An Approach to Improve the Performance of WSN during Wormhole Attack using Promiscuous Mode

Parminder Singh
Chandigarh Engineering College
Landran, Chandigarh [INDIA]

Damandeep Kaur
Chandigarh Engineering College
Landran, Chandigarh [INDIA]

ABSTRACT

Due to dynamic topology and non-wired infrastructure of Wireless Sensor Networks (WSN), they are prone to attacks. Wormhole attack is one of the most popular and serious attack in WSNs. In Wormhole attack two or more malicious nodes makes a covert channel which attracts the traffic towards itself by depicting a low latency link and then start dropping and replaying packets in the multi-path route. This paper proposes promiscuous mode method to detect and isolate the malicious node during wormhole attack by using Ad-hoc on demand distance vector routing protocol (AODV) with omnidirectional antenna. This paper proposes that the nodes which are not participating in multi-path routing generates an alarm message during delay and then detects and isolate the malicious node from network.

Keywords:

Wormhole attack, Wireless Sensor Networks, Promiscuous mode, Ad-hoc on demand distance vector routing protocol, Malicious nodesifx

1. INTRODUCTION

Wireless sensor networks (WSN) are networks comprised of nodes known as sensor nodes, a transceiver end called sink and a gateway through which information is transferred. In WSN each node act as a routing path for another nodes in the network, follows multi hop multi path routing. Due to its dynamic topology, lack of reliability and wireless infrastructure WSN are prone to various attacks which leads to the tampering of wireless networks by attackers. WSN's are deployed in those areas in which quick feedback or control is required for e.g military personals and medical operations. In this paper a network layer attack known as wormhole attack in discussed. In Wormhole attack two colluding nodes makes a tunnel which attracts traffic towards itself by creating illusion that it is the shortest path with low latency and high bandwidth but in actual the packets are not forwarded to the actual destination rather they are relayed or dropped.

2. LITERATURE SURVEY

In [1] WSN is a network consisting of devices with low size and low complexity denoted as nodes. Information on wireless attack i.e., wormhole attack is discussed in [2], later on author [3] proposed the DELPHI method based on two parameters i.e., hop count and delay per hop indication based on assumption that rescheduling of packet is very high in wormhole attack during normal conditions furthermore, author [4] implied two step process i.e., to collect route path information from sender to receiver and embracing time stamps on request packets and then increasing hop count by 1, then calculating RTT between packet sent and received. [5] differentiates the behavior between the bottleneck and wormholes. Major differences in the use of routing protocol were discussed in [[5], [6]]. AODV was used in the DSR routing protocol. The routing protocol to be used is given by author [7] and proposed that how AODV protocol works better than other routing protocols. Trust based security model based on routing protocols were proposed in [[8], [9]] to detect intrusion arithmetical models which are used to identify wormhole attack. The link with very high frequency is checked with previously defined threshold coefficient value. If packet drop is greater than packet sent there there is presence of wormhole attack. Author [[10], [11]] discussed the impact of wormhole on localization proposed novel distance consistency based secure localization scheme and make to collect conflicting set of abnormalities of message exchange among neighbor locator only if there is no packet loss which is downside of this methodology. Graph theory approach was developed by author [12] for the prevention of wormhole attack with the use of location aware guard nodes using "local broadcast keys" which are encrypted and valid only between instant one hop neighbors. [[10], [11]] defined security extensions to OLSR to prevent generation of false messages. [13] used hash chain and digital signature whereas, [14] used signing OLSR packet with digital signature. In [15] cluster based detection technique is used assumes that MANET is made of cluster of nodes based on AODV protocol. [[8], [16]] proposed different data structures and algorithm worked on cross layer approach. Cluster head informs other nodes if they are expecting wormhole attack. Node at overlapping position act as a guard node can hear every packet send by source to destination and monitors packet route. Source informs guard node if it detect any malicious activity while sending packet to destination. [17] proposed the methodology based on beacon nodes. Implies easy and effective method to detect and locate wormhole by using Distributed Algorithm. Beacon node act as detector and sensor node participates for hop counting, base station controls start and end and estimate locations based on alarm messages sent from beacon nodes act like guard nodes of cluster based technique [18]. This paper proposes a wormhole detection and prevention scheme in WSN.

In this paper promiscuous mode has been proposed to detect the node which is malicious and then isolating it from the network when all the sensor nodes enters into promiscuous mode. The rest of the paper is organized as follows: Section 3 explains different types of network layer attacks in WSNs, Section 4 explain when two or more colluding nodes makes a tunnel and attract traffic towards it, Section 5 detects and isolate the malicious nodes from the network and enhance performance. Section 6 discusses numerical simulation and results obtained. At the last, Section 7 presents conclusions and make a projection on possible future research path.

