, a number of beacon nodes are released in the network constantly. These beacon nodes are aware of their location and detect the wormhole attack by sending a series of probe messages for each other. Since the wormhole attack causes these probe messages reach other beacon nodes with fewer steps, so beacon nodes use this to detect the wormhole attack. In [7], a general mechanism called packet leashes is proposed to cope with wormhole attack. A leash is in fact any type of information added to a packet to limit the allowed maximum transmission distance of packet. Two types of geographical and temporal leashes are introduced in this study. A geographical leash ensures that the packet receiver is in a determined distance from the transmitter. A temporal leash ensures that the packet has an upper bound on its' lifetime which limits the maximum moving distance, because the packet can move at a maximum speed of light. These two types of leashes ware used in [8] to provide a protocol to cope with wormhole attack. In [9], the impacts of wormhole attack on localization protocols based on DV-Hop have been analyzed. Also, a safe localization protocol based on label has been provided. The main idea of this protocol is to produce a list of quasi-neighbors for each beacon node and use all lists of quasi-neighbors receiving from neighboring beacon nodes to categorize all attacked nodes in a different group and then label all neighboring nodes (including all sensors and beacons). Based on the labels of neighboring nodes, each node will prevent from communication with its neighbors treated by wormhole attack. In [10], an algorithm based on another beacon called WRL was presented. WRL is a localization algorithm resistant to the wormhole attack benefiting from DV-Hop methods. In [11] a group-based expansion has been provided to cope with wormhole attack. In this method, sensor nodes are spread in the environment in group form and they are aware of the location of their group. During the establishment of the route, the location of group between sensors is exchanged and a link between two sensor nodes is created only when the location distance of the group of these two nodes are

close enough. In [12], a clustering-based mechanism is proposed to cope with wormhole attack. In this algorithm, a series of beacon nodes is used between clusters in order to detect the wormhole attack. In [13, 14] additional algorithms are provided to deal with wormhole attack which uses the connection information to search for forbidden infrastructures in the connection graph. These algorithms are completely local and require no special hardware. In [15], a lightweight IDS (Intrusion Detection System) framework called LIDeA has been proposed to cope with wormhole attack. In this system, the nodes hear the communication of their neighboring nodes and cooperate with each of them for successful infusion detection [16]. In [17], a secure routing protocol called SeRWA has been provided to cope with wormhole attack. This algorithm also requires no specialized hardware such as directional antennas. This protocol takes advantage of discovering single-hop neighbors and also the original route to cope with this attack. In [18] also another algorithm has been presented which benefits from local and neighborhood information to detect the wormhole attack. This algorithm uses the message broadcasting to two-hop neighbors through special single-hop neighbors to detect the wormhole attack.

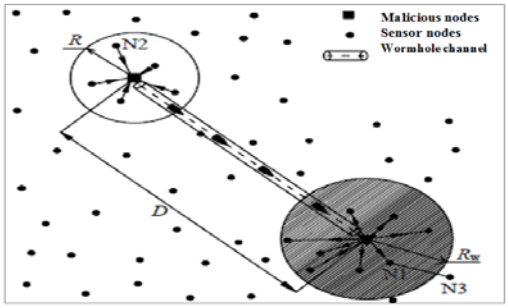

Fig. 1. Wormhole attack model

In this article, a new distributed algorithm is presented to deal with the wormhole attack in order to solve the disadvantages of previous algorithms desirably. The main idea of the proposed algorithm is to discover separate paths between pairs of nodes. For instance, as shown in Figure 1, the existence of wormhole attack causes the N1 and N2 nodes wrongly think that they are neighbors, while these two nodes are much far from each other and they are real neighbors. In the proposed algorithm, node N1 can realize occurring of a wormhole attack between itself and node N2 which appears to be neighbor by discovering all separate routes with maximum stride length α (e.g. 2 or 3) between them. As there is only one path with maximum stride length 3 between these two nodes. This is while if these two nodes were real neighbors, then there would be more separate routes (depending on the destination of the network) between them. Thus, the proposed algorithm can easily estimate the possibility of wormhole attack and its' occurring location in the network with great accuracy.

