DETECTING WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS USING HOP COUNT ANALYSIS

Lan Yao, Zhibin Zhao and Ge Yu

School of Information Science and Engineering

Northeastern University, Shenyang

Liaoning, China

Emails: {yaolan, zhaozhibin, yuge}@mail.neu.edu.cn

Submitted: Nov. 05, 2012 ***Accepted: Jan. 20, 2013*** ***Published: Feb. 20, 2013***

Abstract- The wormhole attack is a severe threat to wireless sensor networks. Most existing countermeasures for detecting and locating wormhole links either require extra hardware or are too complex for the inherently capability-constrained sensor nodes. Actually, wormhole links can enormously change the original sensor network topology. In this paper, we introduce the HCA4DW mechanism for detecting and locating wormholes in wireless sensor networks. It is based on the basic idea that the change of topology can be detected through neighborhood validation. We discover the maximum necessary hop count between the sensors in the same neighbor set for neighborhood validation. We describe the detail procedure of HCA4DW in this paper and test the performance of the HCA4DW mechanism rigorously through simulative experiments.

Index terms*: wireless sensor networks, wormhole attack, hop count, neighborhood validation.*

I. INTRODUCTION

The concept of a wormhole is originally suggested in physics. In a 2-dimention space, wormhole points will twist its surface, and form a shortcut through the space. The wormhole attack in wireless sensor networks is a severe threat to security. A trip through the wormhole link could take less time or have a better QoS than that through normal links. Therefore, the wormhole links will absorb most of the transmission, and perform selective forwarding or information theft. Many countermeasures have been proposed in the literature to track and defend wormhole attacks. Generally, the exiting methods are highly dependent on the extra hardware, or with high calculation complexity. It makes them unsuitable for the inherently capability-constrained sensor nodes and large-scale deployments.

We aim to detect and locate wormholes without using any extra hardware or excessively complexity. In this paper, we propose the HCA4DW mechanism which is based on hop count analysis to detect and locate wormholes in wireless sensor networks. The main idea is that the initial topology will be changed if wormhole nodes are introduced into the network. It will be reflected by the change of the neighbor relationship. We discover the mapping between the deployment density of sensor nodes, the communication radius and the maximum necessary hop count among the neighbors. With this maximum necessary hop count, we can validate the neighborhood as well as the change of topology.

II. RELATED WORKS

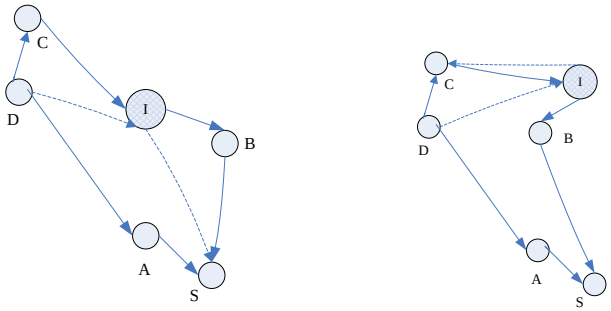
Wireless Sensor Networks (WSNs) have been used in a wide-range of applications, including environmental monitoring, object tracking, health monitoring, and military systems [1][2]. With the wide applications of WSNs, the security of WSNs becomes more and more important. Reliable and secure data collection is an important task in a sensor network. The security of the routing protocol directly influences the security and reliability of the WSNs. It's the most important element in the research of secure WSNs. However, the security of WSN which needs to be revised from practical angles [3] is facing great challenge, because a WSN consists of a large number of unattended sensors with limited storage, battery power, computation, and

communication capabilities, where battery power (or energy) is the most crucial resource for sensor nodes [4]. Moreover, it has dynamic topology, open network environment and limited energy. Malicious nodes can easily monitor, intercept or tamper data packets flowing in WSN. Communications can not be established because of the attack to routing information, which would affect the network performance seriously and even collapse the entire network. Past researches on sensor network routing have been focused on reliability, efficiency and effectiveness of data dissemination. Few of them considered security issue during the protocol design time. How to create secure routing for WSN has become the most important issue in the study of security in WSN.

