National conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

Analysis of wormhole Intrusion Attacks in MANETs

Deepthi V S[1], Dr. Vagdevi S[2]
[1]Research Scholar, VTU RRC, Assistant Professor, Department of ISE, GAT, Bangalore, India
[2]Prof & Head, Department of EEE, GSSSIETW, Mysuru, Karanataka, India

ABSTRACT

Security of different networks has always been a primary concern as its necessary to protect the resources being shared and communication being done among the legitimate users. If we let down our safeguards, an attacker can transform the routing protocol and interrupt the network operations through mechanisms such as packet drops, flooding, data fabrication etc. MANET is a type of network whose dynamic topology, decentralizing governance and other such features are always in favour of many security attacks. This paper presents detail study of wormhole attack, algorithms to detect them that has been proposed so far and also directs the reader toward the areas that can be explored and work upon in future.

Keywords: Security, MANET, Wormhole attack, Wormhole detection technique, Wormhole prevention, classification

I. INTRODUCTION

The is the features of MANET (mobile adhoc network) that makes it vulnerable to many security attacks. MANET contains various mobile hosts (laptops etc.). As the name suggests the hosts can move anywhere within the network so there is no fix structure of this network so providing security to such network is a really significant issue [1]. There is no centralizing body for governing all network activities. This feature saves from the bottleneck of having single governing body but there is no specific area where providing security may assure safeguarding from every type of attacks. Moreover, nodes in this type of network have limited transmission ranges so if any two nodes are within the transmission range of each other, they communicate directly otherwise, nodes situated on paths between them act as a router and forwards the information from source to destination. This characteristics highlights an important aspect of MANET that is, to transmit data efficiently there is need of cooperation among intermediate nodes that also means, if any of the node is malicious node it can adversely affect the communication. Any attacker can do harm to network activities in two ways, either, he can affect routing methods involved in transmission like misleading the rules used in routing protocols or altering the information needed in routing methods (AODV, DSR etc.) like hop count, no. of nodes etc or data being delivered can be affected like adding or subtracting any of the bits in any frame field. Thus, a slight modification can do serious harm to transmission.

Security ssues like is in MANET are the fields that have Been worked upon a lot in recent days.

Various algorithms has been proposed and various papers have been published. If we go for employing security algorithm at a time than it will affect the network performance like delay in transmission due to calculation of different factors and if we keep in view enhancement of network performance only it may result in inadequate security measures hence any measure provided for security in MANET should

maintain the trade-off of better network performance and adequate security measures. Security attacks in MANET are classified in two different categories: active attacks versus passive attack as depicted in Fig. 1. Passive attacks: Attackers in this attack snoops the data being exchanged without altering it. Active attacks: This type of attacks disturbs the normal functioning of network by altering or dropping the packets being exchanged. Internal attacks: Attacks of this type are from compromised nodes that are part of network. External attacks: Attackers carry out this type of attack through nodes that does not belong to network in consideration.

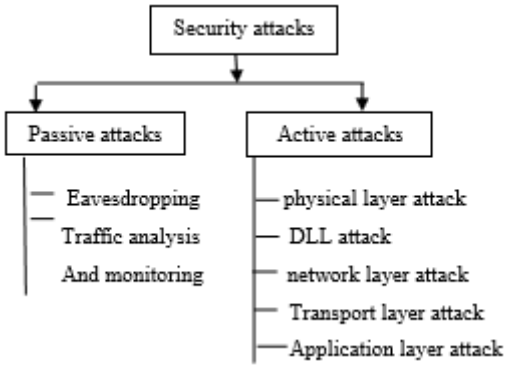

Fig 1: types of security attack

Wormhole attack is an active attack as shown in fig 2

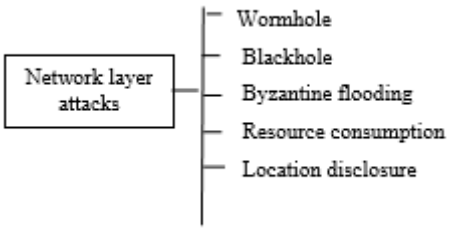

Fig 2: network layer attacks

II. WORMHOLE ATTACK

A wormhole attack [2] is one of the most sophisticated and severe attacks in MANET. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a tunnel like link. The level of affect it can have on network can be understood by the fact that it can be launched against all communications that provide authenticity and confidentiality. The malicious nodes involved in attack are called wormholes. For example, in fig 3, the path from S to D via wormhole link (W1, W2) has the length of 5 when the normal path has the length of 11.

