A Survey on Wormhole Attack and its Prevention Techniques

Nilofer Khan
Computer Science & Engineering Department,
Rajiv Gandhi Technical University, Bhopal, India

Prof. Ashish Tiwari
Vindhya Institute of Technology and Science
Indore, India

Abstract— ***MANET has become a paramount research area in today's networking system. Mobile nodes when connected through wireless links form an ad-hoc network. It is termed as MANET which is an autonomous system. An infrastructure less network which is self organized network is withal the other name for MANET. MANET is a Mobile ad-hoc NETwork utilized in sundry business application; battlefield, remote areas etc .Performance and security are the two major issues of this field. Due to lack of centralized ascendancy it is suspicious to sundry types of attacks. Wormhole assailment is one of them. This paper provides a survey on challenges of MANET, its application, types of attacks in MANET, wormhole attack, its types, includes study of wormhole detection and prevention techniques.***

Keywords—Active attack, MANET, Passive attack, Wireless network, Wormhole attack.

I. INTRODUCTION

Wireless Network is a method which evade the costly process of installing the cables in homes, buildings etc. Telecommunication network, homes, enterprises etc are not connected by any type of cable. Various equipment locations are withal connected without the utilization of cable. For the implementation of wireless telecommunication system a transmission system is utilized. This transmission system is called as Radio Waves which is utilized for the administration additionally. This Implementation through radio waves is done at physical layer of the network system. Mobile phones are the example of this type of wireless technology. Inter Continental network is another example which uses radio satellites to communicate all over the world such as emergency accommodations like police utilizes the wireless network to communicate with each other efficaciously .It is withal utilized by the businessmen and individuals to apportion their data in the network.

A. Types of AD-hoc mobile communication

Ad-hoc network are categorized into two types-

1) Infrastructure Network- In the Infrastructure Networks there is fine-tuned gateways. Base stations are fine-tuned which are connected with other base stations. A cell is the transmission range of a base station. According to the transmission range a "hand-off" occurs. In this way the host which is mobile can be able to communicate in the network.

2) Infrastructure less network- There are no fine-tuned routers. All nodes are dynamical and are capable to move. The individual terminals can be move anywhere in the entire network that is we can verbally express that the entire network is mobile. For example MANET is an Infrastructure less Network.

The mobile nodes connected with wireless links forms an autonomous system called as MANET. Hence it is a self organized network connected by mobile nodes with wireless links. MANET is an infrastructure less and decentralized network that is why it is used in various applications such as, remote areas, business application, battle field etc. Each node acts as the router as well as the end system. When used as the router it forward the packets. by its own characteristics; it is self-organizing, mobile communication manner where topologies are dynamically created. Due to the ad hoc nature of the network infrastructure and mobility it is still an area of new research and development. Due to lack of infrastructure various issues arise in the network i.e. security, performance and simulation.

MANET have some special features through which its is different from other type of network.

1. Every node deport as a role of both host and router. Therefore it is autonomous in nature.

2. Multi-hop radio relaying- When a message of source node and destination node is out of range in that case ,the MANET is utilized multichip routing..

3. Distributed nature of operation of security, routing and host configuration. A fixed firewall is absent in the MANET.

4. Due to the dynamic nature in the network each node can connect and leave the network at any time.

5. Mobile nodes have less recollection, power and light weight features.

6. In the wireless links the reliability, efficiency, stability and capacity are much more preponderant than wired links This shows the fluctuating link bandwidth of wireless links.

7. By the nature of mobile and spontaneous comportment minimum human participation to configure the network.

8. All nodes have kindred features with homogeneous responsibilities and capabilities and hence it composes a planarity symmetric environment.

9. Utilizer density is high and level of utiliser mobility is withal high.

10. Nodal connectivity is intermittent.

The above features of MANET keep attracted researchers in field of MANET, but some major issues and challenges are also present which is decreases the performance and security level of MANET.A MANET environment has to overcome certain issues of limitation and less efficiency. It also consists of:

1. The wireless link features are time-transmuting in nature: There are transmission impediments like fading, loss of path, blockage and interference that integrate to the sensitive comportment of wireless channels. The wireless transmission has less reliability due to all this factors.
2. A circumscribed range of wireless transmission –In the wired network by inhibited radio band the data rates results is so much less as compared to the wireless network. Hence the optimum utilization of bandwidth is indispensable by keeping less overhead as possible.
3. Packet losses due to errors in transmission – MANETs have much higher packet loss due to some reasons like hidden nodes that results in collisions, wireless channel issues (high bit error rate (BER)), interference, and frequent paths break due to the mobility of nodes, incremented collisions due to the presence of obnubilated nodes and unidirectional links.
4. Route changes due to mobility- The dynamic nature of network topology provide the frequent path breaks.
5. Frequent network partitions- The random movement of nodes provide the partition of the network. This mostly harms the neighbour nodes.

