ISSN 2319 - 5975

Volume 8, No.3, April - May 2019
International Journal of Networks and Systems
Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns07832019.pdf
https://doi.org/10.30534/ijns/2019/07832019

Review on Detection of Wormhole Attack in AODV Protocol based MANET

Telma George[1], Suma R[2]
[1]APJ Abdul Kalam Technological University, India, telmageorge10@gmail.com
[2]APJ Abdul Kalam Technological University, India,suma.r@sjcetpalai.ac.in

ABSTRACT

A Mobile Ad-hoc Network (MANET) is a self-configuring, infrastructure-less network of mobile devices connected wirelessly. MANET is used commonly around the world, because it has the ability to communicate with each other without any fixed network. Routing protocols are requires for communication and synchronization in such ad hoc networks. Security is most important service of all kinds of network communications. MANET are more vulnerable to security attacks due to its features like open medium, changing its topology dynamically, lack of central monitoring and management. Security attacks in MANET are classified into passive attacks and active attacks. Among some of the prominent security threats worm-hole attack is considered as one of the most severe security attack because it is difficult to detect. A wormhole attack can be easily launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms. Hence an efficient mechanism to detect wormhole attack has to be developed.

Key words: Mobile ad hoc networks , Security , Attacks in MANET, Wormhole attack

1. INTRODUCTION

A mobile ad-hoc network also known as wireless ad-hoc network [1], is a continuously self-constituting, infrastructure-less network of mobile devices that are connected wirelessly. Every moving devices in a network is self-governing. The mobile devices are free to move and organize themselves randomly. Nodes in the MANET communicate via the wireless medium and network topology is dynamic in nature. In MANET, breaking of communication link is constant.

MANET have introduces many applications in different networks. With many applications there exist some design problems and challenges to overcome. The main objective of mobile ad-hoc network is to expand mobility into the

state of autonomous, wireless domains, mobile where a set of nodes which may be combined hosts and routers, they form the network routing infrastructure in an ad-hoc manner. Lots of security vulnerabilities in MANET are identified and a set of counteractions are also proposed. But only a few of them provide a guarantee which is statistically independent to security critical challenge. The main aim of mobile ad-hoc network while considering above factors is to support robust and efficient operation in mobile wireless networks by including routing functionality into mobile nodes. Such networks have future responsibility to be dynamic, sometimes quickly-changing, random, many to many hop topologies which are likely composed of proportionately bandwidth-constrained wireless links. MANET is more vulnerable than wired network because of mobile nodes, hazards from com-promised nodes, dynamic topology, limited physical security, capability and lack of centralized control. Because of these vulnerabilities, MANET is more prone to malicious attacks.

In MANET, every single networking activities such as packet forwarding and routing, are executed by nodes themselves in a self-organizing fashion. So that, securing a mobile ad-hoc network [2] is too challenging. The security goals of MANET is as follows:

- Availability – it refers to datas which are accessible to authorized ones at proper times.
- Confidentiality - it makes sure that datas are accessed only by authorized persons.
- Integrity - Integrity means that resources can be altered only by authorized persons or only in authorized manner.
- Authentication - Authentication enables a node to make the identity of neighbouring node is exactly right.
- Authorization - Authorization is used to ascribe different access rights to different rank of users.

Routing is the way towards transmitting data or packets to destination node from source node. As ad-hoc network changes their topology and making packet routing troublesome at that moment. Routing protocol controls the stream of information in systems and chooses the best way to attain the goal. Routing protocols [3] define

a set of ruleswhich governs the strategy of message packets transfer to destination in a network.

- Proactive Routing Protocols
  In this protocol each node maintains all information about message dissemination over the network through the table. By this reason proactive routing protocol also known as Table-Driven routing protocol. The network topology data are stored in table. These tables exchange data periodically for current data .

- Reactive Routing Protocols
  Each node in this protocol stores data of effective routes to the destination. A route scan is needed for every new destination during this means the correspondence overhead is belittled at the expense of delay to go looking the route. Quickly ever-changing wireless configuration could interrupt active route and cause sequent route scan. Reactive Routing protocol is additionally known as the on-demand routing protocol. During this routing protocol route is established based on demand. AODV and DSR are the Reactive routing protocols.

