Link-Based Wormhole Detection in Wireless Sensor Networks

Xiaoyuan Zhou, Lijun Chen
National Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, P.R. China, 210023
zxy@smail.nju.edu.cn, chenlj@nju.edu.cn

ABSTRACT: *Wormhole attack is one of the most severe threats against multi-hop wireless sensor networks. An attacker can easily prevent a normal network from collecting information. Most existing methods have difficulty in finding out the wormhole accomplice nodes or obtain a high detection success rate. In this work, we propose a novel detection mechanism. Our method requires only a small number of anchor nodes. Using these anchor nodes disposed in a network, we can get many links among nodes for detecting the existence of a wormhole channel quickly. A node matching algorithm based on the links is proposed to find out the wormhole nodes. For a hidden wormhole attack, a traffic analysis algorithm based on the links is proposed to distinguish the infected area nodes which locate around wormhole nodes. Finally, our wormhole detection method is evaluated to be efficient by experiments.*

Keywords: Wormhole Attacks, Detection, WSN, Anchor Nodes

Received: 15 May 2013, Revised 28 June 2013, Accepted 30 June 2013

1. Introduction

As a kind of sensing networks, the wireless sensor networks, WSN, play an increasing important role in the development of smart city. By sensing devices wireless sensor networks are able to monitor environment status information in a certain range, such as temperature, light, sound, vibration. Due to the limit of energy and storage capacity of nodes in WSN, an actual application will be faced with a lot of security problems. Wormhole attack is one of the most severe threats against wireless sensor networks.

A wormhole attack model is shown in Figure 1. The WS-WR is a special, high-quality, and low-latency channel arranged by adversaries. By using this special channel, one co-conspirator node can pass the data to another accomplice node in a hop. We classify wormhole attacks into explicit wormhole attacks and hidden wormhole attacks by checking that the header of the packet is tempered or not. If there is no wormhole, a packet, which is sent by the source node SS, travels 12 hops to the destination node SD. In an explicit wormhole attack, the packet gets the routing link like SS-Sa-WS-WR-Sc-SD. But in a hidden wormhole attack, the packet will be just forwarded by 3 hops. By using the special channel WS-WR, the wormhole nodes WS and WR attract large

numbers of information from many nodes. In addition, an attacker can also eavesdrop on information from the communication easily without being detected, since communications among nodes are wireless. Therefore, an adversary can collect and analyze large amounts of data and discard or tamper with part of the data to affect normal monitoring of the network. An adversary is also able to prevent a network from collecting information, even though the network has adopted authentication and encryption mechanisms. The existence of such channels not only undermines the routing of a network, but also affects the normal monitoring of a network terribly.

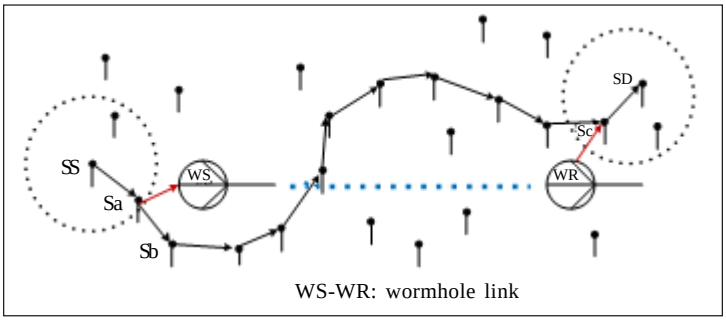


Figure 1. A wormhole attack model

There are lots of methods to detect the wormhole intrusions. A method [1] is based on the clock synchronization in a wireless network. It requires that the clock is fully synchronized so the method is not suitable for WSN. Because of the high cost and low success detection rate, the method [2] based on the directional antenna for WSN has restriction of wormhole detection. A literature [3] utilizes tree-based MAC method to detect wormhole attacks in Ad Hoc network. However, it will consume more energy in the calculation. There are two kinds of methods based on anchor nodes for detecting the existence of a wormhole: localization algorithm and end-to-end methods [4, 5, 6]. Localization algorithm is used to calculate the distance between anchor nodes and other ordinary nodes for detecting wormholes. When the distance is too far, the results of the localization algorithm have more accumulative errors which affect the wormhole detection success rate. To avoid the deviation, some end-to-end approaches to get the distance between nodes using the anchor nodes' geographic information instead. In addition, there are many methods to detect wormholes which do not require any strong constraints, such as special hardware, clock synchronization, directional antenna, etc. A method based on the connection between nodes is proposed [7], by which no special equipment is needed. In [8], a method is proposed to reconstruct the network topology by MDS. And based on the connectivity information, [9] utilizes the model UDG to detect wormholes. The authors of [10] propose a detection method based on k-hop neighbor information. Clustering coefficient calculated by the method has a great impact on the results of the wormhole detection. Other neighbor-based detection methods [11, 12] use clustering coefficient in different ways. But such methods have difficulty in finding out the wormhole accomplice nodes further or obtaining a high detection success rate.

