International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 6, Nov-Dec-2019, ISSN (Online): 2395-566X

Review of Worm Hole Attack in WSN

M.Tech. Scholar Bharti Yadav
Dept. of CSE
Astral Institute of Technology & Research Indore
yadavbharti10@gmail.com , M.P., India

Prof. Shailendra Tiwari
Dept. of CSE
Astral Institute of Technology & Research Indore
Shailendra.tiwari4@gmail.com, M.P., India

***Abstract* - Wormhole attacks can undermine or put out of action wireless sensor networks. In a typical wormhole attack, the attacker be given packets at one point in the network, forwards through a wired or wireless network with take away latency than the network links, and transmits them to a different point in the network. This paper describes a give out wormhole recognition algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. Since wormhole attacks are passive in nature, a hop count technique is used by the algorithm as a explore procedure, renovates local maps in each node, and then uses a diameter element to detect abnormalities reason by wormholes. It can provide the approximate location of wormholes, which is useful in implementing countermeasures this is the main advantage of algorithms.**

***Keywords* - Wormhole Detection, Wireless Sensor Network, Distributed Algorithm.**

I. INTRODUCTION

Wireless sensor network (WSN) is talented technology consisting of small, low-power devices that integrate limited computation, sensing and radio communication capabilities. The technology has the potential to provide exile infrastructures for numerous applications, including healthcare, industry automation, observation and attack. Currently, most WSN applications are designed to work in trusted environments. However, security issues are a major concern when WSNs are deployed in entrusted environments. An adversary may put out of action a WSN by interfering with intra-network packet transmission via wormhole attacks, Sybil attacks, jamming or packet injection attacks. This paper focuses on wormhole attacks. In wormhole attack the malicious node receives packets at one point within the network, forwards them through a wired or wireless network with less latency than the network, and relays the packets to a different point in the network. Such an attack cryptographic knowledge; consequently, it puts the attacker in an influential position compared with other attacks (e.g., Sybil attacks and packet injection attacks), which make use of vulnerabilities in the network infrastructure. Indeed, a wormhole attack is possible even when the network infrastructure provides co veniality and authenticity, and the attacker does not have the cryptographic keys.

II. LITERATURE REVIEW

Raja Mohmood, R. A; Khan, A.I: According to these author the source node send two RREPs message, but selectively picking any consecutive RREP packets. This approach will likely appropriate in cases where a Wormhole node is located nearer to a source node and likely to underperform when it is located many hops away from the source node. A source node waits for a susceptible duration to receive other RREPs with next hop details from the other neighbouring nodes, without sending the DATA packets to the early RREP node. Simultaneous the expiry of the timer, it checks in CRRT table to find out any repeated next hop node. The chance of malicious path is limited if any repeated next hop node is present in the RREP paths. The simultaneous comparison of the received RREPs, selects a neighbour which has the equivalent next hop as other alternative routes to send the data packets. This solution adds a delay and decreases throughput as more RREPs are waited for, and the process of finding repeated next hop is an extra computation overhead.

Hao Yang, Haiyun Luo: They observe that how the AODV routing protocol works and then implemented Blackhole attack on it at the same time a trust based mechanism for its prevention. The trust based detection method has the better packet delivery ratio and correct Wormhole node detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. Another proposed mechanism i.e. reactive detection method eliminates the routing overhead problem from the on demand way of route generation. Our complete implementation reveals that the proposed method of trust mechanism when applied on AODV protocol gives better results in all the cases for MANET as compared with normal AODV in case of Wormhole attack.

Xiao Yang Zhang; Sekiya; Y., Wakahara. Y.: Analyze the impact of the presence of the Wormhole nodes on the MANET performance. They found that as the percentage of Wormhole nodes increases, the network performance degrades.

Okoli Adaobi [04] et al worked to find the impact of Wormhole attack on the performance of MANET and also found the impact of position of Wormhole node. According to them under the on-demand routing protocol, the closer a malicious node is to the source of traffic, the greater extent of damage inflicted on the network.

N. Balaji, A Shanmugam,"A Trust Based Model to mitigate Wormhole attacks: In this paper we have presented a trust based routing model to deal with Wormhole and cooperative Wormhole attacks that are caused by malicious nodes. We believe that fellowship model is a requirement for the formation and efficient operation of ad hoc networks. The paper represents the first step of our research to analyse cooperative Blackhole attack over the proposed scheme to analyses its performance.

III. WORMHOLE ATTACKS

In wormhole attack the malicious node receives packets within the network, forwards them through a wired or wireless link with much less latency than the default network used by the network, and then relays them to an extra location in the network. In this paper, we assume that a wormhole is bi-directional with two endpoints, although multi-end wormholes are possible in assumption. A wormhole receives a message at its derivation end" and transmits it at its objective end." Note that the designation of wormhole ends as origin and destination are dependent on the context. We also assume that it does not send a message without receiving an inbound message and static i.e., it does not move

IV. WORMHOLE DETECTION ALGORITHM

a hop counting technique as a probe procedure is used in our wormhole geographic distributed detection (WGDD) algorithm. After running the probe procedure, each network node collects the set of hop counts of its neighbour nodes that are within one/k hops from it. (The hop count is the minimum number of node-to-node transmissions to reach the node from a bootstrap node.) Next, the node runs Dijkstra's (or an equivalent) algorithm to obtain the shortest path for each pair of nodes, and reconstructs a local map using multidimensional scaling (MDS). Finally, a \diameter" feature is used to detect wormholes by identifying distortions in local maps. The procedure involved in the wormhole detection algorithm is described in the following sections.

