Detection and Isolation of Worm Hole attach as Selfish Node in Mobile Ad-Hoc Network

[*]Harish Indriya, [**]G.S. Darbar
[*,**]Department of Computer Science and Engineering, Vinayak Polytechnic College, Nagpur.
[*]indriyaharish1@yahoo.com, [**]darbar.ghanshyam@yahoo.com

Abstract— Mobile ad hoc Netwo is bank on the cooperation of nodes to provide the basic operation like routing. For industrial deployment of those networks, it's important that they consider adequate security measures. Selfish behavior of ad hoc network nodes like wormhole attack could be a serious threat to mobile ad-hoc network because it cannot be detected easily may greatly degrade the performance of network. Such behavior ought to be known and isolated. This paper uses demonstrate totally different existing worm hole deduction mechanism and discus downside in existing mechanism.

Keywords— Mobile ad hoc Network, Selfish, Malicious, ICMP

1. INTRODUCTION

An ad hoc network may be a group of nodes that cooperates and forward packet for every other as a router. In wireless ad hoc network node can be mobile. Here it's attainable that nodes might not be inside the communication range of every other, such ad hoc networks extend the transmission range by multi hop packet forwarding. That's a reason for ad hoc network being similar temperament for the eventualities during which are deployed infrastructure support don't seem to be compatible. For example emergency relief operation and terrorist act response. In ad hoc network nodes may be of 4 following types:

1. Cooperative nodes: Nodes that accommodates the standard at all times.

2. Inactive nodes: Nodes that embrace lazy nodes and constrained nodes (e.g. energy strained or field strength constrained).

3. Malicious nodes: Nodes that drops packet with the intention to cause network attack.

4. Selfish nodes: selfish nodes attempt to save their own resources since resources are terribly strained in wireless network. Selfish nodes might conceive to conserve their resources by not forwarding information packets for alternative nodes:

This can be achieved in 2 ways:

1) Selfish node type 1: These nodes participate correctly in routing function however not forward information packets they receive for alternative nodes; thus information packets could also be dropped instead of forwarded to their destination.

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

In ad hoc network nodes can be malicious or selfish because:

1) No central authority is there to authorize nodes.

2) Nodes may be simply additional.

3) Beneath a large verity of circumstances most protocol silently assumes that each one node is well behaving and cooperating to forward packets. Once operative outside the library conditions, the chance of misbehaving nodes arises.

2. MOBILE ADHOC NETWORK

Mobile ad-hoc networks are temporary infrastructure less communication network. They incorporate a group of wireless mobile nodes, that act with one another without the employment of any stable network infrastructure. Mobile ad-hoc networks are appropriate for applications wherever the installation of an infrastructure isn't attainable as a result of the infrastructure too valuable or too vulnerable or the power is just too volatile, or the infrastructure was destroyed, as in the military, rescue and pointed mining and in conference [10].

Because of their exclusive properties ad hoc networks are vulnerable to security attacks [11] compared to wired network. For example, create the use eventualities, the practicality necessities, and also the restricted ability of those types of networks; they're at risk of an oversized group of attacks. During this paper we have a tendency to specialize in detecting and locating wormhole attacks. The wormhole attack is difficult attack in Mobile ad hoc Networks. During a wormhole attack intruders record packets at one place, they cause another packet encapsulation or by out-of-band channels, and sends it back to power [12, 13]. The wormhole attacker will significantly interfere with the communication over the network through the implementation of targeted denial of service (DoS) attacks. These DoS attacks are troublesome to detect statistically, whether or not the attackers drop packets at random, or it should interfere greatly if the attacker to delete certain varieties of frames and / or essential times to them drop target. The hole attackers acquire the means that to analyse traffic through the acquisition of management of a link in the network and also the influence of the number of traffic that goes through them to perform, and supply uncertainty in situational awareness by distortion of the network topology.

3. WORM HOLE ATTACK

The wormhole attack is a serious threat to mobile ad-hoc network because it cannot be detected simply. in an exceedingly wormhole attack (figure 1), two attacker nodes be part of along. One attacker node receives packets at one purpose and “tunnels" them to a different attacker node via a non-public network connection, then replays them into the network. The wormhole puts the attacker nodes in a very powerful position compared to alternative nodes within the network. In the reactive routing protocols like AODV, the attackers will tunnel every route request packets to a different attacker that's near to destination node. Once the neighbours of the destination hear this RREQ, they'll rebroadcast this RREQ then discard all alternative received RREQs within the same route discovery method. This kind of attack prevents other routes rather than the wormhole from being discovered, and so creates a permanent Denial-of-Service attack by dropping all the information, or by selection discarding or modifying bound packets as required [14].