In this paper, we propose a novel link-based method to detect wormholes. Compared to most existing methods [4,5,6] based on geographic location information, our method only needs a small amount of the anchor nodes and in which we also propose a different procedure to build the network communication graph. Compared to the most wormhole detection methods that do not need any strong constraints, our method can find out the wormhole nodes after detecting the existence of a wormhole channel. The link-based node matching algorithm, LBNM, is used to find out the wormhole nodes in the network within explicit wormhole attacks. For a hidden wormhole attack, the link-based nodes' traffic analysis and comparison algorithm, LBNF, is used to determine the infected area. The nodes' traffic, which we are talking about, refers to the amounts of nodes' effective information which is forwarded by each node. And the effective information is only the first packet which reaches to the root node from every node in the network. Approaches in [7, 8, 13, 14] are based on the network topology. Note that these methods may have a high detection rate in theory. But other factors in an actual complex environment, such as sleeping and wake-up mechanisms, adding a node in a network, routing mechanisms, will have a great impact of the results of detecting wormhole. But our approach has further work to confirm it.

This paper is organized as follows. In section II, we describe some assumptions of our detection system and four kinds of wormhole model. In section III, we introduce our wormhole detection mechanism in detail. The next section is our experiments and analysis of the results. And we conclude our work in section V.

2. System model

In this section, we first describe some assumptions of our detection system, which are mostly weaker conditions the same as those needed by other researchers. And then we introduce the hardware components of our detection system. Finally, we raised two goals for our wormhole detection mechanism.

2.1 The system assumes

Our detection method needs no strong constraints in addition to a small amount of anchor nodes. The wormhole channel is able to provide a shorter path for routing a packet, by which we assume that a node in the network should have a certain routing capability. But our wormhole detection mechanism still takes effect on flood-routing. During detecting a wormhole, we mainly consider impacts caused by the presence of the wormhole channel. We assume the contents of links are not discarded or tampered by wormhole nodes. We assume that we have known a parameter, the maximum transmission distance of all nodes. Our method does not take the mobility of nodes into consideration, which is different from the wormhole detection method in Ad Hoc network.

The hardware of our wormhole detection system mainly consists of four parts: the root node for issuing the command and gathering information, large numbers of ordinary nodes for sensing the environment and supporting to forward data packets, a certain amount of anchor nodes that can direct access to the location and a back-end system for collecting and analyze the information.

2.2 The wormhole existing models

Depending on the amount of ordinary nodes around the wormhole nodes, we create four models for wormholes as shown in Figure 2. Nodes T are anchor nodes. Nodes S represent ordinary nodes. Nodes, W, are wormhole accomplice nodes. In the model 1, there is only one ordinary node near *W*1 and *W*2. There are more nodes in models 2 and 3. Model 4 illustrates the actual environment, which contains more ordinary nodes near the wormhole nodes, both *W*1 and *W*2.

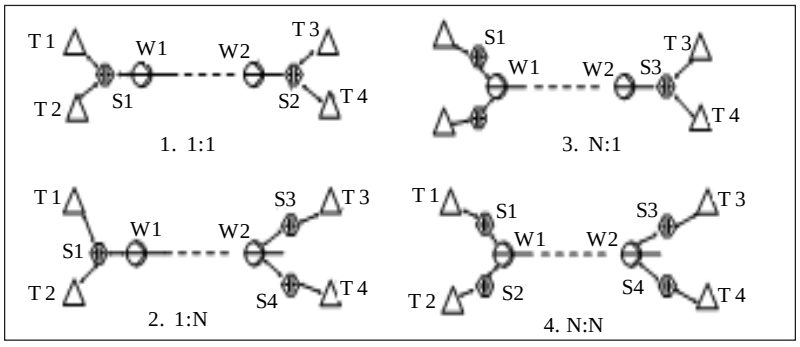


Figure 2. The wormhole existing models

In our wormhole detection algorithm, packets sent by the anchor node T go through an ordinary node S and a wormhole node W to another anchor node which is near the other end of the wormhole channel. By our link-based node matching algorithm, we can find out the wormhole accomplice nodes W1 and W2 in models 1-4. But both W1 and W2 disappear from links in hidden wormhole attacks. For example, in model 4, the algorithm detects the existence of the wormhole in some paths that may be T1-S1-S3-T3 and T2-S2-S4-T4. In order to solve the problems in the hidden wormhole attacks, we use the method that insulating the nodes of infected area to isolate the wormhole accomplice nodes. The algorithm, link-based nodes' traffic analysis and comparison, aims to find the nodes in the infected area. Nodes, S1, S2, S3 and S4, are in the infected area in the model 4.

3. Wormhole Detection Mechanism

Particularly note that our detection mechanism includes discovering the existence of wormhole channels, finding out wormhole nodes in explicit wormhole and infected area nodes in hidden wormhole, does not only consider the first one. The Root node utilizes the packets, which are sent by anchor nodes and detected containing wormhole channels, to perform the link-based node matching algorithm. Then the root node utilizes the packets sent from all nodes to run the link-based nodes' traffic analysis and comparison algorithm.