2. SECURITY ATTACKS IN MANET

Securing wireless ad-hoc networks is a really challenging problem. Understanding feasible type of attacks is always the initial step for developing a noble solution. Security of communication is required for the secure the transmission of data in MANET. Absence of centralized system and shared wireless channel makes MANET more vulnerable to attacks than wired network. There are various attacks [4] that affect MANET. These attacks can be mainly classified into two types – Active and passive attacks.

Active attacks are done by the malicious nodes that carry some energy cost in order to perform the attacks. Active attacks involve some modifications to data or formation of false data stream. Active attack is divided into internal attack or external attack. External attacks are carry through nodes that do not belongs to the network. Internal attacks are carry through nodes that belongs to the network.

- Black hole Attack - A malicious node sends false information about route, declaring that it has an optimum route and makes other nodes to send packet information through the malicious node. A malicious node drops all packets that it receive.
- Wormhole Attack - In this attack, the malicious node captures packets at one point, routes them to another point and then resend it to the network from that point. Routing can be interrupted when the routing message are tunnelled. The tunnel between two collaborating nodes is called a wormhole.
- Byzantine attack - A compromised set of intermediate nodes that are working within network carry attacks such as routing loops creation, forwarding packets through incorrect paths or selectively drop packets which results in disturbance or degeneration of the routing within the network.
- Replay attack - An attacker retransmits the valid data frequently to introduce the network routing traffic that is captured previously.
- Flooding - Malicious nodes insert wrong packets into the network, or produce ghost packets which loo around due to incorrect routing information, effectively using the bandwidth and processing resources along the path.

Passive attacks does not interrupt proper operation of network .Attackers investigate data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to decode the information gathered through snooping. Detection of these attack is difficult since the operation of network does not get affected.

- Traffic Monitoring - It can be developed to identify the communication parties and functionality which could provide information to organize further attacks.
- Eavesdropping - In this attack intercepting, reading and conversation of message by unplanned receiver take place.
- Traffic Analysis - traffic analysis is a passive attack which is used to gain information on nodes that are communicating with each other and how much data is processed.

2.1 Wormhole Attack

A wormhole attack is the most serious attack among the security attacks in the MANET because it does not use any node in the network. It has the most impact on the network because it halts the overall performance of the network by dropping the packets. In this type of attack, the two attacking nodes are connected to each other through a link called tunnel. The malicious node captures the packet from the legitimate node and by enclosing the packet, transmits it to another malicious node.

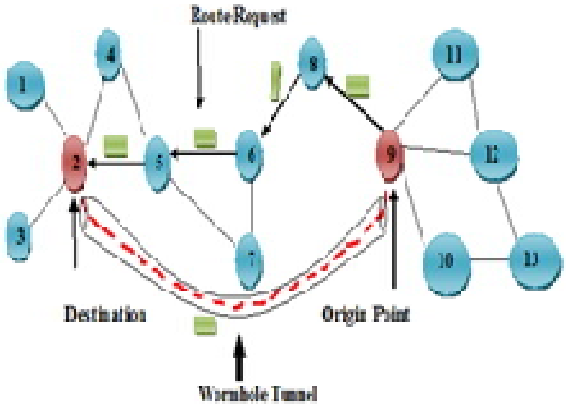

Figure 1: Wormhole attack

Wormhole attack is shown in figure 1. The nodes 2 and 9 are the malicious nodes in the network and these nodes will try to receive the RREQ message packets. Node 9 will route a packet which carries them in correct route to node 2. But, in actual it is not the original path. The actual path is follows from node 9-8-6-5-4-2. The path from node 9 to node 2 is the wormhole link or tunnel created by the compromised nodes.

Wormhole attack is shown in figure 2.1. The nodes 2 and 9 are the malicious nodes in the network and these nodes will try to receive the RREQ message packets. Node 9 will route a packet which carries them in correct route to node 2. But, in actual it is not the original path. The actual path is follows from node 9-8-6-5-4-2. The path from node 9 to node 2 is the wormhole link or tunnel created by the compromised nodes.

