International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

SECURITY ATTACKS AND PREVENTION IN MANET

T.V.Ashwini,
Dept. of Information Technology,
Velammal Engineering College,
Chennai,India.

L.Hemalatha,
Dept. of Information Technology,
Velammal Engineering College,
Chennai,India.

R.Sridharshini,
Dept. of Information Technology,
Velammal Engineering College,
Chennai,India.

Abstract: The main aim of this research paper is to study about attacks that are present at different layers and always face the security threats. Black Hole and Worm Hole are the attacks present at Network Layer. MANET (Mobile ad hoc Networks) and security attacks present in MANET. MANETs are Powerless against different types of Cooperative Black Hole Attack is an attack in which two or more black hole nodes are working in a group. In our proposed work we using PEI (Plain Encryption identifier) to detect and prevent the Cooperative black hole attack. Wormhole attack is one of the well-known and noticeable attacks. These type of attack lets the malicious node to pretend like it's an actual node in the network and acts like it is the nearest node to the source node. And also it is capable of dropping the packets sent by the source node to the destination node An efficient method is proposed using AODV (Ad hoc On demand Distance Vector) routing protocol which is capable of reducing packet loss and delay.

Keywords: MANET, Cooperative Black hole attack, PEI, RSA, Worm Hole attack and AODV Routing Protocol

I.INTRODUCTION

Mobile ad-hoc network (MANET) is a "infrastructure-less" network and having a "dynamic topology". As mobiles are portable device, it can be moved from networked area to non-networked area. If there were no any network, no two devices establish connection with eachother. So, in these types of cases mobile ad-hoc networks are used. The mobile device or node can communicate directly with other device available in network or can use mediator nodes to makes communication between source and destination.

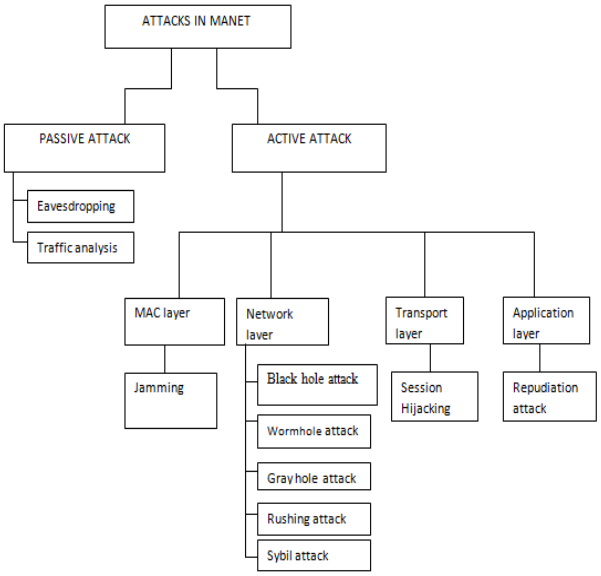


Fig 1:Types of attacks in MANET

MANET mobile nodes are forming a temporary network. No centralized control is there in MANET . MANET's topology is dynamic in nature and also there is a lack of centralized control, hence it is affected from lots of security attacks.As it is an infrastructure less network security has become a key issue. First of all let we explain how many layers are there in MANET stack. Basically there are five layers i.e. application layer, transport layer, network layer, Mac layer, & physical layer.

The main three layers of ad hoc that take part in routing mechanism are physical layer, MAC layer and network layer. As the structure of MANET is vulnerable to attacks, there could be routing disorders cause by it. In MANET each node acts as a router and forward packets so it is easy for attacker to get into network. Main idea behind network layer attack is to place itself between the source and destination. Thus attacker can capture the data transmitted, can drop the transmitted packet and can create routing loops. These all can cause congestion in the network. The different types of network layer attacks are

- Black hole attack: A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors then it effectively separates the network in to two disconnected components.
- Wormhole attack: This type of attack makes a tunnel between two malicious nodes and attracts the data flow through these attacker nodes.

II.BLACK HOLE & COOPERATIVE BLACK HOLE ATTACK:

In a blackhole attack a attacker node sends fake routing information in the network to claims that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example in an Ad-Hoc on

demand distance vector routing (AODV), attacker can send fake RREQs including a fake destination sequence number that is fabricated to be equal or higher than the one contain in the RREQ to source node, claiming that it has a sufficient fresh route to the destination node. This causes the source node to select the route that passes through the attacker node. Therefore all the traffic will be routed through the attacker and therefore, the attacker can misuse the information or sometime discard the traffic .

Cooperative Black hole Attack in an attack in which two or more black hole nodes are working in a group. In cooperative black hole attack when in route reply the next hop information is asked than the first malicious node will present the next malicious node as its next hop, when confirmed with the next malicious node it will send the route reply packet that I m having the route to destination, but actually it don't have any information about the destination node.It is one of the most severe DATA traffic attack and can totally disrupt the operation of an Ad Hoc network.

