A Review Paper on Wormhole Attack Detection in Wireless Sensor Networks

Shailani, Dr. Sukhvir Singh

***Abstract*— In mobile ad hoc networks, data transmission is performed within an untrusted wireless environment. A Wireless Networks are more vulnerable to different types of attack than wired Network.Various kinds of attack have been identified and corresponding has been proposed. Wormhole attack is one of the serious are attacks which forms a serious threat in the networks, especially get against many ad hoc wireless routing protocols and location- based wireless security system. In which traffic is forwarded and replayed from one location to another through the wormole tunnel without compromising any cryptographic techniques over the network. Thus, it is challenging to defend against this attack. The wormhole attack is very powerful and preventing the attack has proven to be difficult.We identify two types of wormhole attacks. In first type, malicious nodes do not take part in finding routes, meaning that, other nodes in the network does not know their existence. In second type, malicious nodes do create route advertisements and other nodes are aware of the existence of malicious nodes, but they do not know that these are the malicious nodes. Many researchers have proposed detection mechanisms for the first type. Existing some solutions to detect wormhole attacks require special hardware or strict synchronized clocks or long processing time. Moreover, some solutions can not even locate the wormhole.**

***Index Terms*—Ad hoc network, Wormhole attack, Nodes**

I. Introduction

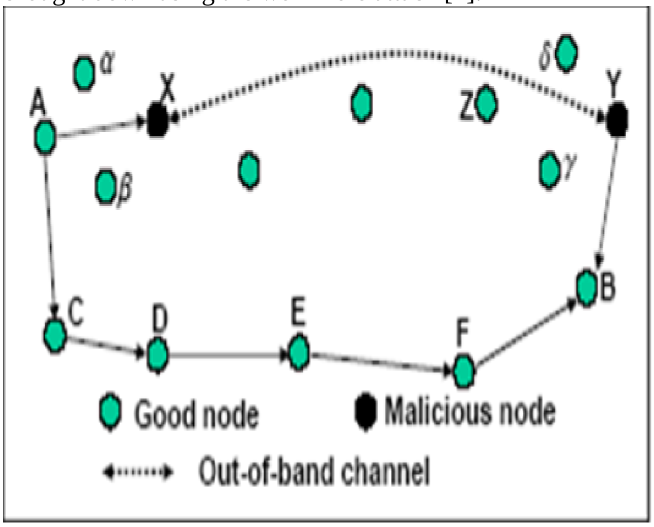
Ad Hoc network are popular and useful because of infrastructure less nature. Ad-hoc Network is a group of nodes, in which individual nodes corporate by forwarding packets for each other to allow nodes to communicate beyond direct transmission range. Security is primarily concern in order to provide protected communication between mobile nodes in hostile environments. A large number of routing protocols for MANET has been proposed to enable quick and efficient network creation and restructuring. MANET has several challenges. They include- 1) Multicast routing :- Designing of multicast routing protocol for a constantly changing MANET environment. 2) Power consumption :- Since the nodes in MANET network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements. 3) Dynamic Topology : - The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time. 4) Quality of service (QOS) :- Providing constant QoS for different multimedia services in frequently changing environment. 5) Security :- The ultimate goal of the security solutions for MANET is to provide a framework covering availability, confidentially, integrity, and authentication to insure the services to the mobile user.

Shailani, M.Tech, CSE, N.C. College of Engineering, Panipat-132103, Haryana, India.

Dr. Sukhvir Singh, Associate Professor, CSE, N.C. College of Engineering, Panipat-132103, Haryana, India.

I. WORMHOLE ATTACK

Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another [5]. A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network. Consider Figure 1[7] in which node A sends RREQ to node B , and nodes X and Y are malicious nodes having an out-of-band channel between them . Node X "tunnels" the RREQ to Y , which is legitimate neighbor of B. B gets two RREQ – A-X-Y-B and A-C-D-E-F-B. The first route is shorter and faster then the second, and chosen by B. Since the transmission between two nodes has rely on relay nodes, many routing protocols have been proposed for ad hoc network. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes as shown in Figure 1. The resulting route through the wormhole may have lower hop count than normal routes. In with this leverage, attackers using wormhole can easily manipulate the routing priority in MANET to perform eavesdropping, packet modification or from a DOS attack . The entire routing system in MANET can even be brought down using the wormhole attack [7].



There are different types of techniques to detect wormhole attack on network. Mahajn et al. [5] consider several terms for measuring the capacity of nodes involved in wormhole attack. These are defined below:-

1) Strength: - It is amount of traffic attracted by the false link advertised by the colluding nodes.