3. LITERATURE REVIEW

This section comprises of various algorithms and methods for the detection of wormhole attack.

The proposed methodology of wormhole detection and prevention is based on statistics based scheme and graphical based solution of wormhole problem. The main theme of the proposed method [5] is to identify wormhole in the path suggested by AODV protocol by using divide and conquer technique. The wormhole detection is done between all the possible combination of node to its next to next node and decision will be taken on the basis of each and every possible combination. If wormhole is identified in any of possible combination then whole suggested path is consider to be as wormhole affected path. For detection, every node find alternate path for its next to next node. If number of hop count in any of alternate route is greater than threshold then that node send wormhole detection message between itself and its next to next node. In proposed algorithm all decision will take on the basis of value of threshold that is, mini-mum number of node in alternate route between every pair of node to next to next node with the path discover by AODV is greater than or not. If it is greater than threshold value, then it is declared that there is wormhole between its next node and next to next node, otherwise not.

An efficient method to detect a wormhole attack called modified wormhole detection AODV protocol has been proposed. Wormhole attack is identified by using number of hops in different routes to the destination from the source. The destination can detect both types of wormhole attacks. The performance of modified wormhole detection AODV protocol is justified by simulations. This paper proposed a modified wormhole detection AODV protocol based on the AODV protocol and can detect the attack in this network in an efficient manner. In MAODV [6], a concept which detects wormhole attacks in network by collecting the delay and neighbour count information for various path from source to destination, it can offer a typical solution for wormhole attacks. The reason behind is that in under legitimate situation, the delay of every packet is similar along every hop in the route and the delay for each packet should be excessive for those nodes are included in the wormhole attack because there can be many nodes between them or can be connected through a link. Therefore, if compare the delay per hop of every node in the normal path and a path under wormhole attack, finds thatdelay per hop of a path that is under wormhole attack is greater in comparison of normal path.

A technique is to overcome a special type of attack called wormhole attack introduced by at least two colluding nodes within a network. In this work, some modifications done in AODV routing protocol to identify and remove wormhole attack in real-world MANET. WADP is implemented in modified AODV. Also node authentication is used to identify attacker nodes and remove the false positive problem that arise in this algorithm. Node authentication not just only removes false positive but it also helps in mapping exact location and is a type of double verification for the wormhole attack detection.

The proposed technique is implemented in modified AODV protocol. Also for removal of false detection we are adding two extra fields in RREP packet that is containing IP of intermediate node and unique number assigned to it. The unique number is a prime number and increments by19 after every hour. It is assumed that this information is known only to authentic nodes. When a node is unable to specify the right IP and number combination, it is treated as malicious. With implementation of this node authentication test along with WADP [7] in modified AODV, we have a double verification in presence of wormhole attack. WADP confirms presence of exposed worm-hole nodes and node authentication detects it. This removes false positive problem in WADP also it indicates the exact position of malicious nodes. Node authentication alone can detect exposed wormhole attacks but it cannot detect hidden wormhole attacks as when the existence of malicious nodes are unknown then their IP and unique number cant help in detection, therefore , integration of WADP and node authentication in modified AODV protocol removes the short comings of each other. Another work[8] is divided into two phases, in phase-1 the generation of wormhole attack is described and in phase-2 an efficient approach for analyzing and restriction of wormhole attack is described.

In [9] a protocol which will protect ad-hoc networks from blackhole and wormhole attacks and to improve the network stability is proposed. This paper presents an intrusion detection system depends on the concept of specification-based detection to detect and prevent blackhole attacks. This paper also presents a hop count analysis method to detect wormhole attacks along the routes. The proposed protocol does not need any location information, time synchronization, or special hardware to detect wormhole attacks.

Another method is depends on the Hash based Compression Function (HCF) which is using some secure hash function to compute value of the hash field for RREQ packet. This proposed approach [10] is for defending against

the wormhole attack in MANET environment with AODV routing protocol. Security is a necessary service for wireless and wired network communication. Due to security vulnerabilities of the routing protocols, MANET is unsafe from attacks done by compromised nodes. This survey workdisturbed with a severe security threat that affects ad-hoc networks routing protocols, namely wormhole attack. There are several solutions to detect and then prevent this attack but any of them is a perfect solution. This approach looks very effective compared to others proposed in literature.