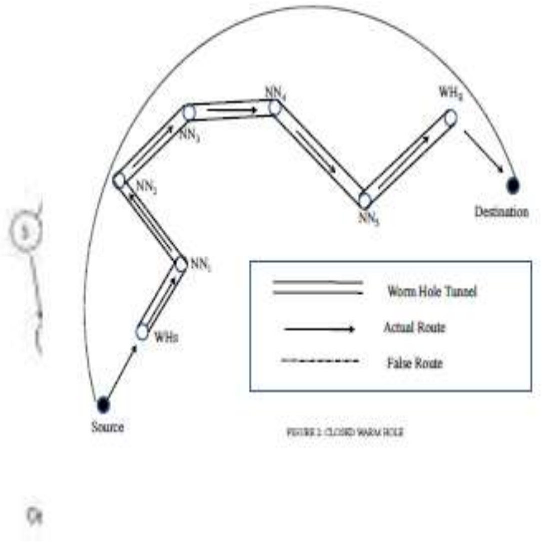

Fig. 1 Worm hole.

4. ORGANIZATION OF WORMHOLE ATTACKS

Organization of wormhole depend on visibility of attacker on the route, wormholes is classified into three types: closed, half open, and open. As show in figure 1 contemplate two nodes behave like worm hole stating point (WHS) and worm hole ending point (WHE), represent the malicious nodes and every one alternative node entitle with NNi treated as good node .The nodes between the pipe are the nodes which are on the path however invisible to source and Destination as a result of they're in a very wormhole. In closed wormhole attack tunnel begin from source and embody the entire intermediate node and wherever as in open wormhole tunnel begin from source however not embody the complete intermediate node. In figure 2, WHS and WHE tunnel the neighbour discovery beacons from source to Destination and the other way around, for this reason source and Destination assume that they're direct neighbours to every alternative. In figure 3, WHS is a neighbour of source node and it tunnels its beacons through WHN to Destination, only one malicious node is visible to source and Destination node. In an open wormhole, each attackers are visible to source and Destination node as shown in figure four [15].

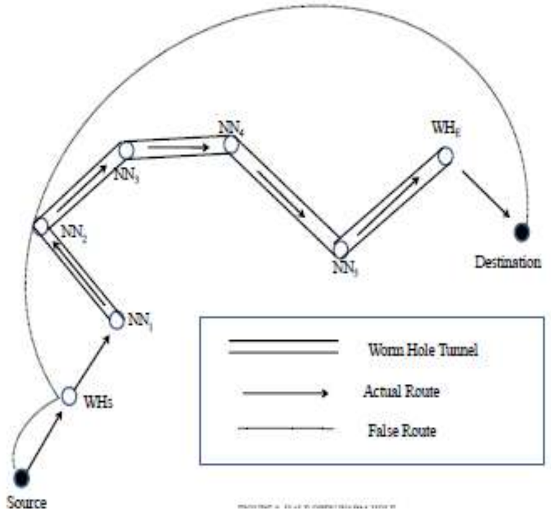

Fig. 3 Half open Worm hole

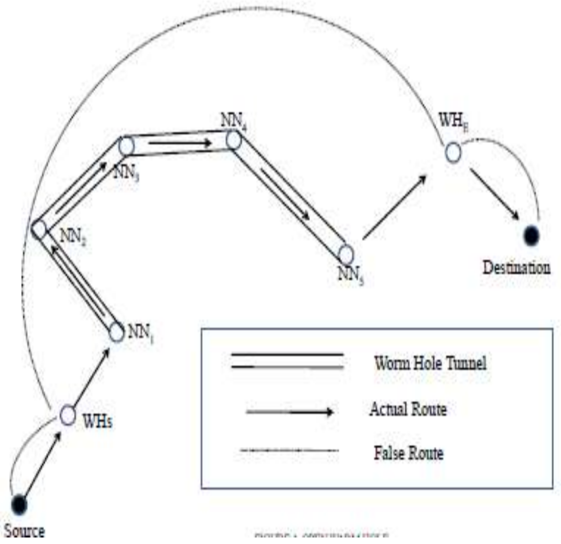

Fig. 4 Open Worm hole

5. RELATED WORK

In [1] this paper projected 2 techniques that improve throughput in an advertisement hoc network within the presence of selfish and malicious nodes [1]. The watchdog technique is employed for each node to sight misbehaving nodes within the network. When a node sends a packet to next hop, it tries to catch the packet forwarded by next hop. If it hears that the packet is forwarded by next hop and also the packet matches the previous packet that it's sent itself, it considers ensuing hop node behaves well. Otherwise it considers the next hop node is misbehaving. The pathrater uses the information about misbehaving nodes acquired from watchdog to select the route that's possibly to be reliable. Each node maintains a trust rating for each alternative node. When watchdog detects a node is misbehaving, the trust rating of the node is updated in negative means. once a node desires to choose a secure route to send packets, pathrater calculates a path metric by averaging the node ratings within the path.