3.1 The discovery of wormhole attacks

At first, we want to know whether there is a wormhole attack in the network. The algorithm, which can give me the answer, is described as follows:

a) *The root node broadcasts a detecting command, that a parameter R of nodes' max communication distance is attached to. Every node in the network marks when the command is received at the first time.*

b) *Every node, including all anchor nodes, sends information with its identification to the root node by a certain routing mechanism or broadcasting. Geographic information is added to the packets by anchor nodes.*

c) *When a node receives a packet which has been sent or received previously, it discards the packet; otherwise the node adds his identification to the packet and forwards it after the hop plus one.*

d) *If a packet arrives at the root node at the first time, the root node accepts it. Since the packet includes a shorter path from the source node to the root, we can perform the procedure* 1 *on the packets sent by all anchor nodes.*

Procedure 1. OnDiscover()

1: Calculating the distance between anchor nodes *i* and *j* by their location information, as "*D_i_j*";
2: Counting the amount of hops between anchor nodes i and j, as "*N_i_j*";
3: **if** (∃ i and ∃ j satisfy the equation
D_i_j > *N_i_j* * *R*) **then**
4: a wormhole channel exists between *i* and *j*;
5: **end if**
6: return;

When the distance *D* between two adjacent anchor nodes is much bigger than the length of the wormhole channel, the amount of hops between two adjacent anchor nodes is too large so that there is no advantage for the wormhole channel. It implies that we need to increase the density of anchor nodes to improve the accuracy of our wormhole intrusion detection system.

3.2 Link-based node matching

Procedure 2 is an algorithm showing the matching process. In procedure 2, "*link*" is a collection of paths which are sent by all anchor nodes. "*link_i*" is a collection of paths which are sent by an anchor node i and received by other anchor nodes and found out the existence of a wormhole channel. "*Wormhole_link*" is the collection of channel we want to find, which is initialized as link.

Procedure 2. OnMatch( )

1: Intersecting with *link_i* and *link_j*, as *link_i_j*;
2: **if** (∃ *i* and ∃ *j* satisfy the situations that *i* is not *j* and *link_i_j* is not NULL) **then**
3: ∀*k* *Wormhole_link_k* in "*Wormhole_link*" is assigned to the result of intersecting with *Wormhole_link_k* and *link_i_j* if the result is not NULL;
4: **end if**
5: Deleting the same *Wormhole_link_k* in *Wormhole_link*.
6: **if** (*k* satisfies the number of nodes in *Wormhole_link_k* is two) **then**
7: output "*Wormhole_link_k*";
8: **end if**
9: return;

In the case of a single wormhole exists in explicit wormhole attacks, the wormhole channel will be found in all paths, in which the existence of the wormhole attack has been detected. In order to find out the wormhole channel, we only need the packets sent by anchor nodes. If more than one wormhole channels exist in explicit wormhole attacks, "*link_i_j*" may be empty in Procedure 2.

The number of cycles in Procedures 1 and 2 can be limited by the amounts of anchor nodes. In Figure 2, we find two explicit

wormhole paths, link T1-S1-WR-WS-S3-T3 and link T2-S2-WR-WS-S4-T4, by the method of discovery of the wormhole attack. And then we can find the wormhole accomplice nodes WR and WS by the matching algorithm.

3.3 Construct a network communication graph

When detecting infected area in hidden wormhole attacks, we utilize the anchor nodes again. The links among anchor nodes and neighbors of all nodes are used to build the network communication graph. No precise location of a node is needed, while we only need to put together all nodes which are neighbors. The anchor nodes distributed in the network divide the network into many small graphs. So we can construct a graph to describe real network better. Every anchor node sends out the packet with its ID. If two anchor nodes *i* and *j* are on the same boundary of a small graph, a packet, sent by the node *i* and received by node *j*, has a path from *i* to *j*. Then we can connect *i* to *j* with the nodes in the packet. Therefore, we can generate a network communication graph, in which the distribution of nodes is approximate to that in real networks.

3.4 Link-based nodes' traffic analysis and comparison

The wormhole nodes are hidden in the model of hidden wormhole attacks. If we have found the existence of the wormhole attack in a path, some infected nodes are mostly included in the path. The root node gathers a collection of paths from all nodes to the root node. If there are routing protocols and the wormhole nodes, the nodes in the infected area are attracted to put their packets to wormhole nodes. So the occurrence amounts of nodes in infected area increase greatly in paths, which are collected by the root node. While that in some areas, which are filled with ordinary nodes and stridden over by the wormhole channel, decrease greatly. These changes are shown in Figure 3 in detail.

In order to visually observe the effect caused by wormhole attacks. The occurrence amount of each node is statistically as the height of the graph constructed before. In order to identify the nodes in the infected area in the graph, we can construct two three-dimensional surface charts. One is in the situation a wormhole exists. And the other one is in the situation no wormhole exists. By comparing the two 3-D curved surfaces, it is obvious that some significant changes have been happened in the height of nodes in some region. But the changes in the graph are likely to be results of other factors. The situation, nodes in some critical region go into sleep, may cause that network traffics flow to some key nodes. But be different with some methods based on the topology and neighbors, we have an interest in the results for further verification. In order to reduce the impact on the 3-D curved surface of other factors from a physical environment, we utilize link information in wormhole attack detecting algorithm to verify again. If nodes in the region are also found in paths which have been detected containing a wormhole channel, then we make sure that the region is an infected area. In order to avoid the situation some infected nodes are missed by the method because there is no packet needed to forward by them, we can select different nodes as the root node and repeat the procedure more times. These will not only be contributed to determine most nodes in an infected area, but also improve the wormhole detection success rate.