Therefore, in most routing protocols, S prefers sending data to D along the path with wormhole link. The wormhole link can be formed by many type of links such as by using Ethernet cables, long-range wireless transmissions, an optical link in wired medium etc. Wormhole attack stores packets at one end-point in the network and tunnels them to other end-point. However, the above method is difficult to deploy because it requires some special hardware to create an out-of-band channel. Hence another technique that uses encapsulation is more popular to launch wormhole attacks. Instead of using an out-of-band channel, the malicious node W1 encapsulate packets it acquires and send them to the second malicious node W2 through the tunnel that exists between them. W2 decapsulates and gets the original packets and rebroadcasts them again in network. As the original packets were encapsulated, they were not changed by intermediate nodes that lies in the path between W1 and W2. Through this way, W2 seems to get the packet directly from W1 with the same hop count although they are several hops far from each other. Wormhole attacks affect the network in following way

- It decreases the number of hopes per route
- Route discovery time get reduced
- Reduces average delay time
- Increases average retransmission time

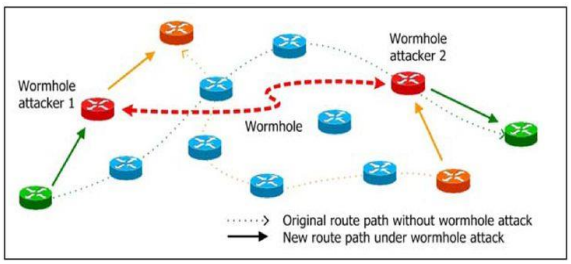

Fig 3: wormhole attack

TAXONOMY OF TYPES OF WORMHOLE ATTACK

Wormhole can be implemented in various ways [3],[4],[5] depending upon various factors. If classification is to be done on the basis of attackers then there can be three types of wormhole Open wormhole, half open wormhole and close wormhole [6]. Consider the scenario in which m1 and m2 are malicious nodes, S and D are the good nodes that are source and destination respectively, a and b are the good nodes between source and destination. If node S and D are connected by using a wormhole, then source and destination nodes think that they are neighbors and all data between them will be transmitted by using a wormhole link. Both the nodes m1 and m2 are in the wormhole. In open wormhole both the wormholes are visible In half open wormhole, m1 node is the neighbor of S and it tunnels m2 to destination and only one node can be seen due to wormhole attack. In the close wormhole attack both nodes m1 and m2 are not visible to source node and destination node. If classification is to be done on the basis of implementation, it totally depends upon the manner in which the attack is launched like if attacker is using encapsulation then packets get encapsulated at one wormhole and travel along all the intermediate nodes in encapsulated form and finally get delivered to another wormhole, this resists increase in hop count. In this case both wormholes are not directly connected; they just make other intermediate node believe they are directly connected. If attacker is using out-of-band channel then both colluding nodes are directly connected using channel with high bandwidth. This channel can either be a wired connection or wireless connection. This attack requires extra hardware to be launched but it provides simplicity. If colluding nodes have potential of high power transmission attacker can use high power transmission. If attacker is using protocol deviation method to attack network, he causes violation in rules to be followed while using any specific routing method that may result in discarding of any genuine request. If classification is to be done on the basis of medium to be used there are two types: in-band wormhole which has no change in medium to be used for creating wormhole tunnel as in packet relay, encapsulation etc. and out-of-band wormhole which require different medium to be used for creating wormhole tunnel like in high transmission mode. If classification is done upon the basis of location of victim nodes there are two types of wormhole attack: simplex in which victim node is in the range of only one attacker and duplex in which victim node is in the range of both the attacker. If classification is done on the basis of data that can be carried through tunnel, wormhole attack can be of three types: threshold based in which packets having size greater or equal to threshold value get dropped, all pass based in which all packets get passed irrespective of size and all drop based in which all packets will be dropped.