II. APPLICATIONS

The applications of MANET include highly dynamic networks, immensely colossal-scale application, mobile networks, minute networks, static networks etc. Incipient accommodations and incipient environment are perpetual to evolve under this field. The sundry applications of MANET are as follows-

1) Military Battlefield: Some computer equipments are utilized by the military routinely. Military utilize this technology of ad- hoc networking so that it can maintain and retrieve the information from the soldiers and their headquarters.

2) Commercial Sector: Rescue operations and emergency accommodations utilize the technology of ad hoc networking system such as efforts that includes disaster mitigation like flood, earthquake, fire or other types of natural calamities. The networks where expeditious and rapid deployment is required there emergency rescue operations should be implemented. Damaged and non subsisting communication infrastructures are withal best suited area for them. Through a diminutive hand-held one member of the rescue team transmits the information to other rescue team member over a minute hand held. Law enforcement and ship to ship ad hoc mobile network are the other examples of Commercial Sector.

3) Local Level: Local networks can additionally be established by the ad hoc networking. Palmtop computers and notebook computers can be facilely linked ad interim and apportion or spread the information and data among the users. The classroom and conference are the examples. To exchange the data home networks can withal be engendered which is a local level application and contrivances can communicate directly. Local level applications withal include other applications such as sports stadium, diminutive aircraft, boat, taxicab etc.

4) Personal Area Network (PAN): Personal Area Network utilizes the concept of ad hoc networking. Sundry types of mobile contrivances such as a laptop, PDA, a cellular phone can interconnected and can be communicate facilely by these wireless links. Wireless connections superseded the astronomically immense and intricate cables. GPRS, WLAN, UMTS can withal be accessed through this ad hoc network.

A.MANETs Challenges -

1 Limited bandwidth: Wireless link have significantly more diminutive capacity in comparison to the infrastructure predicated networks. In the wireless network the effect of multiple access, noise, fading and intrusion situation etc., is often much less than a radio’s maximum transmission rate.

2) Dynamic topology: Due to the dynamic nature of the network the relationship between the nodes may be perturb.. The trust may additionally be perturbed if some nodes are detected as compromised.

3) Routing Overhead: In wireless adhoc networks, nodes transmute their location very desultorily within network. So, some state routes are engendered in the routing table which increases the nonessential routing overhead.

4) Hidden terminal quandary: Due to the hidden terminal quandary refers to the collision of packets at a receiving node due to the concurrent transmission of those nodes that are not in the direct transmission range of the sender, but are in the transmission range of the receiver.

5) Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the kineticism of nodes; hence the network suffers fast path breaks. This situation provides the recurrent route changes.

6) Battery constraints: Devices utilized in these networks have restrictions on the puissance source in order to maintain portability, size and weight of the contrivance.

7) Security threats: The wireless mobile ad hoc nature of MANETs brings incipient security challenges to the network design. As the wireless medium is vulnerably susceptible to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are essentially exposed to numerous security attacks.

III. BACK GROUND

Security issues are paramount in wireless network even more than in wired network. A particularly major attack in wireless network is the Wormhole Attack. For outsider its easy to listen the network traffic or interface with it for the open nature of the wireless medium. For these factors make wireless network introduce to several different types of malicious attack. This malicious node can carry out both Passive attack and Active attack against the network.

A. Types of Attack in MANET:

1. Passive Attack: In Passive attack a malignant nodes only eavesdrop upon the packet contents.

2.ActiveAttack: A packet can modify legitimate, drop or imitate facilely in the active attack. A typical example of particularly devastating security attack is known as Wormhole attack.

3. Wormhole Attack: In wormhole attack, one malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are again resent into the network. In between this two colluding attacker one tunnel is maintained this is refers as wormhole. It could be established through a single long-range wireless link or wired links between two colluding attacker. In this type of attack the wormhole may create by the attacker even for packets not addressed to itself because radio channel has broadcast in the nature.

For example in Fig. 1, A and B are two malicious nodes then the packet can be encapsulated by this two malicious node and create falsified the route lengths.