4. Experiments

In this section, we explain the validity of using some anchor nodes to detect the existence of the wormhole channel and to find out the wormhole nodes or infected areas in WSN by experiments. In our experiments, we consider a wormhole channel. But the method proposed by us is able to detect more wormholes. When a packet requires to be forwarded, the complex routing mechanism and Flooding have no differences in our experiments. For a number of copies of a packet sent by a node, the other nodes only receive the packet that arrives firstly.

Our experimental environment is a plain of $800m * 500m$. 20 anchor nodes are distributed in the rectangular area. An anchor node in rectangular Cartesian is selected as the root node. Only a wormhole is arranged on center. Depended on the needs of our experiments, the length of the wormhole channel can be changed. Then we generate a large number of ordinary nodes by random or grid in the area.

4.1 The wormhole attacks detection

In this section, we mainly verify the effectiveness of the link-based nodes' traffic analysis and comparison algorithm in the model of hidden wormhole attacks. 2000 nodes are randomly arranged within the rectangular region. By setting the maximum transmission distance as 24m, we obtain that the average degree of all nodes in networks is 10. Figure 3 (a)-(f) are in the situations mapping the 3-D curved surfaces to the $x - z$ plane or $y - z$ plane. And the heights are the amounts of each node in paths collected by the root node. There will be a normal phenomenon that many nodes' heights are much smaller than that of some nodes nearby in Figure 3. Some nodes are close to the root node in x-coordinate and far from the root in y-coordinate. So

these nodes shall be far away from the root node. But in our figures, they are closed.

The difference between (a) and (b) in Figure 3, is that whether the wormhole exits or not. We set the same y-coordinate for the wormhole nodes. So we can transfer the 3-D curved surface into 2-D. It is useful to detect the wormhole nodes in an actual network. In Figure 3 (a) and (b) are drawn as stairs depended on increasing distances between the source nodes and the root node. If two nodes have the same hops to the root node, they will on the same rung. All neighbors in Figure 3 (a) are on the same rung basically. But in Figure 3 (b), there are two nodes which have far distance on the same rung. We are informed of that these two nodes may be wormhole nodes.

In Figure 3, (c) and (d) are under no wormhole attacks. The difference between them is that they depend on the *x*-coordinate or *y*-coordinate in the network communication graph. In Figure 3, (e) and (f) are under the attacks of a wormhole. Our wormhole accomplice nodes have the same *y*-coordinate, so (d) and (f) have similar results. By comparing (c) and (e), the height of the nodes in certain areas, *x*- coordinate is from 220m to 480m, have changed significantly. Thus we determine that two regions, which are close to 220*m* or 480*m* in *x*-coordinate, are wormhole infected areas. The values of *y*-coordinate in the infected areas are able to be obtained by the same method.

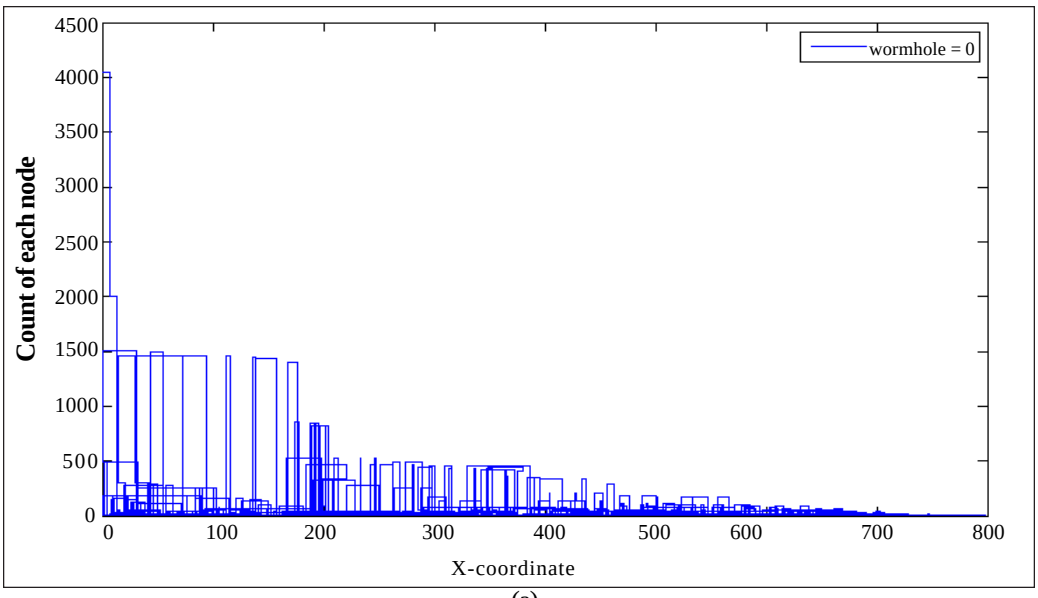
4.2 Compared to an existing approach

An approach is proposed in [7], we call it CBW in Figure 4, which is also based on wireless sensor network for wormhole detection. And our method based on the link is called LBW. In this experiment, nodes are arranged by the models of random and perturbed grid. In Figure 4 (a) and (b), it implies that our method is able to obtain a relatively higher detection success rate. The reason is that our approach is mainly based on link. It is not necessary for a network with high redundancy by ours. Because anchor nodes are able to be arranged by the distribution of nodes in a network, the distributed model of ordinary nodes has little effect on the wormhole detection success rate by our approach.