2) Length: - Larger the difference between the actual path and the advertise path , more anomalies can be observed in the network.
3) Attraction: - This term refers to the decrease in the path length offered by the wormhole. If the attraction is small then the small improvement in normal path may reduce its strength.
4) Robustness:-The robustness of a wormhole refers to the ability of the wormhole to persist without significant decrease in the strength even in the presence of minor topology changes in the network. Besides these, the packet delivery ratio which is the number of packet of delivered divided by the total number of packets dispatched forms a basic metric to quantify the impact.

II. PREVENTION OF WORMHOLE ATTACK

Choi al et.[16] considered that all the nodes will monitor the behavior of its neighbors. Each node will send RREQ messages to destination. If source does not receive the RREP message within a define time, it detects the presence of wormhole and adds the route to its wormhole list. Each node maintains a neighbor node table which contains a RREQ sequence no. , neighbor node ID, sending time and receiving time of the RREQ and count. The source node sets the Wormhole Prevention Timer (WPT) after sending RREQ packet and wait until it overhears its neighbors retransmission. The maximum amount of time required for a packet to travel one hop distance is WPT/2. Therefore, the delay per hop value must not exceed estimated WPT. However, the proposed method does not fully support DSR as it is based on end-to-end signature authentication of routing packets. Mahajan et al. [5] proposed some proposals to detect wormhole attacks like: 1) The abrupt decrease in the path lengths can be used as a possible symptom of the wormhole attack. 2) With the available advertised path information, if the end-to-end path delay for a path cannot be explained by the sum of hop delays of the hops present on its advertised path, existence of wormhole can be suspected. 3) Some of the paths may not follow the advertised false link, yet they may use some nodes involved in the wormhole attack. This will lead to an increase in hop delay due to wormhole traffic and subsequently an increase in end-to-end delay on the path. An abrupt increase in the end-to-end delay and the hop queuing delay values that cannot be explained by the traffic supposedly flowing through these nodes can lead us to suspect the presence of wormhole. “Time of Flight” is a technique used for prevention of wormhole attacks. It calculates the roundtrip journey time of a message; the acknowledgement estimate the distance between the nodes based on this time, and conclude whether the calculated distance is within the maximum possible communication range. If there is a wormhole attacker involved, packets end up travelling further, and thus cannot be returned within the short time.

III. WORMHOLE ATTACK DETECTION TECHNIQUES

In this section, we review related works in the literature which discuss proposed wormhole attack defenses.
Packet leash [2] is a mechanism for detecting and thus defending against wormhole attacks. A leash is any information on that is added to a packet designed to restrict the packet‟s maximum allowed transmission distance. The mechanism proposes two types of leashes for this purpose: Geographic and Temporal. In Geographic Leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender
handoff by increasing the probability of its operation in predictive mode. It is done by using initiation handoff link. Event indication is used in it which helps in forwarding the packet to new access router without waiting for the announcement of attachment from FMIPv6. MIPv6 has long handover delay for real time application like Voice Over IP (VOIP). FMIPv6 reduces the handover delay by using link layer triggers to perform address acquisition before L2 handover. The packet loss is prevented by creating a tunnel between Previous Access Router (PAR) and New Access Router (NAR).
The access router discovery is reduced with the help of MIH [26-27]. In [28-29], the schemes reduce the effect of duplicate address detection (DAD). MIH defines a network function of the network entity called MIH-F for communicating upper and lower layer through Service Access Point (SAP). MIH-F is used to detect changes in the proportion of link layer, to control link proportion cost to handover and switching between links.We collected the neighbor’s information before the handover triggers for handover delay and use MIH for links ups and downs. The handover latency (ms) of FMIPv6 is compared with MIH-FMIPv6 with respect to wireless link delay which shows that it reduces the handover latency, buffer size and critical size in handover.

