International Journal of Engineering Technology and Applied Science
ISSN 2395-3853, Vol 1 Issue 2 April 2015

Wormhole Attack: Security threat over Sensor Network

Mithilesh Kumar[1], Prof. Praveen Kataria[2]
Department of Computer Science and Engineering, ASCT Bhopal[1]
Department of Computer Science and Engineering, ASCT Bhopal[2]
er.mithilesh.30@gmail.com[1], praveenkataria2008@gmail.com[2]

Abstract: Sensor Network (Mobile Ad hoc Network) bank on the cooperation of nodes to provide the basic operation such as routing. For commercial deployment of these networks, it is important that they consider adequate security measures. Selfish behaviour of ad hoc network nodes such as wormhole attack is a serious threat to Sensor Network as it cannot be detected easily could greatly degrade the performance of network. Such behaviour should be identified and isolated. This paper demonstrate various existing wormhole deduction mechanism and discus problem in existing mechanism.

Keywords: Mobile Ad hoc Network, Selfish, Malicious, ICMP

1. INTRODUCTION

An ad hoc network is a group of nodes that cooperate and promote packet for each other as a router. In wireless ad hoc network node can be mobile. Here it is possible that nodes may not be within the communication range of each other, such ad hoc networks extend the transmission range by multi hop packet promoting. So ad hoc network is the most suitable for the scenarios in which pre deployed infrastructure support are not available. For example emergency relief military operation and terrorism response. In ad hoc network nodes can be of four following types:

1. *Cooperative nodes:* Nodes which can comply with the standard at all times.
2. *Inactive nodes: A* node which consist both i.e. lazy nodes and constrained nodes (e.g. energy constrained or field strength constrained).
3. *Malicious nodes:* Nodes which drops packet with the intention to cause network attack.
4. *Selfish nodes:* Selfish nodes try to conserve their own resources as resources are very constrained in wireless network. these nodes may decide to save their resources by blocking data packets for other nodes:

This can be achieved in two ways:

1) Selfish node type 1: These nodes have participation correctly in routing function but they don`t forward data packets which they receive for other nodes; so data packets may be dropped rather than forwarded to their destination.

2) Selfish node type 2: These nodes also don`t participate correctly in the routing function by not advertising the available roots. In DSR, selfish nodes may drop all RREQ packet they receive or not forward RREP packet to some other destination.

Ad hoc network nodes can be either malicious or selfish because:

1) No central authority is there to authorize nodes.

2) Nodes can be easily added.

3) Under various circumstances most protocol silently assumes that all nodes are well behaving and cooperating to forward packets. When operating outside the library conditions, the probability of misbehaving nodes arises.

2. RELATED WORK

Marti et al. proposed two techniques that improve throughput in an ad hoc network in the presence of selfish and malicious nodes [1]. The watchdog method is used for each node to detect disobedient nodes in the network. When a node sends a packet to next hop, it tries to hear the packet sent by the next hop. If it hear that the packet is forwarded by next hop and the packet matches the previous packet that it has sent itself, it considers the next hop node behaves well. Otherwise it considers the next hop node is misbehaving. The pathrater uses the knowledge about misbehaving nodes acquired from watchdog to pick the route that is most likely to be reliable. Each node maintains a trust rating for every node. When watchdog detects misbehaving any node, the trust rating of the node is updated in negative way. When a node wants to choose a safe path to send packets, pathrater calculates a path metric by averaging the node ratings in the path.

Marti et al. implemented the solutions on DSR protocol using ns2 as simulation environment. The simulation result shows the throughput of the network could be increased by up to 27% in a network where packet drop attack happens. However routing overhead is also increases by up to 24%.