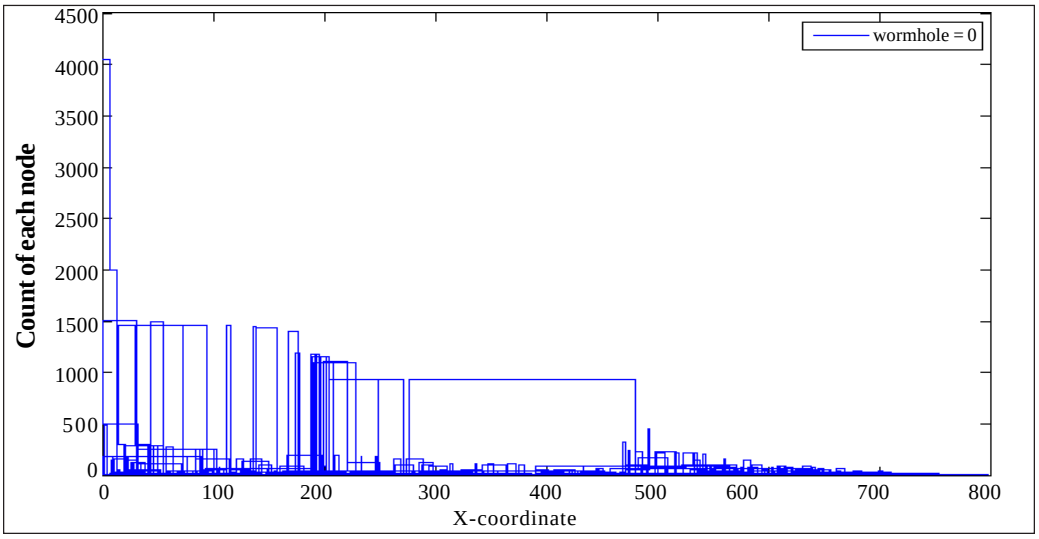
4.3 Anchor nodes' density and their impact of detection success rate

We build some networks, in which ordinary nodes have amounts of 200, 400, 600, 800, 1000, 1500, 2000, 4000, 5000, 6000, 8000 respectively. We arrange 20 anchor nodes and a wormhole. By adjusting the distance of the nodes' maximum transmission in networks composed with different amounts of ordinary nodes, we ensure that the average degrees of all nodes in all networks are close to 6. We repeat 100 times for each network environment. We count the successful detections from the 100 experiments under each network to figure out the relationship between anchor nodes' density and wormhole detection success rate in Figure 5.

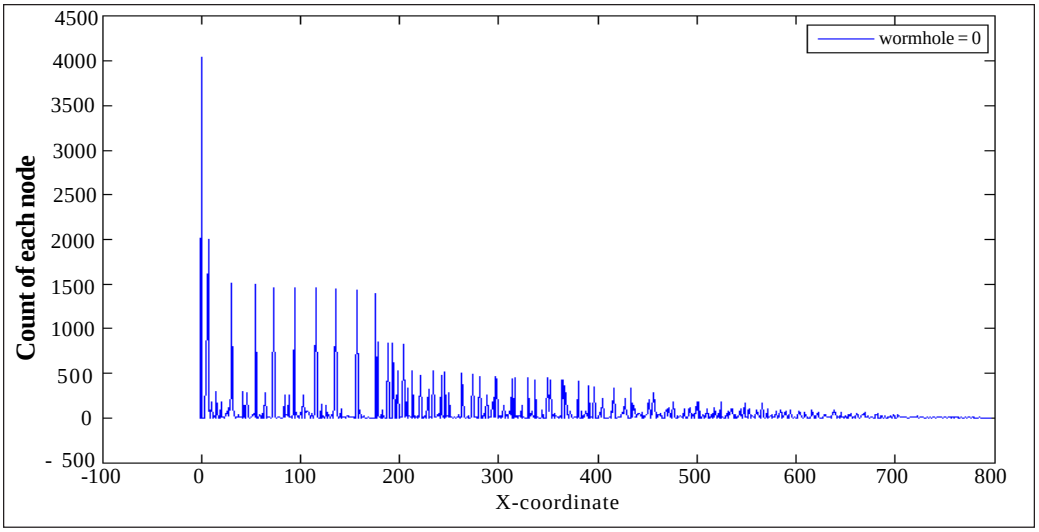
As seen in Figure 5, when the amount of ordinary nodes is 5000, which means that the percentage of anchor nodes in the network is 0.4, our detection method obtains that the wormhole detection success rate is nearly 90%. The wormhole detection