The defined attacks to routing include [5]:

(1) Spoofing

In Fig. 1 (a), a malicious node *I* modifies the routing rules in node *C*, which makes *S* take a path S→I→D. So, *I* attracts the traffics. In (b), suppose that the path D→B is wanted, *D* will send back (D→C) as its response message. When *I* eavesdrops this message, it sends （D→I→B）to *D* to make *D* modify its routing rules. And this new rule is if the destination is *B*, the next hop is *I*. Additionally, *I* takes *C* as the next hop when the destination is *B*. A local loop is formed and the path from *D* to *B* is blocked.



（a） （b）

Figure 1. Spoofing attack

(2) Sinkhole

In a sinkhole attack, as shown in Fig. 2, an accommodationist node attracts major communication in a specific scope to make a accommodationist-centered sinkhole. A classic sinkhole is: a attacker claims that there is a high quality link through it to the sink. The attacker's neighbor will choose it as the key node to the sink. In this case, usually the attacker communicates with the sink through one-hop with a powerful RF level.

(3) Sybil

In a sybil attack, a node plays multi-roles in net, which makes it easier to be accepted by most paths. Sybil definitely decreases the effectiveness of false tolerance. Sybil effects geographic routing seriously. Geographic position based routing protocol usually asks the nodes exchange their coordinates with their neighbors. The whole system works only if every node gets a unique coordinate from each neighbor. However, though sybil, an attacker has more than on coordinate. As Fig. 3 shows, the coordinate of intruder *I* is (5, 6) and its copy's is (3, 4). As far as other nodes' concern, these two nodes are totally different nodes. So, multi-path is established through *I* and its copy, for example, D→E→F and G→H.

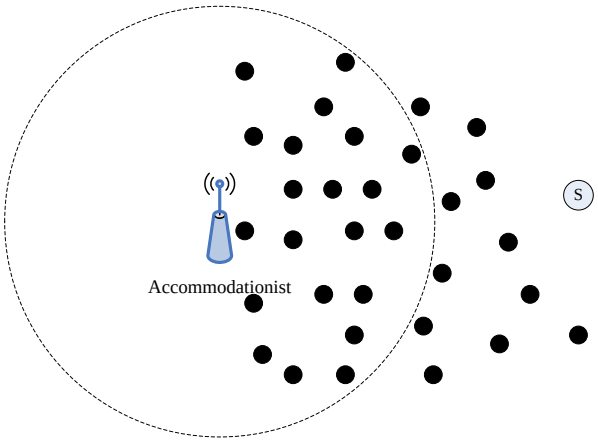


Figure 2. Sinkhole attack

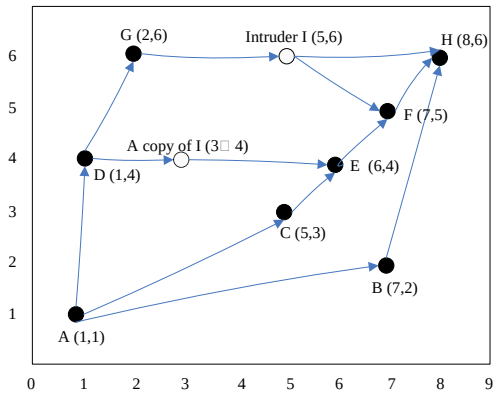


Figure 3. Sybil attack

(4) Wormhole

Wormhole is conducted by the collusion of two attackers. Generally, one is near to the sink and the other is further. The latter one claims that it can establish a low-delay and high-throughput link to the sink. So, it attracts communications. An example of wormhole is shown in Fig. 4.

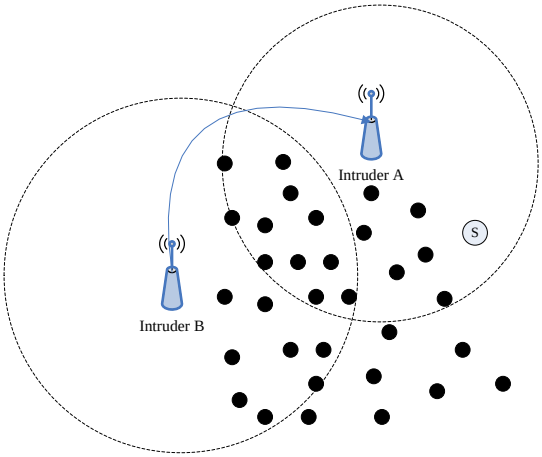


Figure 4. Wormhole attack

Wormhole attacks are firstly defined by Y. Hu [6]. Y. Hu also proposes a mechanism named Packed Leashes for detecting and defending wormhole attacks. The geographical leash is to ensure that there is a certain distance from the destination node to the source node. The temporal leach is to ensure that there is an upper bound for packet lifetime. L. Hu [7] suggests utilizing the directional antennas for neighborhood discovery. Poovendran [8] presents the model of wormhole attacks using a graph theoretical framework, in which one of the nodes is appointed as the network guard for defending wormhole attacks. Chio [9] suggests setting a time threshold for message delivery. All the above methods require extra hardware for location information or tight clock synchronization.