Table 1: Related work

S.N	Paper title	Proposed work	Deficiency &Future scope	Publication year
1	Securing DV-Hop localization against wormhole attack in wireless sensor networks	Severe impacts of the wormhole attack on the DV-Hop based localization in wireless sensor networks. To tackle this secure problem, They propose a label-based secure localization scheme to detect and defend against the wormhole attack for the DV-Hop localization process.	DV-Hop scheme consider network has no packet loss, and the transmission radii of all nodes are identical. But performance degraded when scenario with different types of nodes have different transmission radii.	2014
2	Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Test bed	Proposed a neighbour-probe-acknowledge algorithm (NPA) to detect wormhole attacks by identifying the occurrence of large steed (RTT). Proposed algorithm can achieve near 100% wormhole detection rate and zero false alarm rate both in light and heavy background traffic load scenarios	The parameters in NPA are static and not adaptive. So, in the future work on dynamic adjustment of algorithm parameters and routing algorithm that is resilient to wormhole attacks will be done.	2012
3	An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature	Used the scheme called multihop count analysis (MHA) with verification of legitimate nodes in network through its digital signature. Destination on node analyses the number of hop count of every path and selects the best path for replying. For checking the authentication of selected path, proposed methodology used verification of digital signature of all sending node by receiving node. If there is no malicious node between the paths from source to destination, then source node creates a path for secure data transfer.	Having higher overhead, transmission time.	2011
4	E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks	E2SIW, a routing protocol immune to wormhole attacks. E2SIW uses a simple location information and alternate route finding techniques to detect and prevent wormhole attack in ad hoc networks. E2SIW has a high detection rate and less energy requirements compared to the De Worm protocol And also contributed in reducing the overhead associated with the control packets.	Most of the work done so far in this topic assumes that the wormhole nodes are not capable of maliciously changing the data passing through them. But this may not always be the case.	2012
5	A Kind of Wormhole Attack Defence Strategy of WSN Based on Neighbour Nodes Verification	Wormhole attack defence strategy of WSN based on neighbour nodes verification. Under this strategy, when each normal node received control packet, it will monitor the packet to determine whether it comes from its normal neighbour nodes to avoid Wormhole attack effectively. Modelling and simulation of WSN based on OMNeT++ shows that the AODV added neighbour nodes verification successfully implement effective defence.	Increase handshaking time in neighbour node verification	2011

In [2], Jie Zhou1, Jiannong Cao, Jun Zhang1, Chisheng Zhang and Yao Yu study the impact of wormhole attacks on a real wireless mesh network test bed. Through theoretical analysis and comprehensive experiments, and find that when a path is

under the control of wormhole links, standard deviation of RTT (steed (RTT)) is a more efficient metric than per-hop RTT to identify wormhole attacks. Based on the observation, authors propose a neighbour-probe-acknowledge algorithm (NPA) to detect wormhole attacks by identifying the occurrence of large steed (RTT). The evaluation results on test bed shows that the proposed algorithm can achieve near 100% wormhole detection rate and zero false alarm rate both in light and heavy background traffic load scenarios. But, the parameters in NPA are not dynamic and adaptive. So, in the future work on dynamic adjustment of algorithm parameters and routing algorithm that is resilient to wormhole attacks will be done. Furthermore, there will a possibility of adopt the observation to design a new routing protocol which can resilient to inside attacks without triggering the detection frequently to further decrease the overhead.

In [3], Pallavi Sharma and Prof. Aditya Trivedi used the scheme called multi hop count analysis (MHA) with verification of legitimate nodes in network with the help of digital signature. Destination on node analysis the number of hop count of every path and select the best path for replying. For authentication of path, proposed methodology used verification of digital signature of all sending node by receiving node. If no malicious node present in the paths from source to destination, then source node establishes a path for secure data transfer.

In [4], Sanjay Kumar Dhurandher and Isaac Woungang proposed E2SIW, a routing protocol prone to wormhole attack. E2SIW use a location information and alternate route discovery techniques to detect and stop wormhole attack in ad hoc networks. E2SIW has a high detection rate and less energy requirements compared to the De Worm protocol And also contributed in reducing the overhead associated with the control packets. Almost all the work done so far on this topic shows that the wormhole nodes are not able of maliciously changing the data passing through them. But this may not always be the case. The design of the lessening results is that intelligent wicked nodes may exists is the need of the hour.