II. SYSTEM ASSUMPTIONS

- A sensor network contains n sensor nodes which are randomly distributed in a two-dimensional region.
- The network is homogenous.
- After expansion in the network environment, the nodes remain constant in terms of location status.
- Each node has a unique identifier and not aware of their location status which means they don't need GPS.
- Radio range of nodes is constant and identical.
- Each node is aware of approximate density of the network or the average of the number of single-hop neighbors, d.
- The nodes communicate with each other via wireless radio channel and use broadcasting by Omni-directional method.
- It is also assumed that the sensor network is expanded in a hostile environment. So, the network is insecure and the enemy can start the wormhole attack.
- The two nodes setting up the wormhole attack are called malicious enemy nodes.

III. THE PROPOSED ALGORITHM

The main idea of the proposed algorithm is to discover separate paths between each pairs of nodes u and v to detect the wormhole attack. Since the existence of wormhole attack causes the two legal nodes u and v, which are far from each other, to consider to be two-hop neighbors, so there would be only one unique route with stride length of 2 or even 3 between these two legal nodes. Hence, the wormhole attack can be detected by discovering separate routes between these two nodes. The proposed algorithm is made of three phases of 1: discovering single-hop neighbors, 2: discovering two-hop neighbors and 3: discovering separate routes which will be described in continue.

A. Discovering single-hop neighbors

After expansion of nodes in environment, each u node releases a "Hello" message. All nodes located in radio range u will receive its' Hello message and consider the u node as their single-hop neighbor. The first phase is carried out simultaneously by all nodes in the network.

B. Discovering two-hop neighbors

After the phase of discovering one-hop and two-hop neighbors, the third phase is implemented. As mentioned earlier, the wormhole attack in a specific area of the network causes the number of two-hop neighbors of legal nodes located in that region become much more than normal. Thus, in this phase, if each u node find that the number of two-hop neighbors is more than the threshold T_1, it will doubt to the existence of a wormhole attack in its' neighborhood and consequently, it runs the third phase. The threshold $T_1=\beta \cdot d$ is set up. The parameter $\beta$is a constant value larger than 1. In this status, the u node send a route discovery message for v destination to its' one-hop neighbors per each v existing in its' two-hop-neighbor so that to discover the possible routes to v node. Figure 2 has indicated the form of discovery packets. In source field, there is the ID of each source or the same node producing the packet of route generation, in destination field,

there is the ID of destination node or the same node of two-hop neighbor, in intermediate field, there is the ID of intermediate nodes from source to destination route and the lifetime is in TTL field.

The u node produce and publish a route generation packet with <<u,v,{},2>> value. Each W node receiving this message, first reduce a unit from TTL, add its' ID in intermediate part and then publish the packet. But if TTL is equal to zero, the W node ignores the received packet. The v node returns a confirmation message (containing the ID of intermediate nodes) with TTL=2 per each received route discovery packet to reach the u source node. If the source node receive only one separated confirmation message with completely different intermediate, it will add a unit to its' counter field. The u node repeats this process per all its' two-hop neighbors. After that, if the u node find its' counter value higher than the threshold T_2, it will realize that a wormhole attack is set up in its' neighborhood. Hence, it will release a warning message in the network and turn off its' radio and stop its' operation. The value of the threshold $T_2=d-a$ will be calculated; $0\leq a<d$ will be set up.

IV. SIMULATION RESULTS

The proposed algorithm has been implemented by the C ++ language. Then, its efficiency was evaluated by performing several tests in form of true and false detection rates. Also, the efficacy of the proposed method has been compared with the base algorithm [5].