and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through wormhole or not. In Temporal Leashes, the sender appends the sending time to the packet and the receiving node computes a travelling distance of that packet assuming propagation at the speed of the light and using the difference between packet sending time and packet receiving time. This solution requires a fine grained synchronization among all nodes. Unlike packet Leash, Capkun et al. [1] presented SECTOR, which does not require any lock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD). Node A estimates the distance to another node B in its Transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of Flight, A detects whether or not B is a neighbor or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash is Shalini Jain et al. [10] presented a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. With the help of extensive simulations, demonstrate that scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network establishment and operation phase. The Chiu et al. [4] proposed the Hop Count delay per hop indication [DELPHI] method. Both the hop count and delay per hop indication (DELPHI) are monitored for wormhole detection here. The elementary assumption [4] is that, the rescheduling of a packet under normal condition for propagating one hop is very high in wormhole attack as the actual path between the nodes is longer than the advertised path. Like [4], the proposed methodology in [8] for wormhole detection is also a two step process. In the first place, from a set of dislodge paths from sender to receiver, the route path information are collected. Each sender embraces a timestamp on a special DREQ packet and sigh it before sending it to the receiver. Each node upon receiving the packet for the first time will include its node ID and increase the hop count by 1 and discards the packet next time onwards. The DREP packets will be sent by the receiver for each dislodge path received by it. For three times this course of action is carried out and the shortest delay and hop count information is selected for wormhole detection. In the second phase, the round trip time (RTT) is taken by calculating the time discrepancy between the packet it had sent to its neighbor and the reply received by it. The delay per hop value (DPH) is calculated as RTT/2h, where h is hop count to the particular neighbor. A smaller h will have smaller RTT in normal conditions. But under wormhole attack a smaller hop count is having large RTT. If one DPH value for node X exceeds the consecutive one by some threshold, then the path through node X to all other paths with DPH values larger than it is treated under wormhole attack [8]. The M.A. Gorlatva at el. [9] proposed another technique for the detection of wormhole attack, which is Hello Message Timing Interval Procedure. Here revealing of wormhole nodes is done due to the Hello control messages. As a metric of compliance with the Optimized Link State Routing (OLSR) protocol, the percentage of HELLO Message Timing Intervals (HMTIs) that fall within a range is surrounded by the amount of jitter. A range R=[T-δ, T + δ] is defined. If an HMTI is in this range R, it is considered to be legitimate; otherwise it is out-of-protocol. An inferior evaluation test is done whenever the Hello Message Timing Interval packet behavior is doubtful. On the contrarily, a weakly performing node is associated with it a relatively large number of retry packets, which would not be the case with an attacking node. In this way, the problem of false positive alarms is resolved [9]. Both in Saw [12] and DaW [13] similar propositions are made. Only differences are in the selection of routing protocols. In references [12] AODV protocol was followed while in [13] DSR routing protocol was followed. In both of these papers, trust based security models have been proposed and used to detect intrusion. Statistical Methods have been proposed to detect attacks. If any link is found to be suspicious, then a available trust information is used to detect whether the link is wormhole. In the trust model used, nodes monitor neighbor based on their packet drop pattern and not on the measure of number of drops. Karl Peason‟s formula for correction coefficient is used to find the pattern of the drops. In [13] another algorithm for detecting the presence of wormhole in the network has been proposed. After sending RREQ the source waits for the RREP. The source receives RREP coming from different routes. The link varies with high frequency is checked using the following expression: Pi= ni /N, for all Ii Pmax = max (Pi), where R is the set of all obtained routes, Ii is the ith link, ni is the number of times that Ii appears in R, N is the total number of links in R, and Pi is the relative frequency that Ii appears in R. If $Pmax > Pthreshold$, check the trust information available in the RREP of that route. If the value of correlation coefficient for packets dropped to that sent is greater than the pre-set threshold t, then the node is malicious, inform the operator else continue with routing process.

Khalil et al [14] propose a protocol for wormhole attack discovery in static networks they call LiteWorp. In LiteWorp, once deployed, nodes obtain full two-hop routing information from their neighbors. While in a standard ad hoc routing protocol nodes usually keep track of who their neighbors are, in LiteWorp they also know who the neighbors‟ neighbors are, - they can take advantage of two-hop, rather than one-hop, neighbor information. This information can be exploited to detect wormhole attacks. After authentication, nodes do not accept messages from those they did not originally register as neighbors. Also, nodes observe their neighbors‟ behavior to determine whether data packets are being properly forwarder by the neighbor, - a so-called „watchdog‟ approach. LiteWorp adds an interesting wormhole-specific twist to the

IV. DISCUSSION AND COMPARISON

METHOD	MOBLITY	SYNCHRONIATION	QOS
Geographic Leash Technique	Bound to maximum transmission distance	Low synchronization	Delay up to leash factor
Temporal Leash Technique	Bound to maximum transmission distance	Medium synchronization	Delay up to leash factor
DELPHI	No need	No need	Delay
SECTOR	No need to Time synchronization	No need	No delay
WAP	Maximum transfer distance is calculated	Only source node is synchronised	Deley per hop
SaW	Delay Factor	Not required	Not required
DaW	Not considered	Not considered	Deley parameter
LITEWROP		Static Network only	
HMTI	Short Range Wormhole can be detected	No need	Jitter

V. Future Work

Several mobility methods schemes are studied which provides better result as compared to the standard ones taking different parameters in different situations using simulators (as NS2-Network Simulator) but there is a need of evaluating these methods in a more genuine scenario and applying them to real wireless scenario. There is a need of improving these schemes keeping in mind high speed of vehicles, repeatedly changing topology and huge number of vehicles in city scenarios or in highway scenarios.