Traditional security strategies are usually employed to detect wormhole attacks in wireless sensor networks. The SeRWA protocol [10] utilizes symmetric key cryptography and neighbor list exchange to validate neighborhood. Similarly, Lee [11] proposes using message authentication codes to detect wormhole attacks. Nait-Abdesselam [12] suggests exchanging the encrypted probing packets for neighbor validation. In paper [13], every node makes use of a pair-wise key to establish a secure route to the mobile sink. The encryption methods will inevitably add computing burden to sensor nodes.

Algebraic topology analysis can also be used for locating wormholes. Maheshwari [14] uses connectivity information to look for forbidden substructures in the connectivity topology.

Hayajneh [15] uses the distance between sensor nodes to sense the change of topology. Dong [16] utilizes the closed neighbor sets of the candidate paths to determine whether there are any wormholes. The HCA4DW mechanism is quite different from the mentioned methods above. We discover the maximum necessary hop count between any two sensors in the same neighbor set of a normal sensor node for neighborhood validation. We note that Jen [17] attempts to solve wormhole attacks using hop count method. In [17], the destination nodes simply choose a relatively appropriate hop count route for data delivery. However, our goal is to use hop count for neighbor validation.

III. WORMHOLE DETECTION USING HOP COUNT ANALYSIS

Intuitively, we can detect the topology change through the distance change. However, the calculation of distance depends on the extra hardware such as GPS. In HCA4DW, the location information is avoided. We use the hop count for neighborhood validation and topology change determination.

a. Problem Description

Suppose a 2-dimention space with only one boundary. If wormholes are introduced into the space, the space will be twisted and homeomorphic to a wormhole space [16, 19]. We consider the initial space is contractible, and wormhole is closed [18]. A wormhole link in WSN supplies a shortcut between two normal sensor nodes. For example, Fig. 5(a) shows two sensor nodes A and B which are distant from each other. Fig. 5(b) shows that two wormhole attackers W1 and W2 are introduced into the space. They perform as one node, as depicted in Fig. 5 (c).

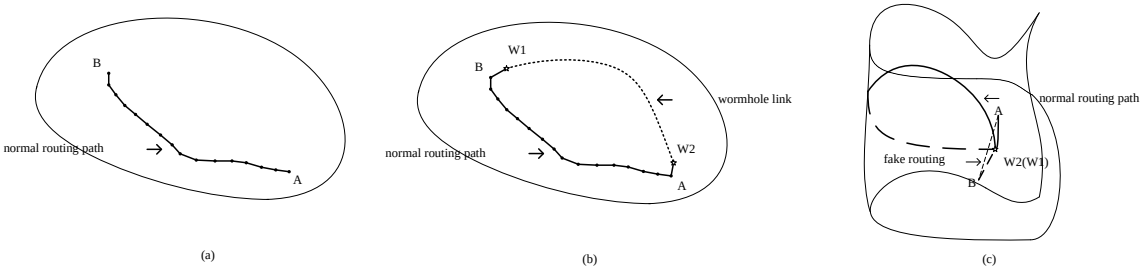


Figure 5. (a) 2-dimention space with the nodes A and B; (b) W1 and W2 are wormhole nodes; (c) A and B become neighbors.

Theoretically, we can determine the wormhole nodes according to the distance change among the neighbor nodes. In $\tilde{S}$, every sensor node i along a routing path P has a small closed neighbor set $N(i) = \{ j \mid 0 < \text{distince}(i, j) \le r \}$, where r is the communication radius of a sensor node, and $\text{distance}(x, y)$ is the Euclid distance between x and y. The maximum distance between any two nodes in $N(i)$ should make the logic expression (1) true.