- True detection rate: a percentage of legal nodes is the neighbor of malicious nodes of wormhole attack which have succeed to detect an attack in their neighborhood.
- False detection rate: a percentage of legal nodes that have wrongly detected a wormhole attack in their neighborhood.

In tests implementation, the network contains n nodes distributed randomly in an area of 1000 x 1000 m. The radio range of nodes is set to R=40 m. The proposed algorithm has been implemented by the C ++ language. Then, its' efficiency was evaluated by performing several tests in form of true and false detection rates. Also, the efficacy of the proposed method has been compared with the base algorithm [5].

- True detection rate: a percentage of legal nodes is the neighbor of malicious nodes of wormhole attack which have succeed to detect an attack in their neighborhood.
- False detection rate: a percentage of legal nodes that have wrongly detected a wormhole attack in their neighborhood.

In tests implementation, the network contains n nodes distributed randomly in an area of 1000 x 1000 m. The radio range of nodes is set to R=40 m. The parameter β=2 and α=0~5 are set. Each test has been repeated 500 times and the final results is obtained from the average of the results of this 500 iterations. It is assumed that there is a wormhole attack in the network so that the distance of its' two malicious nodes is 500 m from each other.

A. First test

In this test, we want to evaluate the efficacy of the proposed algorithm per change in the parameter α. In this test, we will have n=2000 in the network and the parameter α=0~5 has changed. The result of this test is given in figure 3 in form of true and false detection rates. The results of this test show that the threshold T2 is reduced. Consequently, if a legal node has less two-hop neighbors and has discovered only one separate route to them, it reports the wormhole attack with lower value for counter. This will increase both criteria. As can be seen from the results of this test, a suitable value for this parameter is α=1 which leads to true detection rate of 95% and false detection rate of 7%.

B. Second test

This test aims to evaluate the parameter n on efficacy of the proposed algorithm and compare the results with algorithm [5]. In this test, the parameters α=1 and n=500~3000 have been changed. Figure 4 has indicated the results of this test in form of respectively true and false detection rates. The results of this test show that the true detection rate of both algorithms is increased by increasing the number of nodes in the network. Because, by increasing this parameter, there would be the possibility of increasing the number of legal nodes neighboring malicious nodes. As a result, the detection rate will be increased. However, the false detection rate of the proposed algorithm is a bit higher than the base algorithm, but it is tolerable compared with the improvement rate obtained in true detection rate.

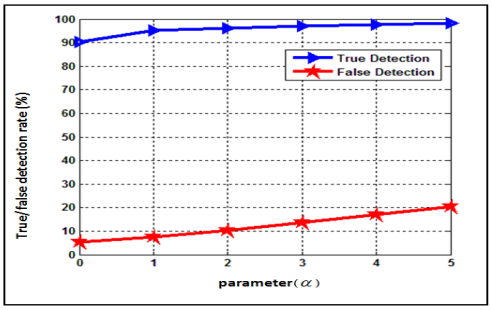

Fig. 2. The effect of parameter on efficacy of the proposed algorithm (n=2000)

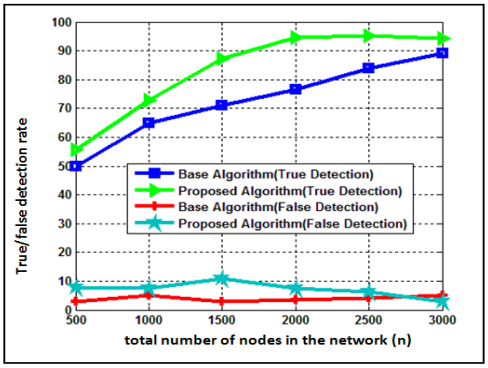

Fig. 3. The impact of n parameter on efficacy of the proposed algorithm (a=1) and comparing with the base algorithm

V. CONCLUSION

In this paper, a new distributed algorithm was proposed to deal with the wormhole attack. The main idea of the proposed algorithm was to discover separate routes between pairs of two-hop neighboring nodes. The proposed algorithm was implemented and evaluated by a series of tests for its efficacy in terms of true and false detection rates and the results were compared with WAPN algorithm. Test results showed that the proposed algorithm offers superior performance.