3. ATTACKS

Most of the WSN's routing protocols are easy and straightforward. Because of this reason they are vulnerable to attacks. There are different types of network layer attacks in WSNs [19] which can be categorised as following:

(1) **False routing Information, Spoofed, Altered, or replayed routing information**: In this kind of attacks, the primary focus is on the routing protocol. In the routing protocols, the main thing to be dealt is with the routing information. Therefore, by just changing the routing information of the routing protocols through malicious code, it is possible to change the complete routing structure of the Wireless Sensor Network.

(2) **Sinkhole attacks**: When Sinkhole attacks are considered, the attacker's main aim is to tempt all the nodes in close proximity constructing a figurative sinkhole. For example, once the main coordinator is attacked with sinkhole all of the other nodes will also fall into the sinkhole following the main coordinator as the parent node at the centre. Sinkhole attacks naturally works by assembling the attacking node to appear like an ideal node particularly targeting the neighbouring nodes. the attacker builds a huge area of control, drawing the attention of all the traffic intended for a base station from nodes multi-hops away from the actual attacked node.

(3) **Sybil attacks**: In this kind of attacks the attacker infects a single node in the WSN network with a malevolent code masked with multiple identities. Then this single node operates as a major setback for the entire sensor network which immensely decreases the efficiency of the fault-tolerance schemes such as multipath routing, topology maintenance, disparity and distributed storage or routes which are supposed to be used by disjoint nodes but in reality could be used by only the attacker with multiple identities.

(4) **Wormholes**: In the wormhole attacks, a malevolent node excavates the messages it receives at one end of the network over a separate low-latency channel. Then it repeats messages at a different point in the sensor network. For example, when a source node is passing on data to a destination node then there can be a malicious node in between them which selectively forwards the data packets. The wormhole attacks usually engage two different and far-away malevolent nodes conspire to minimize their remoteness from each other by replaying packets next to an out-of-reach channel which is only available to the attacker.

4. WORMHOLE ATTACK

In this section the wormhole attacks modes are explained and classes while pointing to the impact of the wormhole attack.There are various severity attacks in WSN. Wormhole attack is considered as the most dangerous attack in wireless sensor network. It is a network layer attack. It is a dangerous attack because it is independent of MAC layer protocols and are immune to cryptographic techniques. In wormhole attack an attacker creates a link between the true node and the malevolent node, with which the malevolent node attracts the traffic towards it by a very high quality connection which is actually not the high quality connection but just an illusion. The colluder node then creates a covert channel with one or more nodes and then the malevolent node passes message to the another node through covert channel and the other node replay the packets in the network or start dropping selected packets. This behavior creates routing race condition.

4.1 Wormhole Attack Modes

Wormhole attacks can be launched using several modes, among these modes [20], i.e., mentioned as follows:

(1) **Wormhole using Encapsulation**: In this mode a malicious node at one part of the network and hears the RREQ packet. It tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the RREQ. The neighbours of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multihop paths. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away. Any routing protocol that uses the metric of shortest path to choose the best route is vulnerable to this mode of wormhole attack. This mode of the wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic information, nor do they need any special capabilities, such as a high speed wire line link or a high power source.

(2) **Wormhole using Out-of-Band Channel**: The second mode for this attack is the use of an out of band channel. This channel can be achieved, for example, by using a long range directional wireless link or a direct wired link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability.

(3) **Wormhole with High Power Transmission**: Another method is the use of high power transmission. In this mode, when a single malicious node gets a RREQ, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high-power broadcast rebroadcasts it towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a colluding node.

(4) **Wormhole using Packet Relay**: Wormhole using Packet Relay is another mode of the wormhole attack in which a malicious node relays packets between two distant nodes to convince them that they are neighbours. It can be launched by even one malicious node. Cooperation by a greater number of malicious nodes serves to expand the neighbour list of a victim node to several hops. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where A and B are not themselves within transmission range of each other. Intruder node X merely tunnels control traffic between A and B (and vice versa), without the modification presumed by the routing protocol.