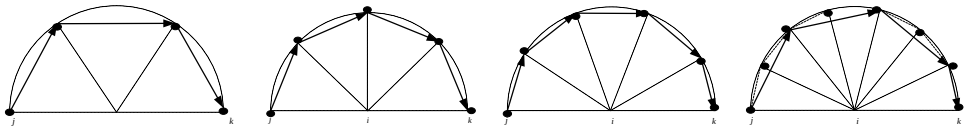
$$\text{distance}(x, y) \le 2r \wedge \forall x \in N(i) \wedge \forall y \in N(i) \quad (1)$$

Unfortunately, we do not know the GPS information of sensor node. We use the hop count for communication to validate neighbor relationship.

b. Maximum Hop Count in the Same Neighbor Set

Assume that there is a sensor i in wireless sensor networks, and nodes j and k are both its neighbors, i.e. $j \in N(i)$, $k \in N(i)$. The number of hops from j to k can help us determine whether i is a wormhole node. The longest distance between sensor j and k is $2r$. In addition, for any three nodes, if they are in neighbor, the maximum intersection angle θ among them is 60^o.

The maximum necessary hop count between two nodes in the same neighbor set is related to the deployment density of sensor nodes D and the communication radius r. Here we consider that the sensor nodes are deployed in uniform distribution. Then, there will be $\left\lceil \frac{1}{2} D \times \pi r^2 \right\rceil$ sensor nodes which distribute within half of the area that sensor i covers. In the worst situation, these $\left\lceil \frac{1}{2} D \times \pi r^2 \right\rceil$ sensors locate on the boundary of the coverage area. Fig.6 shows the maximum necessary hop count N_Hops at the different value of $\left\lceil \frac{1}{2} D \times \pi r^2 \right\rceil$.



$(a)\left\lceil \frac{1}{2}D\times\pi r^2 \right\rceil = 4$ $(b)\left\lceil \frac{1}{2}D\times\pi r^2 \right\rceil = 5$ $(c)\left\lceil \frac{1}{2}D\times\pi r^2 \right\rceil = 6$ $(d)\left\lceil \frac{1}{2}D\times\pi r^2 \right\rceil = 8$

$\left\lceil \frac{1}{2}D\times\pi r^2 \right\rceil$	4	5	6	7	8	9	10	11	12	13	…
N_Hops	3	4	5	3	4	4	3	5	4	3	…

Figure 6. Examples of the mapping between D and N_Hops

To sum up, the mapping between D and the maximum necessary hop count in the worst situation is

$$N\_Hops = \left\lceil \left\lceil \frac{1}{2}D\times\pi r^2 - 1 \right\rceil / \left\lfloor 60\times\left\lceil \frac{1}{2}D\times\pi r^2 - 1 \right\rceil / 180 \right\rfloor \right\rceil. \quad (2)$$

It implies that message from any node in $N(i)$ must be able to reach any other node in $N(i)$ through a routing path without sensor i within N_Hops. If so, sensor i is a normal sensor node. Otherwise, it is a wormhole attack node.

c. The Detail Procedure of HCA4DW

The HCA4DW can be integrated with the SMR protocol [20], which is proved to be suitable to wireless sensor networks because of its lower complexity during the procedure of route discovery. Practically, the SMR protocol is vulnerable to the wormhole attack because the route with minimum hops or best QoS are more inclined to be selected as the communication. The detail steps of HCA4DW are as follows.

Step1: Determine a candidate route path. The source node broadcasts $MSG_{request}$ for route discovery. The destination node selects a primary route P as the candidate route, and reports it to the sink node.

Step2: Examine whether P involves wormhole nodes. On receiving P, the sink node sends MSG_{detect} to all the sensor nodes involved in P to initiate the wormhole detection procedure. For example, after the sensor i receives this detection command, it will collect the information of its neighbors, i.e. $N(i)$, and report $N(i)$ to the sink node.

Step3: The sink will choose one node in $N(i)$ as the seed node and send it $MSG_{validate}$.

Step4: On receiving $MSG_{validate}$, the selected seed node broadcast $MSG_{broadcast}$ to the other nodes in $N(i)$. Each node in $N(i)$ will receive $MSG_{broadcast}$ through different routes. They should select one according to the following regulation: (1) without sensor *i* involved, and (2) with the minimum hops. All the nodes are required to report the detail information of the selected route to the sink.

