INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A REVIEW: ANALYSIS OF WORMHOLE ATTACK AND ITS DETECTION TECHNIQUES

AASHIMA[1], VISHAL KUMAR ARORA[2]

[1]*M Tech Scholar, aashima_kataria@ymail.com*

[2]*Assistant Professor, vishal.fzr@gmail.com*

Deptt. Of CSE, SBSSTC, FEROZEPUR, 152001,

PUINJAB, INDIA

ABSTRACT

Security is an important issue while developing MANET or any other wired or wireless network. The paper presented depicts the previous techniques used in the past and the new technique used in the future work. All the work is revolving around detecting the Wormhole Attack using DSR routing protocol and preventing the network from the wormhole attack so that the performance can be increased considerably. The Techniques used in the previous work are packet leashes, hop count analysis, cluster based approach and optimized DSR protocol. Comparison of all the four previous techniques is also discussed. The overview of the ongoing work is written accordingly.

KEYWORDS: MANET, Wormhole, Leashes, Cluster Approach, Hop Count Analysis, DSR

1. INTRODUCTION

With the emerging areas of technology, MANETS have gained a significant importance in this world of networking. MANETS are infrastructure less networks with varying capabilities like dynamic topology and mobile nodes compromises self configuring networks. There is no fixed base station and also a lack of centralized authority is there. Mobile nodes in MANETS communicate with each other via wireless links like as the communication is done by satellites, microwave relay stations, underground data transfer, under water data transfer etc.

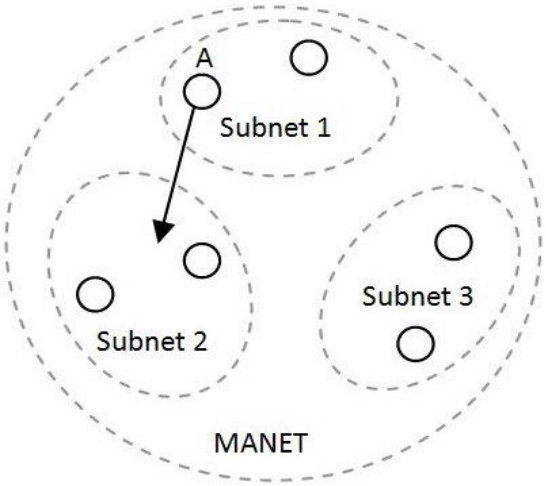

Figure1: EXAMPLE OF MANET

Security is the major concern in MANETS. While communicating, lot of attacks occurs like black hole, sinkhole, wormhole, Sybil, byzantine attacks occur. The attack under consideration in this paper is Wormhole attack. In Wormhole attack, when source and destination are going to start communicate, intruders activate a wormhole link, which is a high speed wireless link and listen to the communication done by communicating agents with the help of wormhole link.