REFERENCES

[1] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey", Computer Networks, Vol. 52, No. 12, pp. 2292-2330, 2008

[2] A. J. Goldsmith, S. B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks", IEEE Wireless Communications, Vol. 9, No. 4, pp. 8-27, 2002

[3] I. F. Akyildiz, I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges", Ad Hoc Networks,Vol. 2, No. 4, pp. 351-367, 2004

[4] K. Sharma, M. K. Ghose, D. Kumar, R. P. K. Singh, V. K. Pandey, "A comparative study of various security approaches used in wireless sensor networks", International Journal of Advanced Science and Technology, Vol. 17, No. 2, pp. 31-44, 2010

[5] F. R. Kong, C. W. Li, Q. Q. Ding, G. Z. Cui, B. Y. Cui, "WAPN: a distributed wormhole attack detection approach for wireless sensor networks", Journal of Zhejiang University Science A, Vol. 2, No. 4, pp. 279-289, 2009

[6] H. Ronghui, M. Guoqing, W. Chunlei, F. Lan, "Detecting and locating wormhole attacks in wireless sensor networks using beacon nodes" World Academy of Science, Engineering and Technology, Vol. 55, No. 31, pp. 10-15, 2009

[7] Y. C. Hu, A. Perrig, D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM 2003", 22nd Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, Vol. 3, No. 1, pp. 1976-1986, 2003

[8] J. Wu, H. Chen, W. Lou, Z. Wang, Z. Wang, "Label-based DV-HOP localization against wormhole attacks in wireless sensor networks", 2010 IEEE Fifth International Conference on Networking, Architecture and Storage (NAS), China, July 15-17, 2010.

[9] L. Buttyán, L. Dóra, I. Vajda, "Statistical wormhole detection in sensor networks", European Workshop on Security in Ad-hoc and Sensor Networks, pp. 128-141, 2005

[10] H. Ronghui, M. Guoqing, F. Lan, K. Chunguang, L. Li, "WRL: a wormhole-resistent localization scheme based on DV-hop for wireless sensor networks", 14th WSEAS International Conference on Computers, Corfu Island, Greece July 23-25, 2010

[11] G. H. Lai, C. S. Ouyang, C. M. Chen, "A Group-Based Deployment for Wormhole Prevention in Sensor Networks", Journal of Information Science & Engineering, Vol. 27, No. 1, pp. 79-93, 2011

[12] D. B. Roy, R. Chaki, N. Chaki, "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks", arXiv preprint arXiv, 2010.

[13] R. Maheshwari, J. Gao, S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information", IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications, Spain, May 6-12, 2007

[14] D. Dong, M. Li, Y. Liu, X. Liao, "Connectivity-Based Wormhole Detection in Ubiquitous Sensor Networks", Journal of Information Science & Engineering, Vol. 27, No. 1, pp. 65-78, 2011

[15] T. Giannetsos, T. Dimitriou, N. P. Prasad, "State of the art on defenses against wormhole attacks in wireless sensor networks", IEEE 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, Wireless VITAE 2009, Denmark, May 17-20, 2009

[16] I. Krontiris, T. Giannetsos, T. Dimitriou, "LIDeA: a distributed lightweight intrusion detection architecture for sensor networks", 4th International Conference on Security and Privacy in Communication Networks ACM, Turkey, September 22 - 25, 2008

[17] S. Madria, J. Yin, "SeRWA: A secure routing protocol against wormhole attacks in sensor networks", Ad Hoc Networks, Vol. 7, No. 6, pp. 1051-1063, 2009

[18] W. Znaidi, M. Minier, J. P. Babau, "Detecting wormhole attacks in wireless networks using local neighborhood information", IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, France, September 15-18, 2008