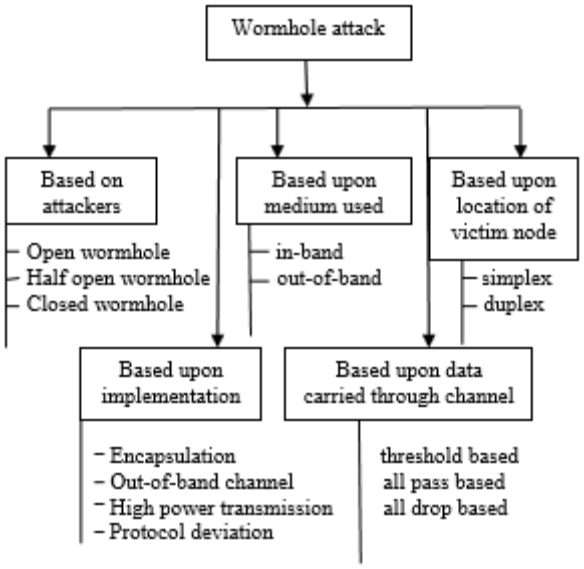

Fig 4: classification of wormhole attack

III. RELATED WORK

The In 2003 hu et al. and Capkun et al. had used geographical and temporal leaches to detect wormhole attack. This technique uses GPS technology for coordination among all nodes .Clocks are loosely synchronized. It is very robust and straightforward solution but carries the limitation of GPS technology [7].

In 2004 various method have evolved for detection of wormhole like Wang and Bhargava had used network visualization that had centralized controller for network and works best for mesh networks but certain features like mobility and varied terrains were not studied, Lazos and Poovendran had used localization method that brought in the concept of guard nodes, every nodes were made aware of their location with respect to the network but as obvious was not readily applicable for mobile networks, Park and Shin had used LISP for detection of wormholes which were applicable for static networks only, Hu and Evans used directional antenna in which each node carry a directional antenna[8].

In 2005 Lazos et al. used a method in which nodes have both directional antenna and GPS. Beside him, Baruch et al. had used time of flight that has hardware that enables onebit message and immediate replies without having CPU involvement, it is highly impractical as it require MAC layer modification, Song et al used statistical analysis that works only for multi-path on-demand protocols, Khalil et al uses LITEWORP that require static topology for network, it uses pre-distribution pair-wise key management protocol which is not applicable if there is any protocol deviation [9].

In 2006 Hu et al devised connectivity based approach that requires connectivity information of nodes and uses tightly synchronized clocks, it is impractical as such synchronization is hard to achieve in any network, Weichao el al uses end-to-end mechanism that requires knowledge of location information and has loosely synchronized clocks, this mechanism uses geographic location and authentication to detect defects in network[10], Eriksson el al used true-link that has authentication and time-based mechanism, it works only with standard 802.11 along with little backward compatibility[11].

In 2007 Trans et al used TTM [12], it is transmission-time based mechanism and requires cooperation of all nodes that lie along the path, Rasmussen and Capkun used radio fingerprinting that uses Chipcon 1000, 433MHz radio[13].

In 2008, Özdemir et al. introduced TTBM i.e. transmission and trust based mechanism [14], Khalil et al. used MOBIWORP that has maximum limit on number of nodes that attacker can capture[15], Papadimitratos et al. and Poturalski et al. introduced secure neighbour discovery. In 2009, Venkataraman et al. introduced GTA that is applicable for proactive protocols that uses adjacency matrix of nodes and has graph- based mechanism [16], Shokri et al. introduced neighbour verification protocol that performs local geometric consistency tests[17], Chen et al. introduced CSB that has consistent-set based resistant localization system and there is no packet loss in the system[18].

In 2010, Chen et al. introduced secure localization that has conflicting-set-based resistant localization [19] and Graaf introduced distributed detection system [20]. Currently various approaches like statistical analysis has been used for detection and prevention of wormhole attack.

IV. COMPARISON AND DISCUSSION

Various methods have been devised so far for detecting and preventing against wormhole attack. Each employ different mechanism and target on different aspect of network like watch dogs, they identify colluding nodes by storing a copy of packet before forwarding it. When packets are overheard, it is matched with copy stored in buffer and if they match, copy is discarded otherwise failure count is incremented and if this counted reaches the threshold it is considered as malicious node. But this method does not able to detect collision during ambiguous collision or receiver collision. In directional antennas it is assumed that each node maintain an accurate set of neighbors so wormhole can be detected if it is able to find false neighbor and ignoring messages from that node. Directional antenna is used to find the direction and angle of

arrival of messages but if attacker poses attack from places between these directional antennas, it is not able to detect it. In statistical analysis scheme frequency of links being used in transmission is noted as links which are part of wormhole tunnel will be used again and again. This method does not require any special hardware, neither there is any alteration of existing protocols. It does not require any set of information as it just uses the routing data which is already available at each node. Graph theoretic model categorizes nodes into two types: guard node and regular node. Guard node uses GPS technology to access location information and regular node calculate their location with respect to the guard node thus they are able to detect any abnormal transmission. In this scheme sender encrypt each transmission by local broadcast key which get decrypted at receiver side but this method has disadvantage of high time delay in calculating position and specialized hardware is required by guard nodes. In TTM (Transmission Time based Mechanism) attack is identified in route setup stage by calculating transmission time among two nodes. It requires co-operation among nodes. Dispersed detection approach uses ranges of nodes for detection of wormholes.