(5) **Wormhole using Protocol Deviations**: A wormhole attack can also be done through protocol deviations. During the RREQ forwarding, the nodes typically back off for a random amount of time before forwarding reduce MAC layer collisions. A malicious node can create a wormhole by simply not complying with the protocol and broadcasting without backing off. The purpose is to let the request packet it forwards arrive first at the destination. The utility of organizing combinations of network attacks as graphs is well established. Network attack graphs represent a collection of possible penetration scenarios in a computer network. The graph can focus on the extent to which an adversary can penetrate a network to achieve a particular goal, given an initial set of capabilities. They represent not only specific attacks but categories of attacks. They can detect previously unseen attacks which have common features with attacks in graphs.

4.2 Wormhole Attack Classification

The classification of such an attack facilitates the design the attackers are visible on the route, we classify the wormholes into three types: closed, half open, and open

(1) **Open Wormhole attack**: In this type of wormhole, the attackers include themselves in the RREQ packet header following the route discovery procedure. Other nodes are aware

that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbors.

(2) **Closed Wormhole Attack**: The attackers do not modify the content of the packet, even the packet in a route discovery packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet.

(3) **Half open wormhole attack**: One side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure.

5. PROMISCUOUS MODE

To mitigate the WSN from wormhole attack, it has been proposed the method of categorizing nodes based upon their dynamically measured behavior, named as Promiscuous mode [21]. In this paper two extensions to Ad Hoc On Demand Routing protocol (AODV) are implemented in order to mitigate the effect of routing misbehavior during wormhole attack. The two extensions namely Watchdog and Path rater are implemented. Watchdog identifies misbehaving nodes and path rater helps routing protocol(AODV) to avoid these nodes. When node forward packet, the nodes watchdog verifies that the next node in the path also forward the packet. Watchdog does this by listening promiscuously to next nodes transmissions. If next node does not forwards the packet, then it is misbehaving node. Path rater use this knowledge of misbehaving nodes to choose the network path that is most reliable to deliver packets. In this paper during simulations the multihop route is established between the source and destination by the source node then the delay parameters are observed when the delay proceeds from the implied time then the watchdog became active and generate the promiscuous mode. In which all other sensor nodes except the path nodes enters into the promiscuous mode after getting alarm message from source node. The watchdog then detects the malicious node and isolate it from the network and pathrater then finds the other most reliable and suitable route to forward the packets from source to destination.

6. SIMULATION RESULTS

In this section, results of simulation of AODV with wormhole attack in WSN are shown. The simulations are done in $NS2$ simulator(version 2.34). In this simulation results on throughput and delay are defined. Parameters used in simulations are summarized as follows

(1) Queue length = 50

(2) Routing protocol=AODV

(3) Packet Size = 1000 bytes

(4) Traffic generator= CBR

(5) Antenna = Omnidirectional

(6) Propagation Ground = 2-way ground

(7) X = 800

(8) Y = 800

(9) Number of nodes = 20 802.11 standard wireless channel

After simulations the results are shown in Fig. 1 and Fig. 2..
From the Fig. 1 It is shown that the throughput before implementing promiscuous mode was very low during wormhole attack and after the methodology implementation the throughput became very high even in the presence of wormhole attack. Fig. 2represents the effect of delay on wireless sensor network during wormhole attack before and after implementing promiscuous mode. There is sharp rise in delay when wormhole attack was done before promiscuous mode implementation.

