International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Wormhole Detection using Wormhole Geographically Distributed Detection Technique in Wireless Sensor Networks

Jyoti Yadav[1], Dr. Mukesh[2]

[1]M.Tech Scholar, Computer Science Department, TIT&S, Bhiwani

[2]Assistant Professor & HOD, Computer Science Department, TIT&S, Bhiwani

Abstract: ***Routing attacks are a major challenge in the process of designing of effective and robust security mechanisms for WSNs. This research work proposes a distributed wormhole detection algorithm called Wormhole Geographic Distributed Detection (WGDD), that is based on detecting disorder of the networks which is caused by the existence of a wormhole inside the network.***

Keywords: Ad-hoc, WSN, Wormhole

1. Introduction

Wormhole attacks are difficult to detect as the malicious nodes replays valid data packets into the network. Moreover, majority of wireless sensor network routing protocols employ lightweight cryptographic solutions to prevent unauthorized nodes from injecting false data packets into the network. Hence, in wormhole attacks, the replayed data packets pass all cryptographic checks. Since wormhole attacks are easy to implement but hard to detect, wormhole prevention and detection has been an attractive research problem. Most proposed protocols to defend against wormhole attacks use positioning devices, synchronized clocks or directional antennas. Wormhole attacks are the main focus of this paper, which belong to outsider, laptop-class.

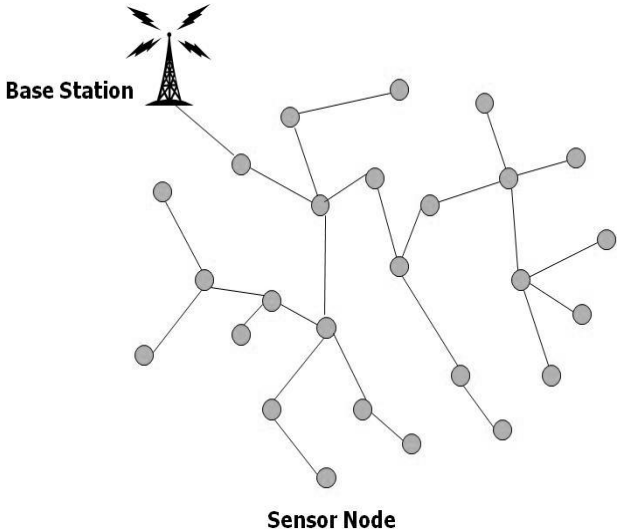

Figure 1: Wireless sensor network

2. Wormhole Attack

Wormholes are one of the most severe attacks on WSN routing. Two or more malicious nodes can collaborate in setting up a shortcut lower latency link between each other Figure 2 and through which they forward packets to each other and replay the packets there locally.

The adversaries convince the neighbor nodes of these two end points that the two distant points at either end of the tunnel are actually very close to each other [12]. An adversary situated close to a base station may be able to completely disrupt routing by convincing nodes that would normally be multiple hops from a base station that they are only one or two hops away via the wormhole [5]. In such a scenario, the attack is similar to the sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station [1].

Wormhole and sinkhole attacks are particularly difficult to defend against, especially when the two are combined. Wormholes are hard to detect because they use a private, out-of-band

3. Wormhole Attack Detection

Our distributed algorithm called Wormhole Geographic Distributed Detection (WGDD) uses a similar hop-counting technique as a probe procedure to detect wormhole attack. After the running of the probe procedure, each node will collect the set of hop-count from its neighbor nodes which are in one(k) hop(s) distance to it, then that node will run Dijkstra's algorithm to get the shortest path for each pair of the nodes, after that, it will reconstruct a local map by MDS (Multidimensional Scaling). After we use a feature called as "diameter" to detect distortions caused by a wormhole in local maps. The overview of this Wormhole Geographic Distributed Detection (WGDD) algorithm can be seen in Procedure 1.

Procedure 1: Wormhole Geographic Distributed Detection (WGDD)
1: Probe Procedure 2: Local Map Computation Procedure 3: Detection Procedure

1. Probe Procedure

Since a wormhole attack is passive, this means that such an attack can only happen when there is some message being transmitted near the wormhole area. In order to detect

whether there is a wormhole attack inside a network, we design a probe procedure to flood a message from some bootstrap node to the whole networks to let all other nodes in the network to count the hop distance from itself to that bootstrap node. Such probe procedure is based on hop-coordinates [18] technique to measure the hop distance from each node to some bootstrap node, which shares the same idea as hop-counting, but has more accurate measurement.

(i) **In bootstrap node**: A bootstrap node x creates a probe message with (i = idx) to flood the network. After that, the bootstrap node will drop any probe message that was originated by it

The bootstrap node has the hop-coordinate:

hopx = 0 and offsetx = 0.

(ii) **In all other nodes in the WSN:** Suppose that a node a is calculating its hop distance, and node b is one of the neighbors of node a. Then the basic probe procedure 2 is as same as hop-coordinates procedure [18] for node a is shown in Procedure 2.