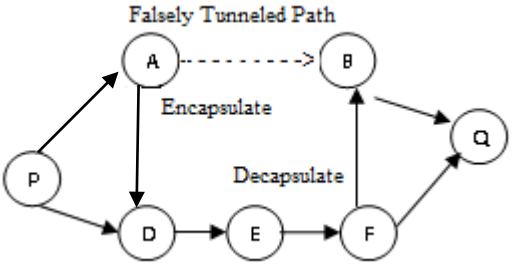

Fig.1 Shows wormhole attack

Suppose node P wishes to compose a route to Q and initiate route revelation. When A receives a route request from P, A encapsulates the route request and tunnels it to B through a subsisting data route, in this case {A→D→E→F→Y}. When B receives the encapsulated route request for Q then it will show that it had only travelled {P→A→ B → Q}. Neither A nor B update the packet header. After route revelation, the destination finds two routes from P of unequal length: one is about 4 and another is about 3. If B tunnels the route reply back to A, P would falsely consider the path to Q via A is better than the path to Q via D. Thus, tunnelling can obviate veracious intermediate nodes from correctly incrementing the metric used to quantify path lengths.

If the wormhole is utilized opportunely for efficient relaying of packets then no harm is engender, it puts the assailant in a potent position compared to other nodes in the network, which the assailant could utilize in a manner that could compromise the security of the network.

The wormhole assailment is most hazardous attack for many routing protocol in the ad-hoc network in which the nodes that hear a packet transmission directly from some other node consider themselves to be in the range of (and thus a neighbour of) that node. For example, when utilize against an on-demand routing protocol such as DSR, a

potent application of the wormhole attack can be mounted by tunnelling each route request packet directly to the destination target node of the request. When the destination node's neighbours aurally perceive this request packet, they will follow normal routing protocols in which the nodes that auricular discern a packet transmission directly from some node consider themselves to be in the range of (and thus a neighbour of) that node. When the destination node's neighbours aurally perceive this request packet, they will follow mundane routing protocol processing to rebroadcast that facsimile of the request and then discard without processing all other received route request packets originating from this same route revelation. This attack thus obviates any routes other than through the wormhole from being discovered, and if the assailer is near the initiator of the route revelation. This attack can even avert routes more than two hops long from being discovered. Possible ways for the assailant to then exploit the wormhole include discarding rather than forwarding all data packets, thereby engendering a permanent Denial-of-Service attack or selectively discarding or modifying certain data packets. So, if opportune mechanisms are not employed to bulwark the network from wormhole attacks, most of the subsisting routing protocols for ad hoc wireless networks may fail to find valid routes.

B. Types of Wormhole Attack: The categorization of such an assailment target on the design of detection and obviation methods of wormhole attack. By this the assailers are facilely optically discerned on the route, we can relegate the wormholes into three types: open, closed, and half open.

Open Wormhole Attack: In this type of wormhole, the attackers involve themselves in the RREQ packet header following the route revelation procedure. Other nodes are having cognizance that the malevolent nodes present on the path but they feel that the malignant nodes are direct neighbours.

Closed Wormhole Attack: If the packet in a route revelation packet then the attacker do not modify facilely the content of the packet.. Instead, the packet can simply tunnel form one side of wormhole to another side and it resend the packet.

Half open wormhole Attack: Only one side of wormhole modify the packet and only another side does not modifies the packet, successive the route revelation procedure.

B.Detection and prevention techniques of Worm hole attack

Localization Technique - Wormhole attack are considered as an astringent security threat in multi-hop wireless ad hoc networks. In this paper, [Sanjay 2012][5] propose an Energy-Efficient Scheme Immune to Wormhole attacks (our soi-disant E2SIW). This protocol utilize the information location of the nodes to detect the presence of a wormhole, and in case a wormhole present in the path, it finds different routes involving the nodes of the culled path so as to obtain a secure route to the destination. The protocol having the ability of detecting wormhole attacks employing either hidden or participating malevolent nodes. Simulations are organize, exhibiting that E2SIW can detect wormholes with a, less overhead, high detection rate and can utilize less energy in short time, compared to the De Worm wormhole detection protocol, cull as benchmark.

Timestamp Technique– A Round Trip Time (RTT) mechanism has been proposed by Zhen et al [3].In this mechanism, each node calculates the RTT between itself and all its neighbours. This mechanism does not require any special hardware and it is easy to implement; however it can not detect exposed attacks because fake neighbours are created in exposed attacks.

The RTT is the time that extends from the (RREQ) message sending time of a node. A route reply (RREP) message receiving time from a node B.A will calculate the RTT between A and it's all neighbours, because the RTT between the two fake neighbours is higher than between the two real neighbours. A can identify both the fake real neighbours. In this mechanism each nodes calculates the RTT between itself and all its neighbour .However it can't detect exposed attack.