In [5], Jin Guo, Zhi-yong Lei gives wormhole attack defence policy of WSN based on neighbour nodes authentication. Under this policy, when each node receive control packet, it keep an eye on the packet to determine whether it comes from its neighbour node to prevent Wormhole attack effectively. Modelling and simulation of WSN based on OMNeT++ shows that the AODV added neighbour nodes endorsement successfully execute effective defence.

A Defence against Wormhole Attacks in Wireless Networks: As mobile ad hoc network applications are structured, security appears as a basic requirement. The author introduces the wormhole attack, a very harmful attack in ad hoc network that is the most difficult to defend against the wormhole attack. Wormhole attack may arise although if the attacker has not tolerated any hosts and if all communication provide authenticity and confidentiality. Author demonstrated the performance analysis of a novel, efficient protocol, called TIK, Particularly, a node needs to perform only between 3 to 6 hash function evaluation per time interval to maintain key information up to date for itself, and nearly 30 hash functions for each received packet. When used in conjunction with precise timestamps and tight clock synchronization, wormhole attack can be prevented by TIK that cause the signal to travel a distance longer than the nominal range of the radio [9] and wireless MAN technology could be adequately time-synchronized using either GPS or LORAN-C radio signals.

3. Sensor Network

Sensor Network networks are temporary infrastructure less communication network. They include a group of wireless mobile nodes, which interact with each other without the use of any stable network infrastructure. Sensor Network networks are suitable for applications where the installation of an infrastructure is not possible because the infrastructure too expensive or too vulnerable or the power is too volatile, or the infrastructure was destroyed, as in the military, rescue and pointed mining and in conference [10].

Due to their limited properties ad hoc networks are open to to security attacks [11] in comparison to wired network. For instance, make the employment scenarios, the functionality requirements, and the limited ability of these types of networks; they are vulnerable to a large group of attacks. In this paper we focus on detecting and locating wormhole attacks. The wormhole attack is difficult attack in Mobile Ad Hoc Networks. In a wormhole attack intruders trace packets at one place, they lead to another packet encapsulation or by out-of-band channels, and sends it back into power [12, 13]. The wormhole attacker can extensively interfere with the communication over the network through the implementation of targeted denial of service (DoS) attacks. These DoS attacks are difficult to detect statistically, whether the attackers drop packets at random, or it may interfere greatly if the attacker to delete certain types of frames and / or critical times to them drop target. The wormhole attackers attain the means to analyse traffic through the acquirement of control of a link in the network and the influence of the amount of traffic that goes through them to perform, and provide uncertainty in situational awareness by distortion of the network topology.

4. WORM HOLE ATTACK

The wormhole attack is a severe threat to Sensor Network as it cannot be detected easily. In wormhole attack (figure 1), two

attacker nodes connect together. One attacker node get packets at one point and "tunnels" them to another attacker node through a confidential connection, and replays them into the network. The wormhole puts the attacker nodes in a very dominant position compared to other nodes in the network. In the routing protocols such as AODV, the attacker tunnels each route request packets to another attacker that is near to destination node. When the neighbours of the destination hear these RREQ, they will again broadcast and then discard all other received RREQs in the same route discovery process. This attack stops other paths instead of the wormhole from being discovered, and thus makes a permanent Denial-of-Service attack by dropping all the packets, or discarding selectively or modifying certain packets as needed [14].