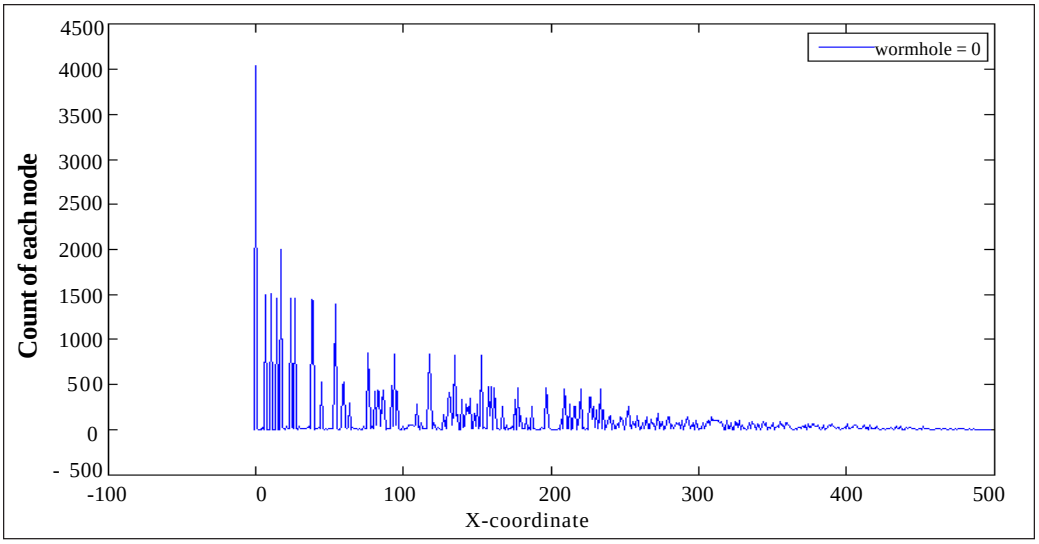
(a)


wormhole = 0
Count of each node
X-coordinate
4500
4000
3500
3000
2500
2000
1500
1000
500
0
0
100
200
300
400
500
600
700
800

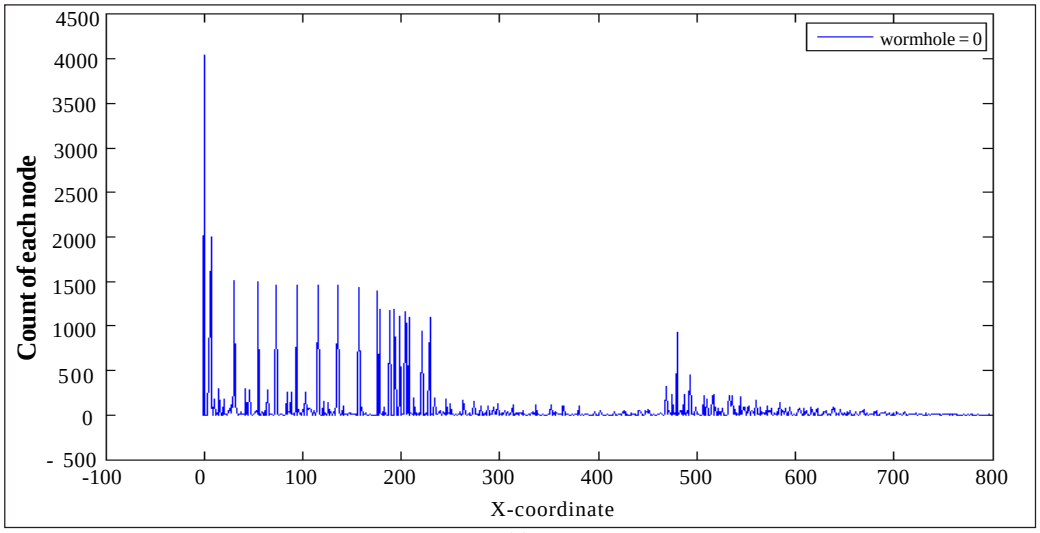
(b)


wormhole = 0
Count of each node
X-coordinate
4500
4000
3500
3000
2500
2000
1500
1000
500
0
- 500
-100
0
100
200
300
400
500
600
700
800