Step5: After receiving all the feedbacks, the sink node will examine this routing information. It will count the number of hops that each route contains, and compare it with N_Hops. For example, there are two sensor nodes x, y in $N(i)$. Node x is selected as the seed, and y is any other element in $N(i)$. The routing path from x to y can be represented as a node set $R = \{z \mid z \in N(i) \wedge z \neq i\}$. If $|R|$ is greater than N_Hops, sensor *i* can be concluded as a wormhole node.

Step6: If all the sensor nodes in P pass the wormhole validation procedure, the sink node will inform the source node that P can be used as the communication path.

IV. PERFORMANCE ANALYSIS AND EVALUATION

We evaluate the performance of our HCA4DW mechanism using OMNET++ simulation. We generate two types of network topology according to the distribution of sensor nodes: uniform distribution topology and random distribution topology. As introduced above, *r* represents the communication radius of sensor node. The square field size is $10r \times 10r$. Since the distribution density of sensor nodes affects the performance of HCA4DW, we fill the square area with different sensor node density. We omit the situation where the node density is less than 10×10 because in this situation the whole network may be in a disconnected status. The location of wormhole nodes and the length of wormhole link are two other considered factors. We need to evaluate the performance of HCA4DW in two aspects: (1) Accuracy Evaluation. It includes Detection Rate and False Alarm Rate; and (2) Communication Cost. It is because the communication is the main reason that leads to the consumption of sensor nodes. We performed 100 times experiments with each variables setting and averaged the results.

a. Accuracy Evaluation

a.i Detection Rate

Detection Rate implies how many malicious nodes are correctly detected and located. Fig.7 shows the detection rate of HCA4DW at different node density. Fig.7 (a) and (b) are the experiment results of detection rate in the situation where both of the two wormhole nodes locate inside the networks. In uniform distribution network, when the density is less than 15×15, every node in the same neighbor set is separate from the others. In this scenario, all the sensor nodes across the network including the malicious nodes are considered by the sink as the wormhole nodes. So, the detection rate is 100%. When the node density is greater than 15×15, the sensor node can contact with each other, and the whole network is available. In this scenario, detection rate is related to the length of wormhole link. It is found that when the length of wormhole link is greater than or equal to $3r$, HCA4DW can detect and locate with accuracy of 100%. When the distance of the two wormhole nodes are shorter than or equal to r, they may have some common neighbor sensors. If one of these common neighbor sensors is selected as the seed node, it is possible that $MSG_{broadcast}$ can reach all the nodes that are neighbor to the wormhole nodes within N_Hops. In this scenario, HCAA4DW can not tell the malicious nodes from the normal ones. However, we hold that most wormhole nodes are deployed remotely from each other, and the length of wormhole link is rarely less than r. In random distribution topology, the connectivity is better than that in uniform distribution topology, which leads that when the node density is less than 15×15, HCA4DW may miss some wormhole nodes. Both in Fig.7 (a) and (b), with the increase of node density, the detection rate for the wormhole nodes with one times r link goes down.

Fig.7 (c) shows the detection rate of the situation where the topology is random distribution and at least one wormhole node is on the boundary. If a node is on the boundary, it has relatively less neighbors. Therefore, when the wormhole nodes are on the boundary and their link length is less than r, they may have more chance to pass the detection of HCA4DW. That is the reason why, at the same node density, the detection rate in Fig.7 (c) for one times r link is less than that in Fig.7 (a) and (b).

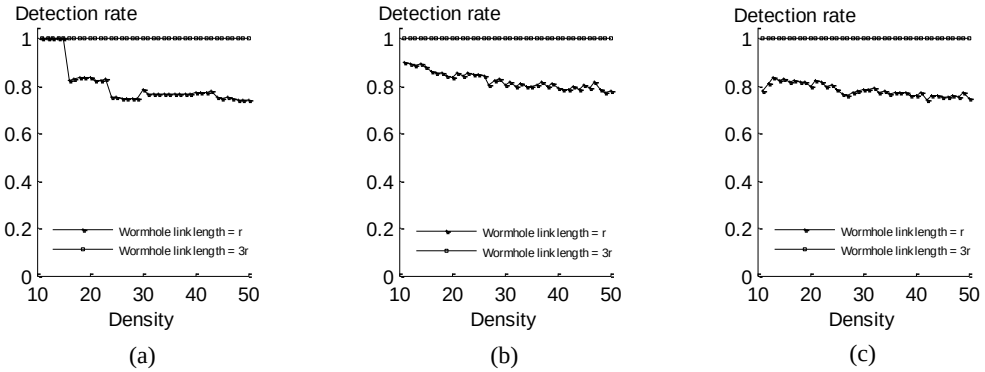


Figure 7. (a) Uniform distribution; (b) Random distribution;
(c) Random distribution with more than one wormhole nodes locate on the boundary