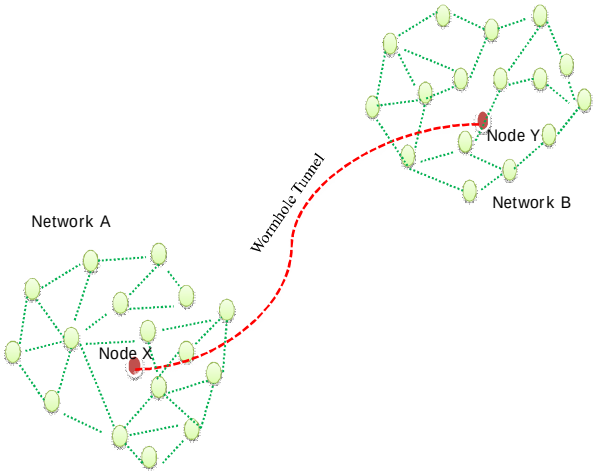

FIG.1. WARM HOLES

5. ORGANIZATION OF WORMHOLE ATTACKS

Organization of wormhole based upon visibility of attacker on the path can be grouped into three types: closed, half open, and open. As show in figure 1 consider two nodes behave like worm hole stating point (WH_S) and worm hole ending point (WH_E), represent the malicious nodes and all other node entitle with NN_i treated as good node .The nodes between the tunnel are the nodes which are on the path but not visible to Source and Destination as they are in a wormhole. In closed wormhole attack tunnel start from source and include the entire intermediate node and where as in open wormhole tunnel start from source but not include the entire entire intermediate node. In figure 2, WH_S and WH_E tunnel the neighbour find beacons from Source to Destination and vice versa, for this reason Source and Destination assume that they are direct neighbours of each other. In figure 3, WH_S is a neighbour of Source node and it connects its beacons with WH_N to Destination, Only one malicious node is visible to Source and Destination node. In an open wormhole, both attackers are visible to Source and Destination node as shown in figure 4 [15].

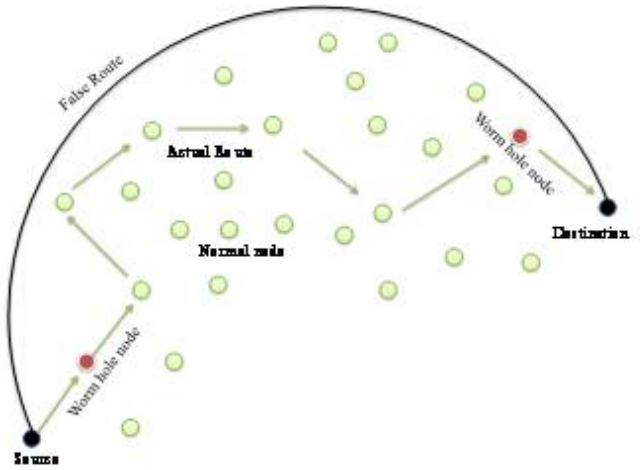

Fig. 2. Collision of Warm hole

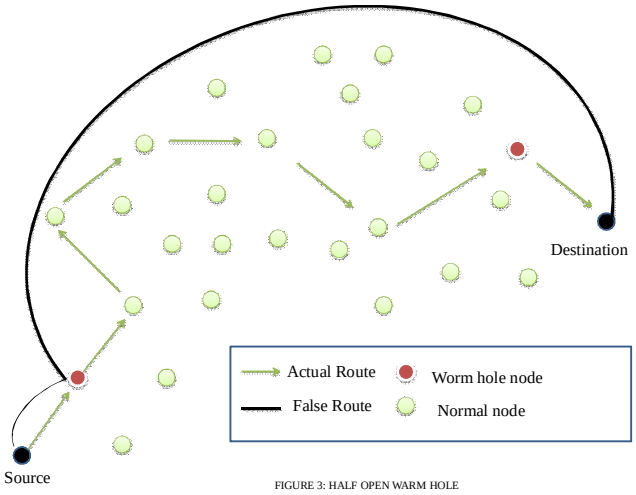

FIGURE 3: HALF OPEN WARM HOLE

Fig.3. Half Open Warm Hole

6. CONCLUSION AND FUTURE WORK

Sensor Network has properties that increase their susceptibility to attacks. We have presented and discussed various issues such as security attacks and threats that can cause susceptibility in Sensor Network.