Watchdog Techniques- To identifies misbehaving nodes and avoids routing through these nodes, watchdog and path rater. In this technique, watchdog identifies misbehavior of nodes by copying packets and maintained a buffer for recently sent packets. The overheard packet is compared with the sent packet, if there is a match then discards that packet. If the packet is timeout, increment the failure tally for the node. And if the tally exceeds the thresholds, then node will misbehave. The implementation of watchdog technique is shown in Fig. of two parts:

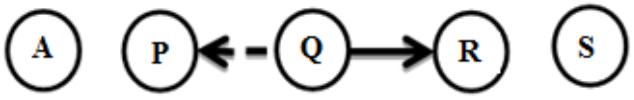

Fig. 2 Watchdog Implementation

Special Hardwasre Based Approach-SECTOR proposed by *Capkun et al* [2] uses Mutual Authentication with Distance-Bounding (MAD). A node estimates the distance to another node in its transmission range by sending it a one-bit challenge, which the node responds to instantaneously. By utilizing the time of flight, neighbours can be detected. However, this approximation uses special hardware that can respond to a one-bit challenge without any delay as packet leash is.

Secure Neighbor Discovery and Monitoring Based Approach- This is given by *Issa Khalil* in[6] *2008*. It prevents surrounding areas from vicious nodes by using local observation schemes. Central authority follows the position of each node and it can separate malicious nodes globally. When the network mobility of this method increases the detection rate decreases.

IV. REVIEW

In the following Table 1 contains all wormhole detection methods that are explained previously and also contains the requirements of each method.

TABLE I
SUMMARY OF VARIOUS WORMHOLE DETECTION TECHNIQUES

S no.	Year	Published By	Method Used	Advantages	Limitations
01.	2012	**Sanjay**	Localization Technique	1. High detection rate. **2.** Less utilization of energy in short time. **3.** Less overhead.	**1.** Only detect the wormhole and find secure path, can't remove it.
02.	2003	**Zhen et al**	Timestamp Technique	**1.** No need of special type of hardware. **2.** Can be easily implemented.	**1.** Exposed attacks can't be detected.
03.	2013	**Yashpalsingh Gohil**	Watchdog Technique	**1.** Misbehaving of nodes is identified and routing is avoided through these nodes.	**1.** A buffer is required. **2.** Most of the time is wasted in comparing the overhead packet with recently sent packets.
04.	2003	**Capkun et al**	Mutual Authentication with Distance-Bounding (MAD).	**1.** Distance is estimated in transmission range by sending one bit challenge. **2.** Utilizes the time of flight scheme.	**1.** To respond a one bit challenge special hardware is needed.
05.	2008	**Issa Khalil**	Secure Neighbour Discovery and Monitoring Based Approach	**1.** Vicious nodes are prevented by using local observation scheme. **2.** Malicious nodes are separated globally. **3.** Detection rate increases.	**1.** Central authority is required.

V. Conclusions

This paper includes the survey of wireless network and wormhole attack. There are various types of attack in the infrastructure less network. This paper presents the types of wormhole attack, the prevention and detection techniques of such type of attack. The issues such as performance and security are discussed. There should be better ways to increase the performance and security of an infrastructure less network by preventing the wormhole attack.

VI. Acknowledgment

This research work is not related with any type of industrial research work. I would like to thank everyone who had contributed to the successful completion of this research. I would like to express my gratitude to my research supervisor, Prof Ashish Tiwari for his invaluable advice, guidance and his enormous patience of the research. I also wish to acknowledge Lect.Mitesh Bargadiya and other to contribute in the preparation of this survey.

REFERENCES

[1] U.Venkanna, R.leela velusamy, proc. Of conf. on advance inrecent technologies in communication and computing 2011

[2] Capkun S., Buttyan L. and Hubaux J. (2003),'SECTOR: Secure Tracking of Node

Encounters in Multi-hop Wireless Networks', In ACM Workshop on Security of Ad Hoc and Sensor Networks (ACM SASN), October 2003.

[3] Zhen J. and Srinivas S. (2003) 'Preventing replay attacks for secure routing in ad hoc networks', In ADHOC-NOW, LNCS2865, pp. 140-150 .

[4] Hu L., Evans D. (2003), 'Using Directional Antennas to Prevent Wormhole Attacks', Proceedings of the 11th Network and Distributed System Security Symposium, pp. 21-30.

[5] Sanjay Kumar Dhurandher, Isaac Woungang, Abhishek Gupta, Bharat K. Bhargava, E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks, 978-0-7695-4652-0/12 $26.00 © 2012 IEEE, DOI 10.1109/WAINA.2012.85

[6] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff, 2008 “MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks” A*d Hoc Networks*, Volume 6, Issue 3, pp. 344-362

[7] Yashpalsingh Gohil,Sumegha Sakhreliya,Sumitra Menaria ,2013 “A Review On:Detection and Prevention of Wormhole Attacks in MANET”,Volume 3,Issue 2,ISSN 2250-3153.