a.ii False Alarm Rate

False Alarm Rate implies how many normal nodes are considered mistakenly as the malicious nodes. Fig.8 (a) and (b) shows the false alarm rate of HCA4DW in the uniform distribution topology and in the random distribution topology respectively. As discussed above, in uniform distribution network, when the density is less than 15×15, all the normal sensor nodes across the network are considered by the sink as the wormhole nodes mistakenly (see Fig.7 (a)). In this situation, the false alarm is much closer to 100% (see Fig.8 (a)). When the deployment density is great enough, which is to say there is an alternative route path which excludes the investigated node between any two nodes in the same neighbor set, the false alarm of HCA4DW is 0. The influence by the node density is more obvious in random distribution network, as depicted in Fig. 8 (b). To sum up, Fig.8 reminds us that the accuracy of HCA4DW is much related to the node density, and we should select proper node deployment density for HCA4DW running.

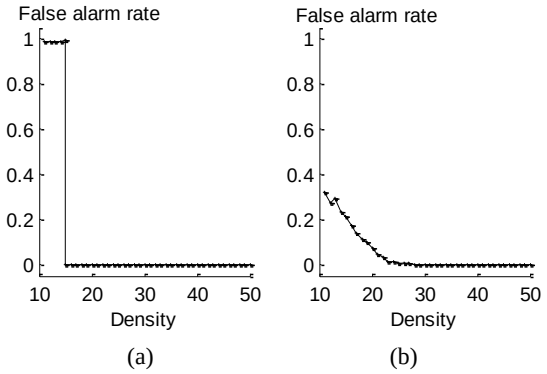


Figure 8. (a) Uniform distribution; (b) Random distribution.

b. Transmission Cost

In the HCA4DW mechanism, the overall communication volume can be divided into two categories: (1) CM_1, the communication between the sink node and in-network sensor nodes; and (2) CM_2, the communication among the in-network sensor nodes for validating the neighboring relationship. Total communication volume CM is the sum of the two categories, i.e.

$$CM = CM_1 + CM_2 \tag{3}$$

(1) The communication volume between the sink node and in-network sensor nodes

Assume that route P is the candidate path. Sink node sends validation command to each node in P, and the related in-network sensor nodes will report their route information generated according to Step 5 in section 3.c back to sink. The communication volume CM_1 is

$$CM_1 = |P| + \sum_{i \in P} (|N(i)| - 1) \tag{4}$$

(2) The communication volume for validating the neighboring relationship

Suppose that we are investigating sensor i. A sensor in $N(i)$, named sensor j, is selected as the seed node to initiate the validation procedure. Sensor j will broadcast the validation message $MSG_{broadcast}$. Any other sensor nodes in $N(i)$ is designed to forward $MSG_{broadcast}$ only once. Then, the communication volume CM_2 is

$$CM_2 = |N(i)| \tag{5}$$

We test the communication volume both in uniform distribution network and in random distribution network. The longest route is selected for transmission test in each experiment. Fig.9 shows that the communication volume is in positive correlation with sensor node density. In addition, there is no obvious difference in communication cost in different topologies.

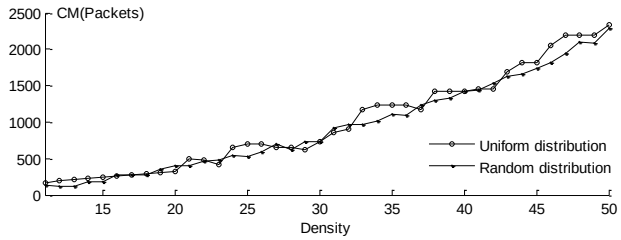


Figure 9. Communication cost of the HCA4DW mechanism

V. CONCLUSION

In this paper, we present the HCA4DW mechanism for detecting and locating wormhole nodes in wireless sensor networks. In HCA4DW, we utilize neighborhood validation to reflect the change of topology so as to discover the wormhole attacks. We present the maximum necessary hop count between the sensor nodes in the same neighbor set. This threshold can be used instead of physical distance for neighborhood validation. Therefore, sensor nodes do not need any extra hardware such as GPS and directional antenna.