Marti et al. enforced the solutions on DSR protocol using ns2 as simulation atmosphere. The simulation result shows the throughput of the network might be redoubled by up to 27th in a network wherever packet drop attack happens. However routing overhead is additionally increased by up to pure gold.

In [2], authors study the impact of wormhole attacks on a real wireless mesh network testbed. Through theoretical analysis and comprehensive experiments, and notice that when a path is underneath the management of wormhole links, standard deviation of RTT (stdev (RTT)) may be a a lot of economical metric than per-hop RTT to spot wormhole attacks. Based on the observation, authors propose a neighbourprobe- acknowledge algorithm (NPA) to sight wormhole attacks by characteristic the incidence of enormous stdev(RTT). The analysis results on testbed show that the projected algorithm are able to do close to 100 percent wormhole detection rate and zero false alarm rate each in light-weight and serious background traffic load eventualities. But, the parameters in NPA are static and not reconciling. So, within the future work on dynamic adjustment of formula parameters and routing algorithm that's resilient to wormhole attacks are done. Furthermore, there'll a chance of adopt the observation to style a brand new routing protocol which might resilient to inside attacks while not triggering the detection frequently to any decrease the overhead.

In [3] authors used the scheme referred to as multi hop count analysis (MHA) with verification of legitimate nodes in network through its digital signature. Destination on node analyses the number of hop count of each path and selects the simplest path for replying. For checking the authentication of elect path, projected methodology used verification of digital signature of all causing node by receiving node. If there's no malicious node between the methods from source to destination, then source node creates a path for secure information transfer.

In [4] authors projected E2SIW, a routing protocol immune to wormhole attacks. E2SIW uses an easy location information and alternate route finding techniques to sight and prevent wormhole attack in ad hoc networks. E2SIW has a high detection rate and fewer energy needs compared to the First State Worm protocol and additionally contributed in reducing the overhead related to the management packets. Most of the work done to this point during this topic assumes that the wormhole nodes don't seem to be capable of maliciously dynamical the data passing through them. However this could not forever be the case. the look of the mitigation solutions keeping in mind that intelligent malicious nodes might exists is that the need of the hour.

In [5] wormhole attack defence strategy of WSN primarily based on neighbour nodes verification. under this strategy, when every traditional node received control packet, it will monitor the packet to work out whether or not it comes from its traditional neighbour nodes to avoid wormhole attack effectively. Modelling and simulation of WSN primarily based on OMNeT++ shows that the AODV further neighbor nodes verification with success implement effective defence. A Defence against wormhole Attacks in Wireless Networks: As mobile ad hoc network applications are structured, security seems as a central demand. The author introduces the wormhole attack, a severe attack in ad hoc networks that's largely difficult to defend against. The wormhole attack is feasible even though the attacker has not compromised any hosts and even though all communication provides authenticity and confidentiality. Author presented the look and performance analysis of a novel, efficient protocol, called TIK, specially, a node needs to perform only between three and 6 hash perform evaluations per time interval to take care of up-to-date key information for itself, and roughly thirty hash functions for each received packet. Once utilized in conjunction with precise timestamps and tight clock synchronization, TIK can prevent wormhole attacks that cause the signal to travel a distance longer than the nominal vary of the radio [9]. And wireless MAN technology may well be sufficiently time-synchronized using either GPS or LORAN-C radio signals.

6. CONCLUSION AND FUTURE WORK

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. We've given and discussed numerous problems like security attacks and threats which will cause vulnerability in MANETs. With authenticated assured, secure routing will be successful in MANETs & the malicious nodes will be identified and excluded from routing. In future we have a tendency to plan to continue our work in field of securing MANETs & present additional security probabilistic routing techniques for MANETs that avoid worm hole attack.

REFERENCES

[1] S. Marti et al. "Mitigating routing misbehavior in mobile ad hoc networks," Proceedings of Sixth Annual IEEE/ACM Intl. Conference on Mobile Computing and Networking , April 2009,PP. 225-256.

[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" in 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" in IEEE ,2011

[4] Sanjay Kumar Dhurandher and Isaac Woungang "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks" in 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" in 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] [12] I. Khalil, S. Bagchi, and N. B. Shroff, LiteWorp: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, in Proceedings of the 2005 IEEE International Conference on Dependable Systems and Networks (DSN 2005), 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.