Table 1

METHODS	SYNCHRONIZATION	MOBILITY FACTOR	QoS FACTOR	FALSE DETECTION
HMTI[21]	Not required. Since PSD profiling is done locally.	Handled weakly. Topologically robust, short range worm-hole can be detected.	Jitter and delay.	Used PSD to detect false positive alarm.
DelPHI [22]	Not required.	Not considered.	Delay	Not handled.
Temporal Leashes Technique[23]	fine-grained synchronization	Restrict the maximum transmission distance of packet	Delay up to leashes factor	Not handled
SaW [24]	Not considered.	Not considered.	Not considered.	Failed to detect.
WORMEROS [25]	Time synchronization not required. RTT between source node and destination node is considered.	Topological change is not considered.	Not considered	Both false positive and false negative alarms are considered.
Farid et al. [26]	Some time delay added to detect suspicious links.	Not considered	Packet processing time, queue delays within nodes.	Not handled.
SAM [27]	Not considered	Cluster and uniform topology considered.	Not considered	Not handled
DaW [28]	Not considered.	Not considered.	Delay parameter.	Failed to detect.
WAP [29]	Only the source node is synchronized.	Maximum transmission distance is calculated.	Delay per hop.	Not handled
Geographical Leashes Technique[30]	coarse synchronization	Restrict the maximum transmission distance of packet	Delay up to leashes factor	Not handled
LITEWROP	Not required	Static networks only	Not required	Not handled

V. CONCLUSION

Wormhole attack is among those attacks that poses serious threat on adhoc network. It is easy to launch wormhole attack in MANET as features of MANET are very favorable for such attacks. Various detection and prevention methods are being proposed so far but to achieve all security goals is not an easy task. This paper indicates various algorithms and protocols for providing counter measure against wormholes but still there is some bottleneck being faced in some or the other way. Future work includes developing more efficient and secure protocol that can work under all circumstances. As MANET has feature of having nodes capable of moving anywhere in network and having characteristics that can make it router as well as source or destination, a protocol that can provide adequate security in such a dynamic natured network is demanded, so by taking help from all the work being done so far in this field and by keeping in view all conditions of the network a more promising protocol should be developed.

VI. REFERENCES

1. S Ci et al., "Self-Regulating Network Utilization in Mobile AdHoc Wireless Networks," IEEE Trans. Vehic.Tech., vol. 55, no. 4, July 2006, pp. 1302–10.
2. Y-C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks, Selected Areas of Communications," in IEEE Journal on, vol. 24, no. 2, pp.370-380, 2006.
3. V Mahajan, M. Natu "Analysis of wormhole intrusion attacks in MANETS", In IEEE Military Communications Conference (MILCOM), 2008.
4. HS. Chiu and K. Lui. "Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of International Symposium on Wireless Pervasive Computing, 2006.
5. R Maulik, N. Chaki. "A Comprehensive Review on Wormhole Attacks in MANET". In 9th International Conference on Computer Information Systems and Industrial Management Applications, 2010.
6. Khin Sandar Win, Pathein Gyi, "Analysis of Detecting Wormhole Attack in Wireless Networks," in World Academy of Science, Engineering and Technology 48, pp. 422-428, 2008.
7. YC. Hu, A. Perrig, and D.B. Johnson. "Packet leashes: A defenseagainst wormhole attacks in wireless ad-hoc networks," Proceedings of 22nd IEEE INFOCOM, pp. 1976-86, Apr. 2003.
8. L Hu and D. Evans. "Using directional antennas to prevent wormhole attacks," Proceedings of Network and Distributed System Security Symposium, pp. 131-41, Feb. 2004.
9. I Khalil, S. Bagchi, and N.B. Shroff. "LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks," Proceedings of the International Conference on Dependable Systems and Networks, pp. 612-41, 2005.
10. W. Weichao, B. Bharat, Y. Lu, and X. Wu. "Defending against wormhole attacks in mobile ad-hoc networks," Wireless Communication and Mobile Computing, vol. 6, no. 4, pp 483-503, 2006.
11. J. Eriksson, S. Krishnamurthy, and M. Faloutsos. "Truelink: Apractical countermeasure to the wormhole attack," International Conference on Network Protocols, pp.75-84, Nov. 2006.
12. P.V. Tran, L.X. Hung, Y.K. Lee, S. Lee, and H. Lee. "TTM: An efficient mechanism to detect wormhole attacks in wireless adhoc networks," 4th IEEE Consumer Communication and Networking Conference (CCNC'07), pp. 593-8, May 2007.
13. K.B. Rasmussen and S. Capkun. "Implications of radio fingerprinting on the security of sensor networks," Third International Conference on Security and Privacy in Communication Networks and the Workshops, pp. 331-40, Sep. 2007.
14. S. Özdemir, M. Meghdadi, and I. Güler. "A time and trust basedwormhole detection algorithm for wireless sensor networks," (manuscript in Turkish), in 3rd Information Security and Cryptology Conference (ISC'08), pp. 139-4, 2008.
15. I. Khalil, S. Bagchi, and N.B. Shroff. "MOBIWORP: Mitigation of the wormhole attack in mobile multi-hop wireless networks,"