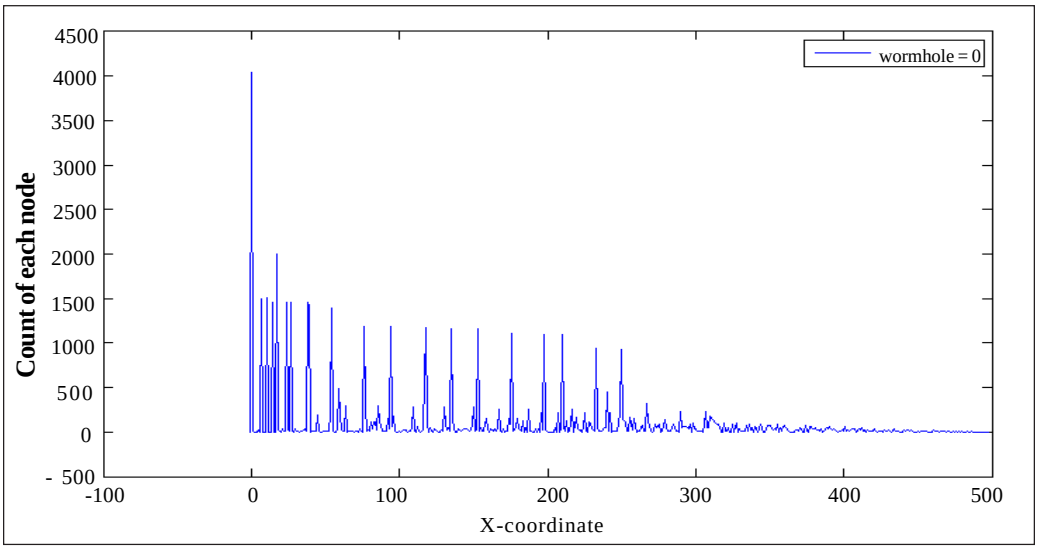
(c)


wormhole = 0
Count of each node
X-coordinate
4500
4000
3500
3000
2500
2000
1500
1000
500
0
- 500
-100
0
100
200
300
400
500

(d)

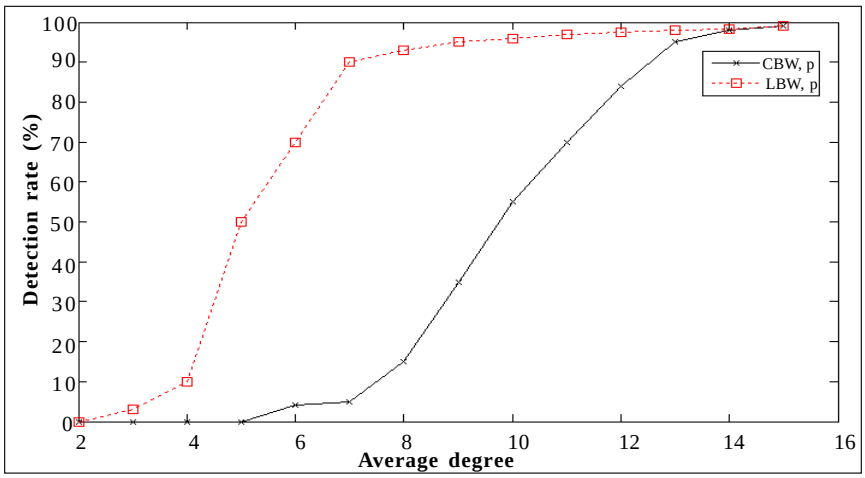


(e)

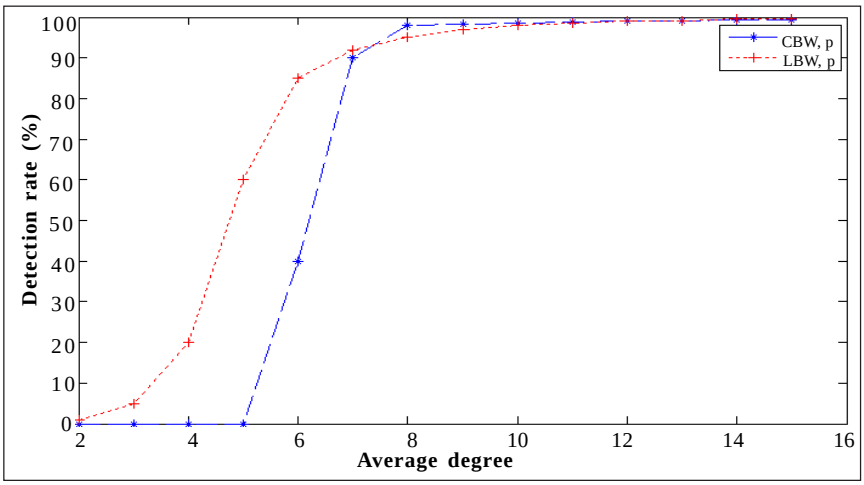


(f)

Figure 3. Counts of each node in paths collected by the root



(a)



(b)

Figure 4. Wormhole detection rates for different configurations. CBW is the method mentioned in literature [7], and the LBW is the method, Link-Based Wormhole Detection of mine. P and R in the legend indicate the distribution model of perturbed grid and random respectively