VI. Conclusion

Wormhole attacks in MANET significantly degrade network performance and threat to network security. Here we have basically surveyed the existing approaches which will help us in future to design a new approach for detecting the wormhole attack in Mobile Ad Hoc network .Overall a significant amount of work has been done on solving wormhole attack problem. We can"t say one solution is applicable to all situations. So there is choice of solution available based on cost, need of security may lead better result, but can be costly, which may affect other networks need. Similarly some network require more security like military area network. A standard solution is still lacking, although several very useful solutions applicable to some networks have been described.

References

[1] Srdjan Capkun, L.evente Buttyan, and Jean-Pierre Hubaux, 2003 "SECTOR: Secure Traking of Node Encouters in Multi-hop Wireless Networks,"*In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS)*, pp. 21-32.

[2] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 "Packet Leashes : A Defence against Wormhole Attacks in Wireless Networks", *Twenty-Second ANNUAL Joint Conference of IEEE Computer and Communications* , pp. 267-279.

[3] Lingxuan Hu and David Evans, Feb. 2004 "Using Directional Antennas to Prevent Wormhole Attack ",In *Proceedings of the Network and Distributed System Security Symposium*, pp. 131-141.

[4] Chiu, HS; Wong Lui KS, 2006 "DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks",*In Proceeding of International Symposium on Wireless Pervasive Computing*, pp. 6-11.

[5] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, Nov. 2008 "Analysis of wormhole Intrusion Attacks In MANETS",IEEE Military Communications Conference,MILCOM 2008.

[6] Y.-C. Hu, A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, Security and Privecy Magazine, IEEE, vol. 2, issue 3,pp. 28-39, May 2004.

[7] R. S. Khainwar, A. Jain , J. P. Tyagi , Dec 2011 ,"Elimination of Wormhole Attacker Node in MANET Using Performance Evaluation Multipath Algorithm *" International Journal of Egineering Technology and Advanced Engineering*, Volume 1, Issue 2, pp. 40-47.

[8] F. Natt-Abdesselam, B. Bensaou, T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Network", *IEEE Communications Magazine*, 46(4), pp. 127-133, 2008.

[9] M.A. Gorlatva, P. C. Mason, M. Wang, L. Lamont, R. Liscano, "Detecting Wormhole attacks in Mobile A d Hoc Networks through Protocol Breaking and Packet Timing Analysis", In IEEE Military Communications Conference, pp. 1-7 ,2000

[10] Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks" , *In Proceedings of the International Journal of Computer Theory and Engineering, Vol. 2, No. 1* February, 2010, pp.78-86.

[11] Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. pp. 2-17.

[12] M.S.Sankaran, S.Poddar, P.S. Das, S.Selvakumar "A Novel Security Model SaW: Security against Wormhole attack in Wireless Sensor Networks", *In Proceeding of International Conference on PDCN*, 2009.

[13] Khin Sandar Win "Analysis of Detecting Wormhole Attack in Wireless Sensor Networks",World Academyof Science, Engineering and Technology, 2008,pp.422-428.

[14] I.Khalil, S.Bagchi, N.B.Shroff, "A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", *In Proceedings of the 2005 International Conference on Dependable Systems and Networks (*DSN"05).

[15] Jyoti et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(2), February - 2013, pp. 137-142 © 2013, IJARCSSE All Rights Reserved Page | 142

[16] Maria Alexandrovna Gorlatova "Review of Existing Wormhole Attack Discovery Techniques" *A Contractor report at DRDC Ottawa*, pp. 1-23, August , 2006.

[17] S.Choi, D.Kim , D. Lee, J. Jung " WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Network ", *In Proceeding International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*, 2008, pp. 343-348.

[18] Guoxing Zhan, Weisong Shi, and Julia Deng, 2012 "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" *IEEE Transactions on Dependable and Secure Computing*, Volume 9, Issue 2, pp.184-197.

[19] H. Vu, A. Kulkarni, K. Sarac, N. Mittal. "WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks". In *Proceedings of International Confernce on Wireless Algorithms Systems and Applications*, LNCS 5258, pp. 491-502, 2008.

[20] On the Survivability of Routing Protocols in Ad Hoc Wireless Networks, A. Baruch, R. Curmola, C. Nita- Rotaru, D. Holmer, H. Rubens, Convergence on Security and Privacy for Emerging Areas Communications, Secure Comm 2005, September 2005