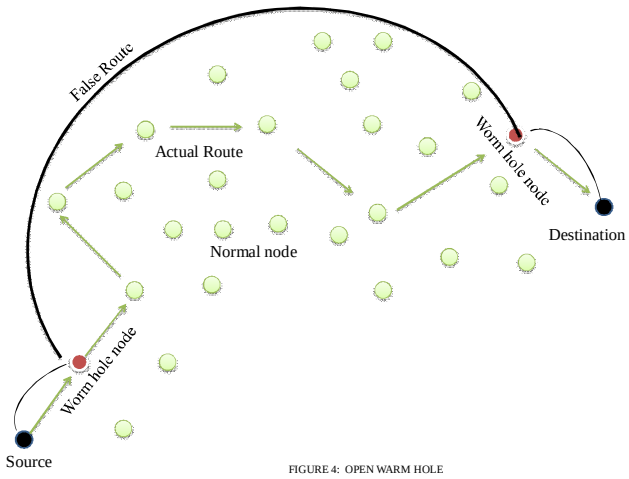

Fig. 4. Open WARM HOLE

With authentic guaranteed, secure routing can be successful in Sensor Network & the malicious nodes can be identified and excluded from routing. In future we plan to continue our work in field of securing Sensor Network & present more security probabilistic routing techniques for Sensor Network that avoid worm hole attack by apply special case of Bayesian probabilistic approach for node authentication as dumpster Shafer belief theory of probability.

REFERENCES

[1] Honglong Chena,b, Wei Louc,d, Zhi Wang, Junfeng Wue, Zhibo Wang, Aihua Xia "Securing DV-Hop localization against wormhole attacks in wireless sensor networks", Volume 16, Part A *Elsevier*, pp. 22 – 35, January 2015.

[2] Jie Zhou1, Jiannong Cao, Jun Zhang1, Chisheng Zhang and Yao Yu, "Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Test bed", *26th IEEE International Conference on Advanced Information Networking and Applications*, 2012.

[3] Pallavi Sharma, Prof. Aditya Trivedi "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", *IEEE*, 2011.

[4] Sanjay Kumar Dhurandher and Isaac Woungang "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks", 26th International Conference on Advanced Information Networking and Applications Workshops in *IEEE*, 2012.

[5] Jin Guo, Zhi-yong Lei "A Kind of Wormhole Attack Defense Strategy ofWSN Based on Neighbor Nodes Verification", *IEEE* 2011.

[6] RFC 792, Internet Control Message Protocol.

[7] D. Johnson, D. A. Maltz, and J. Broch. "The Dynamic Source Routing Protocol for Mobile Ad hoc Networs (Internet-Draft). Mobile Ad-hoc Network (MANET)", Working Group *IETF*, October 1999.

[8] M. Tamer Rafaei, Vivek Srivastav, Luiz DaSilva, "A Reputation-based Mechanism for Isolating Selfish Nodes in Adhoc Networks," *Proceedings of the Second Annual Internatinal Conference on Mobileand Ubiquitous Systems:Networking and Services* MobiQuitous'05.

[9] Katrin Hoeper, Guang Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks," *Signals and Communication Technology*, pp. 65-82, 2007.

[10] Hu. Yih-Chun and A. Perrig, "A Survey of secure wireless ad hoc routing," Security & Privacy, *IEEE*, vol. 2, pp. 28–39, 2004.

[11] Fei Shi, Jaejong Baek, Jooseok Song, Weijie Liu. "A novel scheme to prevent MAC layer misbehavior in IEEE 802.11 ad hoc networks", *Journal of Telecommunication Systems (JTS) Springer*, (DOI) 10.1007/s11235-011-9552-y, 2011.

[12] I. Khalil, S. Bagchi, and N. B. Shroff, "LiteWorp: A Lightweight Countermeasure for the Wormhole Attack in Multi hop Wireless Networks", in *Proceedings of the 2005 IEEE International Conference on Dependable Systems and Networks*, Yokohama, Japan, June 28-July 1, 2005.

[13] Y. C. Hu, A. Perrig, and D. B. Johnson, "Wormhole Attacks in Wireless Networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp.370-380, 2006.

[14] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks" citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110.609

[15] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks: Research articles," *Wireless Communication Mobile Computing*, vol. 6, no. 4, pp. 483–503, 2006.