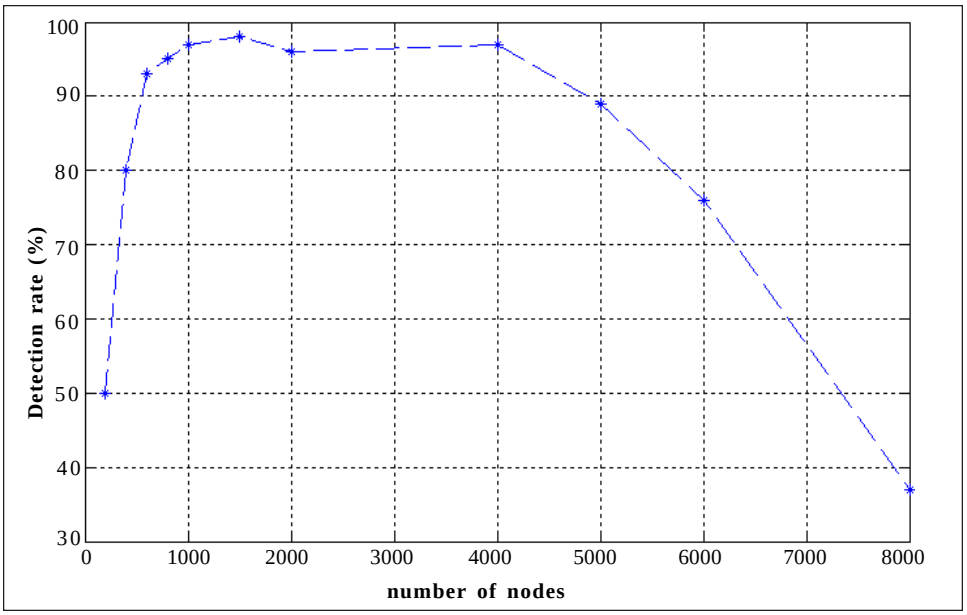


Figure 5. Anchor nodes' density and detection success rate

rate is relatively low when the amount of ordinary nodes is less than 500. The reason is that the average degree of all nodes in a network is close to 6 depended on changing the maximum communication distance. It infers that the advantage of the wormhole channel in the network is not obvious any more. Accounting for it in theory, the situation is that more percentages of anchor nodes in the network, the higher of detection success rate.

5. Conclusion

Wormhole attack is one of the most server security threats in multi-hop wireless sensor networks. Under the condition that the percentage of anchor nodes is 0.4 in a network, the wormhole detection success rate is close to 90% by our method. After we detect the existence of a wormhole attack, further works are taken to determine the wormhole accomplice nodes or infected area nodes. The situation is that more percentages of anchor nodes in a network, the higher of detection success rate. Our method

does not demand on high redundancy in the network. Finally, we take some measures that the wormhole nodes and the infected area nodes are insulated from the network. In order to improve and perfect the wormhole detection mechanism which is based on links, we will consider distributing the anchor nodes by characteristics of a network in the future. We will consider the situation that the wormhole nodes discard and tamper with the packets in the network. We will also study the efficient routing to reduce the cost of the communication for our detection system on an existing monitoring system.

References

[1] Yih-Chun Hu, Perrig, A., Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks, INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. *IEEE Societies*, 3 (30) p. 1976, 1986, March-3 April.

[2] Hu, L., Evans, D. (2004). Using directional antennas to prevent wormhole attacks, *In*: Proceedings of Network and Distributed System Security Symposium, p. 144-154.

[3] Yih-Chun Hu, Adrian.Perrig, Johnson, David, B. (2002). Wormhole Detection in Wireless Ad Hoc Networks, Rice University Department of Computer Science, *Technical Report TR*01-384, Revised: June 15.

[4] Yingfang Fu. (2011). Research on wormhole attacks in wireless mesh networks, *Journal on Communications*, China, January, 32 (1).

[5] Xia Wang, Wong, J. (2007). An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks, *Computer Software and Applications Conference*, 2007. COMPSAC 2007. 31st Annual International, 1, p. 39, 48, 24-27 July.

[6] Xia Wang. (2006). Intrusion Detection Techniques in Wireless Ad Hoc Networks, Computer Software and Applications Conference, 2006. COMPSAC '06. 30th *Annual International*, 2, 347,349, 17-21 Sept.

[7] Dezun Dong, Mo Li. (2011). Connectivity-Based Wormhole Detection in Ubiquitous Sensor Networks, *Journal of Information Science & Engineering*, 27 (1) 65, January.

[8] Wang, W, B., Bhargava. (2004). Visualization of wormholes in sensor networks, *In*: Proceedings of ACM Workshop on Wireless Security, p. 51-60.

[9] Maheshwari, R., Jie Gao, Das, S. R. (2007). Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information, INFOCOM 2007. 26th IEEE International Conference on Computer Communications. *IEEE*, p. 107, 115, 6-12 May.

[10] Znaidi, W., Minier, M., Babau, J. -P. (2008). Detecting wormhole attacks in wireless networks using local neighborhood information, Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on, 1 (5) 15-18 Sept.

[11] Pirzada, A., McDonald, C. (2005). Circumventing sinkholes and wormholes in wireless sensor networks, *In*: International Conference on Wireless Ad Hoc Networks (IWWAN).

[12] Ning Song, Lijun Qian, Xiangfang Li. (2005). Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach, Parallel and Distributed Processing Symposium, 2005. *In*: Proceedings. 19th IEEE International, 8, 4-8 April.

[13] Dezun Dong. (2011). Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks, *IEEE/ACM Transactions on Networking*, December, p. 1787-1796.

[14] Radha Poovendran, Loukas Lazos. (2007). A graph theoretic framework for preventing the wormhole attack, *Journal Wireless Networks*, 13 (1) 27-59, January.