Example of Wormhole Attack

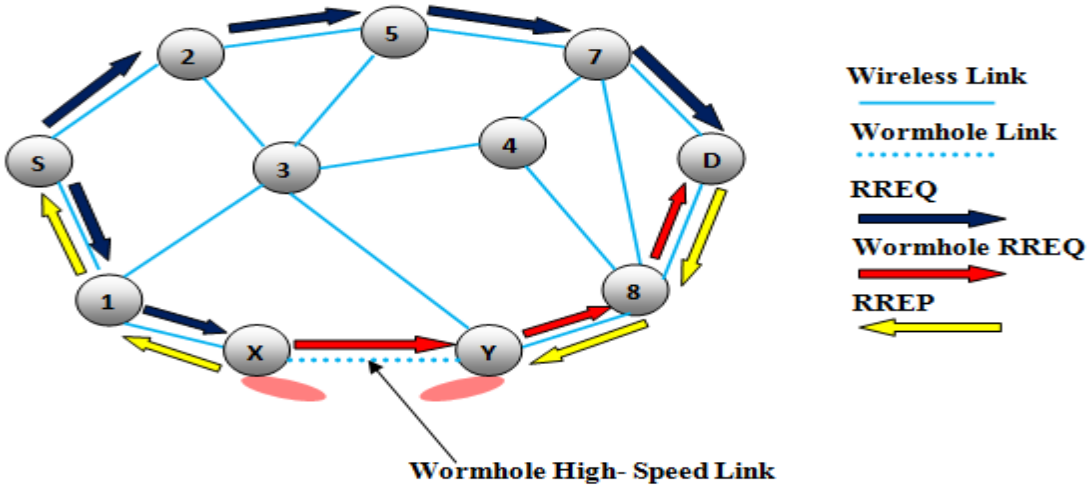

Figure 2: Wormhole Attack

In the above Fig. 2**,** the nodes "X" and "Y" are malicious node that forms the tunnel in network. The source node "S" when initiate the RREQ message to find the route to node "D" destination node. The immediate neighbour node of source node "S", namely "2" and "1" forwards the RREQ message to their respective neighbour "5" and "X". The node "X" when receive the RREQ it immediately share with it "Y" and later it initiate RREQ to its neighbour node "8", through which the RREQ is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-1-8-D> for destination. It results in ignoring RREQ that arrives at a later time and thus invalidates the legitimate route <S-2-5-7-D>. The communication done by <S-1-8-D> is thereby listened by the wormhole nodes "X" and "Y". So the wormhole nodes and their high speed link pose a major security threat to the network.

2. RELATED WORK

The work done so far to detect and prevent wormhole attack cannot get defeated by cryptographic methods. The wormhole attackers do not create separate packets but they replay packets already existing on the network. Several researchers have worked on detecting and preventing the network from wormhole attack. Several techniques have been proposed by them. The next section describes the present mechanism used to detect and prevent the network from wormhole attack.

A. PROBLEM STATEMENT

This section describes the wormhole attack's nature and the present mechanism used to detect and prevent the network from wormhole attack. A wormhole attack is particularly a severe attack on MANETS in which the wormhole nodes are introduced into the network which give belief to the other nodes that they are legitimate nodes and the communication is forced to move through their link as their link i.e. wormhole link is the high speed link which takes shorter time to travel from source to destination. A wormhole attack is thought of as a two phase attack. In the first phase, the working is done as above mentioned that is the illegitimate nodes try to lure legitimate nodes that they are valid and data transfer is done via wormhole high speed link so the communication is overheard by intruders. In the second phase, the intruders do whatever they want to do with the data and exploit it in a variety of ways.

In this paper, we want to discuss the problem statement on which we want to work in future. The mechanism used in this is that it will focus on providing solution for this problem by enhancing multipath algorithm resulting in regaining of the average number of hops as well to get normal delay by excluding the attacker nodes and these factors will be implemented using counter bit algorithm with relevant changes and thus can prevent wormhole attack in MANETS.

B. GENERAL APPROACHES

Several solutions have been proposed for the wormhole attack avoidance like packet leashes, cluster base, hop count analysis and improved DSR protocol. Packet leashes are used as a defense mechanism against wormhole attacks that provide the additional information added to packets to restrict maximum transmission distance of a packet.

There are two types of packet leashes:

1. Geographical Leashes
2. Temporal Leashes

Temporal Leashes have the problem of attacker accessing and modifying the expiration time of these leashes. So TIK (TESLA with instant Key Disclosure) protocol was developed. TIK requires accurate time synchronization between all nodes and each node only needs to know one public value for each sender node. Geographical leashes are less efficient than temporal leashes since they require broadcast authentication. As TIK is designed to implement temporal leashes, they needed to provide authentication of received packets and requires "n" public keys in a network of size "n".