Elsevier Ad Hoc Networks, vol. 6, no. 3, pp. 344-62, 2008.
16. R. Venkataraman, M. Pushpalatha, T.R. Rao, and R. Khemka. “A graph-theoretic algorithm for detection of multiple wormhole attacks in mobile ad-hoc networks,” International Journal of Recent Trends in Engineering, vol. 1, no. 2, May 2009.
17. R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.P. Hubaux. "A practical secure neighbor verification protocol for wireless sensor networks,” ACM WiSec, 2009.
18. H. Chen, W. Lou, and Z. Wang. “Conflicting-set-based wormhole attack resistant localization in wireless sensor networks,” Book Chapter Lecture Notes in Computer Science – Ubiqitous Intelligence and Computing, vol. 5585/2009, pp. 296-309, 2009.
19. H. Chen, W. Lou, X. Sun, and Z. Wang. “A secure localization approach against wormhole attacks using distance consistency,” EURASIP Journal on Wireless Communication and Networking- Special Issue on Wireless Network Algorithms, Systems, and Applications, pp. 22-32, 2010.
20. R. Graaf, I. Hegazy, J. Horton, and R. Safavi-Naini. Distributed “Detection of wormhole attacks in wireless sensor networks,” Springer book chapter Ad Hoc Networks, vol. 28, pp. 208-22, 2010.
21. D.B. Roy, R. Chaki, N. Chaki. "A New Cluster-based Wormhole Intrusion Detection Algorithm for Mobile Adhoc Networks", IJNSA, 1 (1), pp. 44-52, 2009
22. H.S. Chiu and K. Lui. “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”. In Proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, 2006.
23. Dhara Buch, Devesh Jinwala, “Detection of Wormhole Attacks in Wireless Sensor Networks”, IEEEConference on Advances in Recent Technologies in Communication and Computing, pp 714, 2011.
24. M.S. Sankaran, S. Poddar, P.S. Das, S. Selvakumar. “A Novel Security model SaW: Security against Wormhole attack in Wireless Sensor Networks”. In Proceedings of International Conference on PDCN, 2009.
25. 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.
26. F. Nait-Abdesselam, B. Bensaou, T. Taleb. “Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks”, IEEE Communications Magazine, 46 (4), pp. 127 - 133, 2008.
27. N. Song, L. Qian, X. Li. “Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach”. In Proceedings of the 19th IEEE International Parallel and DistributedProcessing Symposium, 2005.
28. Khin Sandar Win. “Analysis of Detecting Wormhole Attack in Wireless Networks”, World Academy ofScience, Engineering and Technology, 48, pp. 422-428, 2008.
29. S. Choi, D. Kim, D. Lee, J. Jung. “WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks”. In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343-348, 2008.
30. Dhara Buch, Devesh Jinwala, “Detection of Wormhole Attacks in Wireless Sensor Networks”, IEEEConference on Advances in Recent Technologies in Communication and Computing, pp 714, 2011.