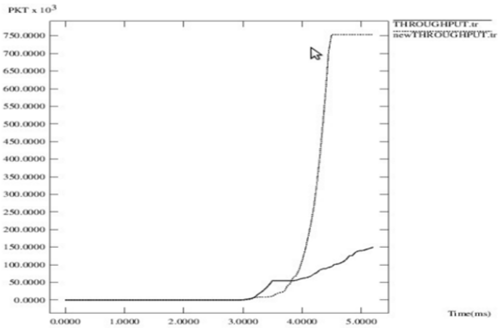

Fig. 1. New throughput vs old throughput graph

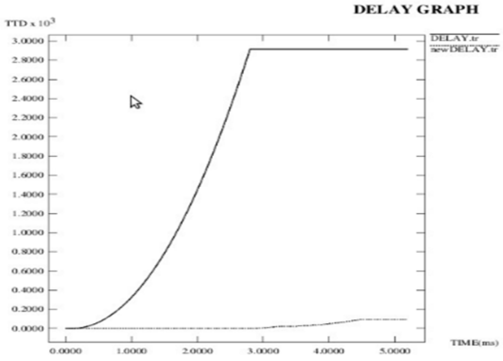

Fig. 2. New delay vs old delay graph

7. CONCLUSION AND FUTURE SCOPE

In this paper we introduced promiscuous mode methodology which works very efficiently in WSNs during wormhole attack. It not only prevents the degradation of the wireless network also helps in improving performance of wireless sensor networks. This methodology has not been proposed yet based on delay metrics. Analysis has been done through simulation to enhance performance of the proposed model in wireless multihop network. The simulation results have shown that in the presence of malicious nodes in ad hoc network. The performance of wireless network with AODV provided extensions with promiscuous mode mechanism is better than wireless network with simple AODV routing protocol in terms of throughput and end to end delay. Furthermore, it can help in putting some constraints on the network topology to design a robust network for such attacks, and in the design of new and more powerful attack countermeasures. In future more complex attacks can be simulated and comparison of their performances can be done to select the optimum method for prevention of attack from attackers point of view. Once selected, it will be tested with some of the proposed countermeasures and will help in the development of new attack prevention and detection schemes.

8. REFERENCES

[1] S. L. Malfa, “Wireless sensor networks,” 2010.

[2] M. Singh and R. Das, “A survey of different techniques for detection of wormhole attack in wireless sensor network.”

[3] H. S. Chiu and K.-S. Lui, “Delphi: wormhole detection mechanism for ad hoc wireless networks,” in *Wireless Pervasive Computing, 2006 1st International Symposium on.* IEEE, 2006, pp. 6–pp.

[4] F. Naït-Abdesselam, “Detecting and avoiding wormhole attacks in wireless ad hoc networks,” vol. 46, no. 4. IEEE, 2008, pp. 127–133.

[5] M. S. Sankaran, S. Poddar, P. S. Das, and S. Selvakumar, “A novel security model saw: Security against wormhole attack in wireless sensor networks,” in *Proceedings of International Conference on PDCN*, 2009.

[6] K. S. Win, “Analysis of detecting wormhole attack in wireless networks,” vol. 48, 2008, pp. 422–428.

[7] H. Singh and G. S. Josan, “Performance analysis of aodv & dsr routing protocols in wireless sensor networks,” 2012.

[8] E. M. Royer and C. E. Perkins, “Multicast operation of the ad-hoc on-demand distance vector routing protocol,” in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, 1999, pp. 207–218.

[9] D. B. Johnson, D. A. Maltz, J. Broch *et al.*, “Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks,” vol. 5, 2001, pp. 139–172.

[10] H. Chen, W. Lou, X. Sun, and Z. Wang, “A secure localization approach against wormhole attacks using distance consistency,” vol. 2010. Hindawi Publishing Corp., 2010, p. 8.

[11] H. Chen, W. Lou, and Z. Wang, “Conflicting-set-based wormhole attack resistant localization in wireless sensor networks,” in *Ubiquitous Intelligence and Computing*. Springer, 2009, pp. 296–309.

[12] L. Lazos and R. Poovendran, “Serloc: Secure range-independent localization for wireless sensor networks,” in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 21–30.

[13] A. Hafslund, A. Tønnesen, R. B. Rotvik, J. Andersson, and Ø. Kure, “Secure extension to the olsr protocol,” in *Proceedings of the OLSR Interop and Workshop, San Diego*, 2004.

[14] F. Hong, L. Hong, and C. Fu, “Secure olsr,” in *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*, vol. 1. IEEE, 2005, pp. 713–718.

[15] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, “An on-demand secure routing protocol resilient to byzantine failures,” in *Proceedings of the 1st ACM workshop on Wireless security*. ACM, 2002, pp. 21–30.

[16] R. Chaki and N. Chaki, “Idsx: a cluster based collaborative intrusion detection algorithm for mobile ad-hoc network,” in *Computer Information Systems and Industrial Management Applications, 2007. CISIM’07. 6th International Conference on*. IEEE, 2007, pp. 179–184.

[17] H. Ronghui, M. Guoqing, W. Chunlei, and F. Lan, “Detecting and locating wormhole attacks in wireless sensor networks using beacon nodes,” vol. 55. Citeseer, 2009.

[18] D. B. Roy, R. Chaki, and N. Chaki, “A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks,” 2010.

[19] D. krishna Chaitanya and G. Arindam, “Analysis of denial-of-service attacks on wireless sensor networks using simulation,” 2011.

[20] M. Azer, S. El-Kassas, and M. El-Soudani, “A full image of the wormhole attacks-towards introducing complex wormhole attacks in wireless ad hoc networks,” 2009.

[21] S. Marti, T. J. Giuli, K. Lai, M. Baker *et al.*, “Mitigating routing misbehavior in mobile ad hoc networks,” in *International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking*, vol. 6, no. 11, 2000, pp. 255–265.