This paper provides a method for secure data transmission via the network and proposes a neighbour node analysis technique to detect the wormhole attcak in Manet. The neighbor node analysis approach [11] analyze the neighbouring nodes so as to examine the authencity of the nodes for secure transmission of data over the network. According to this approach, a node will send a request to its neighboring nodes and performs a request and response message mechanism. Each node will also keep a table to track the timeout. If the reply time is not precise then there is an attack is found in the network. All intermediate nodes are inspected to identify the presence of wormhole attack using AODV protocol in MANET.

The work [12] is about the prevention of the network from the wormhole attack. In this work, a mechanism is presented to secure the communication between source node and destination node in the network. As the node has to start the communication, it first starts with the neighbor discovery from the neighbor list. It first generates the Hello message and encrypts it using the secret key. The encryption mechanism is used to prohibit the network from the wormhole attack. As the neighboring node receives this message, it will decrypt that message using same secret key and send the acknowledgement back to the sender. If the node is not authentic, it will remove its entry from the neighbor list. After the neighbor discovery, it sends the RREQ to its immediate neighbours from the neighbours list through the path to destination. As the RREQ message reaches the destination, it will generate a RREP reply message and unicast it to the source node.

4. CONCLUSION

A study of MANET, various attacks and specifically wormhole attack in MANET has been done. Wormhole advertises a false routing path which is shortest than others and attracts the entire traffic to it. It is found that in this addition of delays in network, there is a decrease in the throughput because of wormhole attack. Overall, a significant number of work has been done for solving wormhole attack problem. One solution is not applicable to all the situations, but the analysis on various kinds of wormhole attacks and their detection techniques exhibit would be useful to device stronger detection technique.

REFERENCES

1. Sudha Singh, S.C. Dutta, D.K. Singh, **A study on Recent Research Trends in MANET**, in International Journal of Research and Reviews in Computer Science (IJRRCS), 2012.
2. Mahendra Dhole, Anand Gadwal,**Wormhole Attack Detection Techniques: A Review** , inInternational Journal of Computer Science And Technology , 2016.
3. Neeraj Verma, Sarita Soni, **A Review of Different Routing Protocols in MANET**, International Journal of Advanced Research in Computer Scienc, 2017.
4. Ashwani Kumar,**Security Attacks in Manet - A Review**, National Workshop-Cum Conference on Recent Trends in Mathematics and Computing, 2011.
5. Pratima Singh, Ashish Srivastava, Nitesh Gupta,**A Novel Approach to Detect Prevent Wormhole Attack over MANET**,IOSR Journal of Computer Engineering, 2013.
6. Kumar chaurasia, Varsha singh,**MAODV : Modified Wormhole Detection AODV Protocol** , IEEE, 2013.
   https://doi.org/10.1109/IC3.2013.6612197
7. Juhi Biswas, Ajay Gupta,**WADP: A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol**, International Conference on Industrial and Information Systems, 2014.
   https://doi.org/10.1109/ICIINFS.2014.7036535
8. ChaShivangi Dwivedi, Priyanka Tripathi, **An Efficient Approach for Detection of Wormhole Attack in Mobile Ad-hoc Network**, International Journal of Computer Applications, 2014.
   https://doi.org/10.5120/18214-9172
9. Kriti Patidar, Vandana Dubey,**Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks**, IEEE , 2014.
   https://doi.org/10.1109/CSIBIG.2014.7056976
10. Anal Patel, Nimisha Patel , Rajan Patel**,Defending Against Wormhole Attack in MANET**,Fifth International Conference on Communication Systems and Network Technologies, 2015.
    https://doi.org/10.1109/CSNT.2015.253
11. Sweety Goyal, Harish Rohil,**Securing MANET against Wormhole Attack using Neighbor Node Analysis**,International Journal of Computer Applications, 2013.
    https://doi.org/10.5120/14227-2478
12. Dimple Saharan, **Detection and Prevention of Wormhole attack on AODV Protocol in Mobile Adhoc Networks,**International Journal Of Engineering And Computer Science, 2014.