The next approach to prevent wormhole attacks is cluster based approach. A n-cluster is defined by a subset of nodes which are mutually reachable by a path of length at most n for some fixed n. The size of a cluster is the maximum number of nodes. Clusters will add robustness during a boundary node failure. Cluster based protocols allow the network to enjoy the liberty of maintaining routes between all pairs of nodes at all times, without causing much network overhead. This approach does not guarantee shortest path. This is due to the fact that the clusters are created using the first fit approach which does not produce the maximum clusters in the graph. Also the routing overhead of this approach is not high.

The third approach to avoid wormhole attack is hop count analysis. This scheme uses a highly efficient protocol which does not require any specified supporting hardware. The protocol is used to split multipath route so that the transmitted data is naturally split into separate routes. This scheme can be directly used in MANET. This analysis does not pinpoint the location of wormhole.

The last approach taken under this paper consideration is the improved DSR protocol. In this scheme, when the communication is going to start, the intruders try to lure valid nodes that they are immediate neighbour and pose a shortest path. So the communication is forced to go through that wormhole path. But when improved DSR protocol works, it eliminates the wormhole path from its routing table when wormhole node is encountered and start route discovery phase to select a path from source to destination. The main limitation in this scheme is that time taken to find a route from source to destination is very much and again when the wormhole node is encountered DSR has to find a route for communication to take place.

C. DSR(DYNAMIC SOURCE ROUTING) PROTOCOL

DSR is an on-demand routing protocol which is designed to restrict the bandwidth consumed by control packets in adhoc networks by eliminating the periodic table update messages required in the table driven approach. The main characteristic of this on demand routing protocol is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions which are used by a node to inform its neighbors of its presence.

To find a route from source to destination, DSR uses a two phase process:

1. Route Discovery Phase
2. Route Maintenance Phase

In the first Route discovery phase, source node starts the discovery for a route to destination for the communication to take place. When the route is found then that path is used for communication and the path is added to the routing table. In future, when any path is to be found then first of all it is to be checked in the route cache or we can say routing table that if that path exists or not. If the path exists then that is used for communication and if path is not found then only route discovery phase starts.