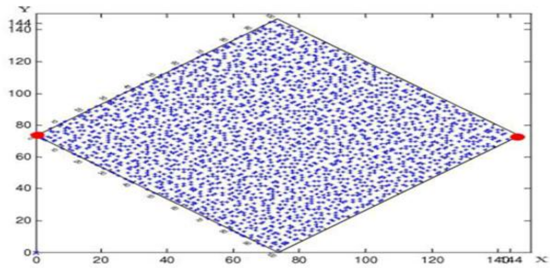

Fig. 1. Wormhole at network edges.

V. PROPOSED METHOD

The wormhole attack is presented in this paper in which two colluding nodes that are far away are connected by a tunnel giving an illusion that they are neighbours. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. These nodes are able to advertise that they have the shortest path through them by using this additional tunnel. Once this link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel. It results in spreading of incorrect topology information throughout the network [8] since these MPRs forward flawed topology information. On receiving this false information, other nodes may send their messages through them for fast delivery. It prevents honest intermediate nodes from source to the destination to establish links between them [11]. Sometimes, due to this, even a wormhole attacker may fall victim to its own success.

VI. CONCLUSION

Wormhole attack is difficult to detect and found to be a challenging work. This attack results in route discovery as well route discovery errors, in addition to the degradation of the communication between the nodes of the network. The proposed method is based on wormhole attack prevention. However, detection of wormhole node is difficult but prevention methods are being implemented. In this work, malicious nodes are implanted in the network and results are examined through simulation. However, implementing this methods or algorithm in a real scenario or a sensor network is more difficult due to limitation of resources.

The proposed algorithm can be improved to detect wormhole attack. The RREP packet sent by the destination can be encapsulated with a code where all the route node information can be given. Also the data packet can be further fragmented into small packets and transmitted via multiple paths to the destination. At the destination, the received packets (through various routes) can be put together to get a valid information. This may allow a secure communication. Additionally, the malicious nodes may not be able to assemble the packets into a valid information as it transmits through different routes. The broken links can be avoided with the help of acknowledgement messages sent by the destination node. The proposed approach presents a decent solution for secure exchange of information while taking into consideration the constraints and limitations imposed by this environment.

REFERENCES

[1]. I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, A survey ofsensor networks, IEEE Communications, vol. 40(8), pp. 102{114, 2002.
[2]. S. _Capkun, L. Butty_an and J. Hubaux, SECTOR: Secure tracking of node encounters in multi-hop wireless networks, Proceedings of the First ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21-32, 2003.
[3]. W. Du, L. Fang and P. Ning, LAD: Localization anomaly detection for wireless sensor networks, Journal of Parallel and Distributed Computing, vol. 66(7), pp. 874{886, 2006.
[4]. L. Hu and D. Evans, Using directional antennas to prevent wormhole attacks, Proceedings of the Eleventh Network and Distributed System Security Symposium, pp. 131{141, 2004.
[5]. Y. Hu, A. Perrig and D. Johnson, Wormhole detection in wireless ad hoc networks, Technical Report TR01-384, Department of Computer Science, Rice University, Houston, Texas, 2002.
[6]. Y. Hu, A. Perrig and D. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1976{1986, 2003.
[7]. J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia and B. Bhargava, Lowcost attacks against packet delivery, localization and time synchronization services in underwater sensor networks, Proceedings of the Fourth ACM Workshop on Wireless Security, pp. 87{96, 2005.
[8]. L. Lazos and R. Poovendran, SeRLoc: Robust localization for wireless sensor networks, ACM Transactions on Sensor Networks, vol. 1(1), pp. 73{100, 2005.
[9]. D. Liu, P. Ning and W. Du, Attack-resistant location estimation in sensor networks, Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks, pp. 99{106, 2005.
[10]. S. McCanne and S. Floyd, The network simulator {ns-2 (nsnam.isi.edu /nsnam/index.php/User Information), 2007.
[11]. J. Newsome, E. Shi, D. Song and A. Perrig, The sybil attack in sensor networks: Analysis and defenses, Proceedings of the Third International Symposium on Information Processing in Sensor Networks, pp. 259-268,2004.
[12]. P. Papadimitratos and Z. Haas, Secure routing for mobile ad hoc networks, Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 2002.
[13]. R. Poovendran and L. Lazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks, Wireless Networks, vol. 13(1), pp. 27{59, 2007.
[14]. The Rice Monarch Project, Wireless and mobility extensions to ns-2(www.monarch.cs.cmu.edu/cmu-ns.html), 2007.
[15]. M. Vieira, C. Coelho Jr., D. da Silva Jr. and J. da Mata, Survey on wireless sensor network devices, Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation, vol. 1, pp. 537{544, 2003.
[16]. W. Wang and B. Bhargava, Visualization of wormholes in sensor networks, Proceedings of the ACM Workshop on Wireless Security, pp. 51{60, 2004.
[17]. A. Wood and J. Stankovic, Denial of service in sensor networks, IEEE Computer, vol. 35(10), pp. 54{62, 2002.
[18]. Y. Xu, J. Ford and F. Makedon, A variation on hop counting for geographic routing, Proceedings of the Third IEEE Workshop on Embedded Networked Sensors, 2006.
[19]. J. Zheng, Low rate wireless personal area networks: ns-2 simulator for 802.15.4 (release v1.1) (ees2cy.engr.ccny.cuny.edu/zheng/pub), 2007.