Procedure 2 Probe Procedure in node a

1: INPUT: message (hop_b) from node b € N_a
2: for message (hop_b) from any B € Na and not TIMEOUT do
3: if $hop_b < hop_a$then
4: $hop_a = hop_b + 1$
5: forward (message(hop_a)) to MAC
6: else
7: drop (message($hopb$))
8: end if
9: end for
10: if |Na| == 0 then
11: $offset_a = 0$
12: else
13: $offset_a =$
14: end if
15: return $hop_a$and $offset_a$

Here, a is a node, hop_a is the minimum number of hops to reach node a counting from some bootstrap node (x), the initial value of it will be the largest positive value in practice. The combination of hop_a and $offset_a$ is the hop coordinate for node a, N_a is a set of nodes which can be reached by node a in one hop, and |Na| is the number of nodes in Na.

4. Result and Analysis

We compared the results before and after the attack to see the impact of the wormhole attack on the network.

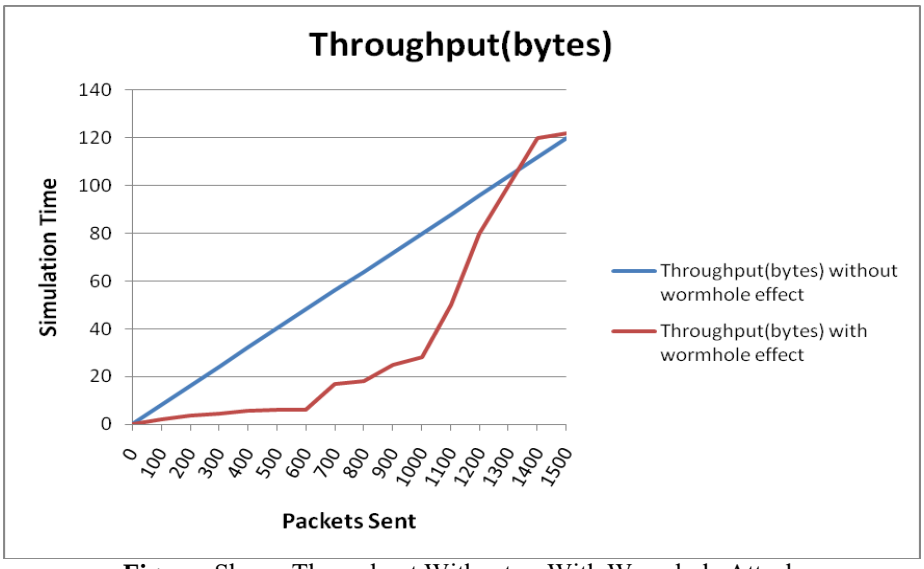

Figure: Shows Throughput Without or With Wormhole Attack

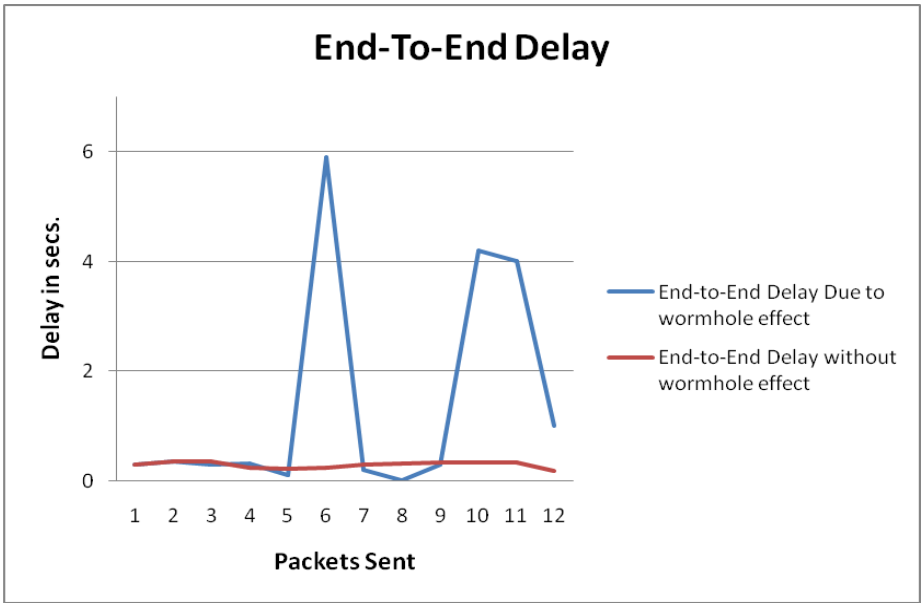

Figure: Shows End-to-End Delay Without or Without Wormhole Attack

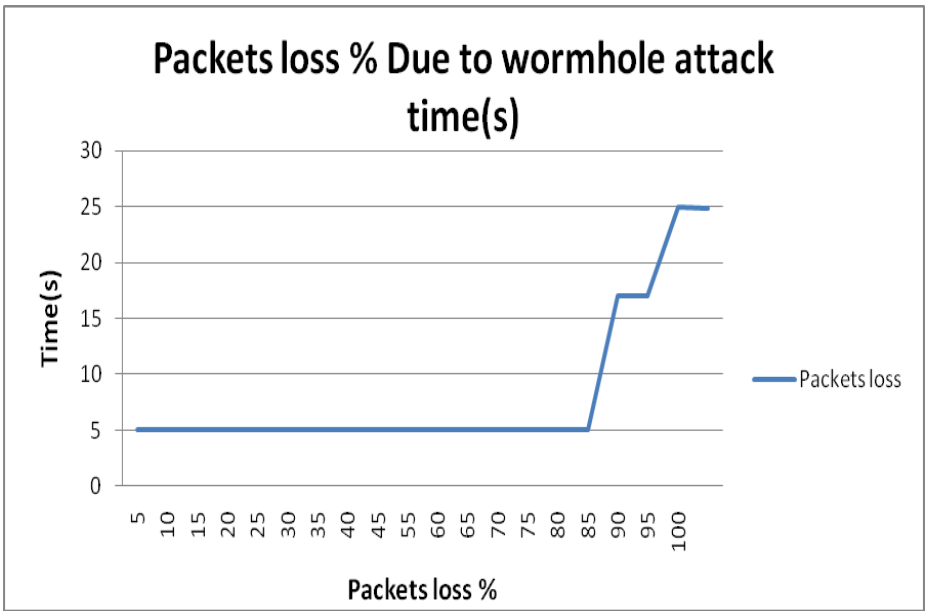

Figure: Shows Packet Loss Due To Wormhole Attack

5. Conclusions

In this paper, we discuss how to detect wormhole attacks in distributed scheme. By assuming that wormhole attacks are passive, we provide a probe procedure to let some bootstrap node flood a probe message to detect some possible wormholes in the network, the probe procedure produces hop-coordinates to each node which represents the hop distance from that node to the bootstrap node. Then each node will compute a local map for its neighbors and itself with the hop-coordinates collected. Since if there is a wormhole in the network, it causes some distortions in some local maps of the nodes which are close to the ends of the wormhole, so we find a feature called "diameter" to detect such distortion in distributed scheme, with the help of that feature– "diameter", we propose a wormhole detection procedure.

We test our Wormhole Geographic Distributed Detection (WGDD) algorithm in simulation environment under different placements of networks. The extensive simulation result shows that our detection algorithm can achieve almost 100% overall detection rate. Even considering about the cases of shorter wormholes which are less than 3 hops long, our algorithm can still make more than 80% detection rate. We can run our detection algorithm in stricter model by setuping $\lambda = 0.1$, it this case, we can achieve almost zero wrong alarm rate.