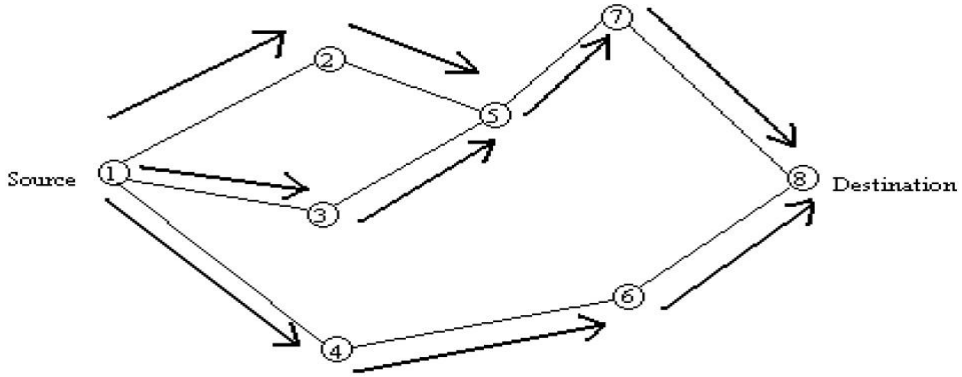

Figure 3: Propagation of request (RREQ) packet

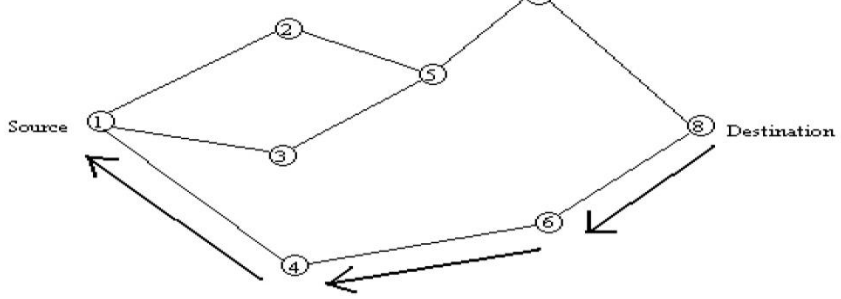

Figure 4: Path taken by the Route Reply (RREP) packet

In the above figure it is clear that when source node 1 wants to send data to destination node 8, they start route discovery phase and found 3 routes to node 8. The communication is done through the shortest path <S-4-6-8>. RREQ(Route Request) packets are send from node 1 to node 8 and the shortest path is selected for communication that is the path <S-4-6-8> and the RREP(Route Reply) packets are send along this path.
The second phase is route maintenance phase, in which the maintenance of all the paths is done that are present in the routing table. This phase checks that if any path is present in the table and that path is no longer used in transferring the packets, then that path is removed from the routing table. So this is how the DSR protocol works.

3. PROPOSED SOLUTION

Based on the above problems discussed so far, a new solution has been developed in which the working of Improved DSR protocol is done. The improved and modified working of DSR protocol is explained further

.

A. PROPOSED TECHNIQUE

Research techniques used so far for detection of wormhole nodes in adhoc networks have some flaws with them. The improved DSR protocol working has the flaw that it takes so much time to find a path and if that contains a wormhole node then that path is rejected and again starts the route discovery phase to find a route from source to destination. In wormhole attack, special mobile nodes called wormhole nodes try to redirect the whole network traffic through them. The intruders introduce wormhole nodes between the network which are actually not the part of network but try to lure the communicating agents that they are immediate neighbour of them and have shortest path. So the communication is forced to go through them. When the intruders listen the information they can exploit or use the information in a variety of ways. This proposed technique works on the misbehaving wormhole nodes and the simulation is done on the DSR protocol for the prevention of wormhole attack using ns-2 simulator and Red-Hat Linux.
The proposed techniques work on the detection of wormhole nodes and then prevent wormhole attack on the network. This can be done by the technique of wormhole avoidance and the working of DSR protocol is again modified with the additional functionality of wormhole avoidance and detection. Proposed scheme starts working when source finds a way to destination. It finds alternatives paths from source to destination in route discovery phase using multipath algorithm. From all that paths first path is selected for transmission of packets. If that path contains wormhole nodes then that path is rejected and second path is selected that is obtained from multipath algorithm. If first path contains no wormhole nodes then that will be used for communication. The path that contains wormhole nodes is not added to the routing table so that in future that path is not used for transmission of packets.

B. SIMULATION ENVIRONMENT

Simulation is used to reproduce the behavior of a system. Simulation refers to the actual running of a program that contains algorithms. It is performed on the model of areal system and then the simulation results are used to compare as well as improve the model and theories of a real system. ns-2 is one of the discrete event simulator used in the field of networking research. Simulation of the wired and wireless networks can be done by ns-2. In ns-2 modeling is very complex and time consuming task because it has no GUI and one who has to use has to learn scripting language, queuing theory and modeling techniques. ns-2 works with routing protocols also like DSR(Dynamic Source Routing), AODV(Adhoc Distance Vector Routing), DSDV(Destination Sequenced Distance Vector) protocol etc.
Red Hat Linux is also used with ns-2. Linux is an open source and free software. It has various commands used with ns-2. This is the operating system used in virtual environment and ns-2 is installed in linux operating system.