In the future, we will make efforts to reduce the communication cost for HCA4DW execution. In the current version of the HCA4DW mechanism, all the work of neighborhood validation is done on the sink node. It needs several rounds of communication between the sink and the in-network nodes. We are planning to push this validation procedure down to the in-network sensor node.

ACKNOWLEDGMENTS

The research work in this paper is supported by the National Natural Science Foundation of China under Grant No. 61100182 and Fundamental Research Funds for the Central Universities under Grant N110404016.

REFERENCES

[1] J. Agre, L. Clare, “An integrated architecture for cooperative sensing networks”, IEEE Computer, Vol 33, No. 5, 2000, pp. 106-108.

[2] D. Estrin, R. Govindan, J. Heideman and S. Kumar., “Next century challenges: Scalable Coordination in Sensor Networks”, Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp.263-270, USA, 1999.

[3] Kewei Sha, Junzhao Du, Weisong Shi, “WEAR: a balanced, fault-tolerant, energy-aware routing protocol in WSNs”, International Journal of Sensor Networks, Vol 1, No. 3/4, 2006, pp.156-168.

[4] Habib M.Ammari, Sajal K. Das, "A trade-off between energy and delay in data dessemination for wireless sensor networks using transmision range slicing", Computer Communications, Vol 31, No. 9, 2008, pp.1687-1704.

[5] Karlof C, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, Vol 1, No. 2/3, 2003, pp. 293-315.

[6] Y.-C. Hu, A. Perrig, D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 1976-1986, USA, March 30 - April 3, 2003.

[7] L.X. Hu and D Evans , "Using directional antennas to prevent wormhole attacks", Proceedings of Network and Distributed System Security Symposium, USA, February 5-6, 2004.

[8] Perrig, Adrian, Trappe, Wade, Gligor, Virgil and Poovendran Radha, "Secure wireless networking" Journal of Communications and Networks, Vol 13, No. 1, 2007, pp. 323-327.

[9] S. Choi and D.Y. Kim, D. H. Lee, J.I. Jung, "WAP: Wormhole attack prevention algorithm in mobile Ad Hoc networks", Proceedings of 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp. 3434-348, USA, June 11-13, 2008.

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

[11] G. Lee , D. K. Kim, J. Seo, "An approach to mitigate wormhole attack in wireless Ad Hoc networks", Proceedings of 2008 International Conference on Information Security and Assurance, pp. 220-225, Korea, April 24-26, 2009.

[12] J Zhu, KL Hung, B Bensaou, F Nait-Abdesselam, "Rate-lifetime tradeoff for reliable communication in wireless sensor networks", Computer Networks, Vol. 52, No. 1, 2007, pp. 25-43.

[13] A. Rasheed and R. Mahapatra, "Mobile sink using multiple channels to defend against wormhole attacks in wireless sensor networks", Proceedings of the 28th IEEE International Performance Computing and Communications Conference, pp..216-222, USA, December 14-16, 2009.

[14] R. Maheshwari and J. Gao, S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information", Proceedings of the 26th IEEE International Conference on Computer Communications, pp. 105-115, USA, May 6-12, 2007.

[15] T. Hayajneh and P. Krishnamurthy, D. Tipper, "DeWorm: a simple protocol to detect wormhole attacks in wireless Ad hoc networks", Proceedings of the Third International Conference on Network and System Security, pp. 73-80, Australia, October 19-21, 2009.

[16] D. Z. Dong and M. Li, Y. H. Liu, X. Y. Li, X. K. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks", IEEE/ACM Transactions on Networking, Vol 19, No. 6, 2011, pp. 1787-1796.

[17] S. M. Jen and C. S. Laih, W. C. Kuo, "A hop-count analysis scheme for avoiding wormhole attacks in MANET", Sensors, Vol 19, No. 6, 2009, pp. 5022-5039.

[18] L. J. Qian and N. Song, X. F. Li, "Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach", Journal of Network and Computer Applications, Vol 30, 2007, pp. 308-330.

[19] A. Hatcher, "Algebraic topology", Cambridge University Press, Cambridge, 2002.

[20] S. J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in Ad hoc networks", Proceedings of IEEE International Conference on Communications, pp. 3201-3205, Finland, June 11-14, 2001.