Since our algorithm is running under distributed scheme, it means that if there is a wormhole, then some nodes close to the wormhole will detect the wormhole attacks, so such advantage of our algorithm may help in defending against wormholes. We may propose the idea of freezing nodes that have detected wormhole attacks in their vicinity, along with their neighbor nodes, in order to isolate and negate the effect of a wormhole.

References

[1] Rehana, J. (2009). Security of wireless sensor network. *seminar on internetworking* (TKK T-110.5190). Helsinki University of TechnologyPadmavathi, G., & Shanmugapriya, D. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security(IJCSIS)*: Vol.4, No.1 & 2

[2] Hanapi,. Z.M. Ismail,. M,. Jumari,. K. & Mahdavi,. M. (2009). Dynamic window secured implicit geographic"forwarding routing for wireless sensor network. *World Academy of Science, Engineeringand Technology*Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks, *IEEE Communications ' Magazine* (p 70-75)

[3] Karlof, C., & Wagner,. D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures.*Ad HocNetworks Journal: Special Issue on Sensor Network Applications and Protocols.Vol.1,* (p293-315), Elsevier Publications

[4] Naeem,. T & Loo,. K. K. (2009). Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks. *International Journal of Digital Content Technology andits Applications*: Volume 3, Number 1. (p 89-90)

[5] Lee , J. C., Leung, V. C. M., Wong, K. H., Cao, J., & Chan, H. C. B. (2007). Key management issues in wireless sensor networks: current proposals and future developments. *IEEE Wireless Communications*,(p76-84)

[6] Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: a survey. *Journal ofInformation Assurance and Security 5*, (p31-44) Lukman Sharif and Munir Ahmed 183Bojkovic,. Z. S., Bakmaz,. B. M,. & Bakmaz,. M. R. (2008). Security issues in wireless sensor networks. *International Journal of Communications*: Issue 1, Volume 2Raj,. P. N. & Swadas,. P. B,. (2009). DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. *International Journal of Computer Science Issues (IJCSI)*: Vol

[7] Lee , J. C., Leung, V. C. M., Wong, K. H., Cao, J., & Chan, H. C. B. (2007). Key management issues in wireless sensor networks: current proposals and future developments. *IEEE Wireless Communications*,(p76-84)

[8] Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: a survey. *Journal of Information Assurance and Security 5*, (p31-44) Lukman Sharif and Munir Ahmed 183

[9] Bojkovic,. Z. S., Bakmaz,. B. M,. & Bakmaz,. M. R. (2008). Security issues in wireless sensor networks. *International Journal of Communications*: Issue 1, Volume 2

[10] Raj,. P. N. & Swadas,. P. B,. (2009). DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. *International journal of Computer Science Issues (IJCSI)*: Vol