4. COMPARISONS OF VARIOUS TECHNIQUES

TECHNIQUE	PROS AND CONS	SPECIAL HARDWARE	OVERHEAD
Packet Leashes	Temporal leashes are highly efficient and are used with TIK. They require tight time synchronization. But geographical leashes do not require tight time synchronization and increases computation and network overhead.	NO	HIGH
Cluster Based Approach	Performance of network increases with the increasing number of guard nodes that further increases the probability of detection of wormhole attack But more study has to be done to analyze performance of this algorithm in presence of multiple attacker nodes.	NO	LOW
Hop Count Analysis	Avoiding attacks in this scheme is from the viewpoint of users not of the administrator's viewpoint. This scheme MHA when applied with constant boundaries performs better than the loose ones in avoiding attacks.	NO	HIGH
Improved DSR protocol	This technique helps in detecting and preventing wormhole nodes quickly and easily but does not show major differences between the network parameters compared with the previous one.	NO	LOW

5. CONCLUSION

Presence of the wormhole nodes in the network is one of the major security problems occurred so far. The work is concerned with the detection of wormhole nodes and then prevents the network from wormhole attacks in future. The routing protocol used in this technique is DSR i.e Dynamic Source Routing Protocol which is further improved so that the effective communication can take place and prevent the network from wormhole attacks. Simulation shows that when a path is found for transmission and if a wormhole node is detected in that path then that path is rejected and removed from the routing table so that in future that path is not used for communication.

This type of attack can also be prevented by other techniques but each of them have its on pros and cons. So a robust network has to be created for effective transmission of packets.

REFERENCES

1. Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", IEEE Third International Conference on Advanced Computing & Communication Technologies, 2013.
2. Weichao Wang, Bharat Bhargava, Yi Lu, Xiaoxin Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Conference of Wiley Journal Wireless Communications and Mobile Computing (WCMC), 2010 .
3. Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, pp 123-127, February, 2010.
4. MahaAbdelhaq, Sami Serhan, RaedAlsaqour and Anton Satria, "Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol", Australian Journal of Basic and Applied Sciences, Volume- 5, issue- 10, pp 1137-1145, 2011.
5. Amol A. Bhosle, Tushar P. Thosar and SnehalMehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Volume- 2,issue- 1, pp 325-331, February 2012.
6. Ms. N.S.Raote, Mr.K.N.Hande, "Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network", International Journal Of Advanced Engineering Sciences And Technologies Volume- 2, Issue- 2, pp 172 – 175, 2010.
7. L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", Research supported by NSF grand and Collaborative Technology Alliance.
8. Shang Ming Jen, Chi-Sung Laih, Wen-Chung Kuo, "A Hop Count Analysis Scheme For Avoiding Wormhole Attacks In MANET", Open Access Journal Sensors- mdpi.com, Sensors 2009,9,5002-5039;doi:10.3390/s 90605022.
9. Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, "A New Cluster Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks", International Journal Of Network Security & Its Applications IJNSA, Vol. 1, No. 1, April 2009.
10. Radu Stoleru, Haijie Wu, Harsha Chenji, "Secure neighbor discovery and wormhole localization in mobile ad hoc networks", SciVerse Science Direct, volume- 10, issue- 7, pp 1179-1190, 2012.
11. Sung-Hee Lee, Young-Bae Ko, Youg-Geun Hong, and Hyoung-Jun Kim, ''A New MIMC Routing Protocol Compatible with IEEE 802.11s based WLAN Mesh Networks'', pp-126-131, ICOIN, International conference, IEEE, 2011.
12. Turgay Korkmaz ," Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless Ad Hoc Networks", Information Technology: Coding and Computing, ITCC, IEEE International Conference, volume- 2, pp 704-709, 2005.
13. Farid Naït-Abdesselam, Brahim Bensaou, Tarik Taleb," Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", Communications Magazine, IEEE, Volume- 46, issue- 4, pp 127-133, 2008.
14. Gajendra Singh Chandel, Priyanka Mur, "Manet Threat Alarming Based On System Statistics & Support Vector Machine", International Journal of Engineering Research and Applications (IJERA), Volume- 2, Issue- 4, pp 1722-1726, July-August 2012.
15. Reshmi Maulik and Nabendu Chaki, "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications, Volume- 3, issue- 1, pp 271-279, 2011.