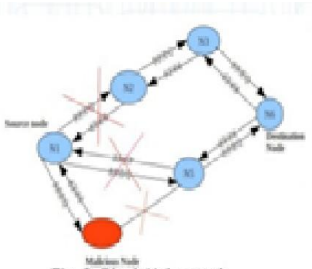


Fig. 2: Black Hole attack

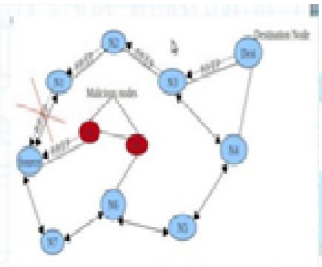


Fig. 3: Cooperative black hole attack

III. PROPOSED METHODLOGY

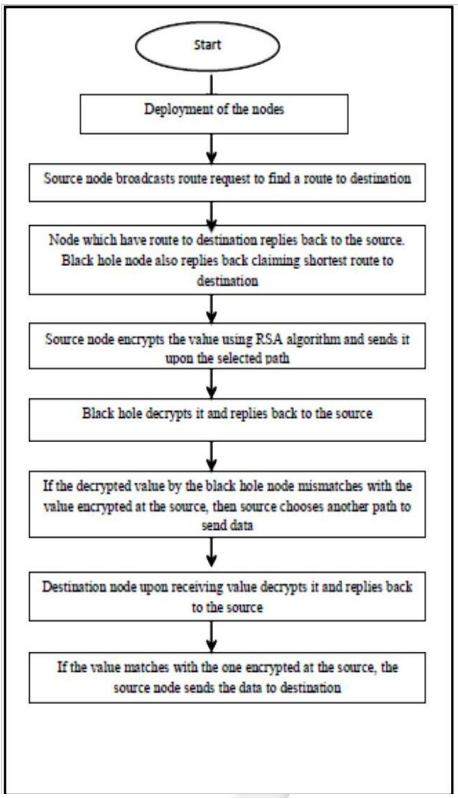
PEI (Plain Encryption Identifier)

To moderate attack in DDOS convention we are utilizing a PEI based personality framework for every hub in the network. Thus every hub in the system will have an identity. These character PEIs will be encrypted by utilizing RSA algorithm. Thus the accompanying steps will be taken:-

- First of all node will start checking the next hop. And will send the route request to find its destination node.
- After getting the route request, the next node will check is it the message from the node with PEI. Then only it accepts the request and passes it next to send it to destination.
- Then the destination node encrypts the PEI by using RSA algorithm to see the PEI number.
- If the PEI number matches then the node will accept request and send route reply to the source node.
- Black hole node will reply with the next hop address of the other malicious node (Both act as Cooperative black hole attack) to the sender node without decrypt the packet. As the PEI number is not matched. Source node declares that path an invalid path. And start sending the route request using different path.

SIMULATION RESULTS:

We will be using Ns2 (network simulator2). It provision for simulation of routing protocols. Ns2 fully simulates a layered network from the physical radio broadcast channel to high level applications. The Ns2 test system has a few peculiarities that make it suitable for our 56recreation



Four parameters are modified in our proposed work.

Packet Delivery Ratio: It is the ratio of data packets delivered to the destination to those generated by the sources. It is calculated by dividing the number of packet received by destination through the number packet originated from source. PDF = (Pr/Ps)*100, Where Pr is total Packet received & Ps is the total Packet sent.

Throughput: The throughput of the protocols can be defined as percentage of the packets received by the destination among the packets sent by the source.

End to End Delay: This includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, retransmission delay at the MAC, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across a MANET from source to destination.

$$D = (Tr - Ts)$$

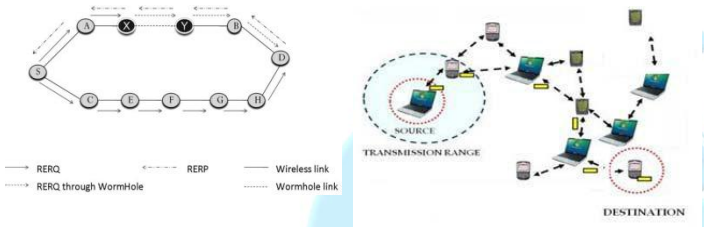
Where Tr is receive Time and Ts is sent Time

Overhead: It provides all the information that tells about the routing just like the route reply and route request. We are using PEI for every node in the network to identify the real nodes. Black hole node sends route reply packet to the source node and the encrypted value is not matched. Source

node will report that path and start sending packets through a new route. Four parameters are modified delay, packet delivery, throughput and overhead.

IV.WORM HOLE ATTACKS

Wormhole attack is one of the severe attack in network. And it is made possible by wormhole nodes which will possibly create a tunnel in between them. And once their establish communication between them, their transfer the data packets received from the source node pretending to be the actual node as a part of the network. These wormhole nodes appear to be neighboring nodes but there will be far apart from each other in reality. The wormhole nodes create an illusion, that there are neighboring nodes. And the route used by them will look like a shortest route compared to the routes used by any normal nodes. Wormhole nodes are very vulnerable which are capable of grabbing the route pretending to be the nearest node and then could drop, alter the data packets which it received from the source node. Confidentiality and authenticity for data packets provided by the MANET becomes useless against the wormhole attack. Wormhole nodes proceed further regardless of the security provided by MANET.



V.PREVENTION & MITIGATION OF WORMHOLE ATTACK

There have been few proposals recently to protect networks from worm-hole attack:

(i) Geographical leashes & temporal leashes: A leash is added to each packet in order to restrict the distance the packets are allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new leash. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet. A temporal leash provides an upper bound on the lifetime of a packet.

(ii) Using directional antenna: Using directional antenna restricts the direction of signal propagation through air. This is one of the crude ways of limiting packet dispersion.

VI.PROPOSED MODEL

Proposed model uses a mechanism to detect and avoid the wormhole attack in the Mobile Ad -hoc network where a wormhole attacker will get caught by its characteristic i.e., offering the source node fake route to destination. I named this mechanism as TAODV (Trapper Ad-hoc Distance Vector) model. This mechanism has some assumptions and is divided into three phases:

A)Pre_AODV Wormhole Discovery Phase.
B)Normal_AODV Route Establishment Phase.
C)Post_AODV Wormhole Discovery Phase

Assumptions: Wormhole attacker node does not act as source and target node. RREP will have one more field called Identity Field. Node will store next-nodes Information into log file.

A. Pre_AODV Wormhole Discovery Phase

In first phase, Bogus Route Request (RREQ) is broadcasted by source terminal with virtual destination (not existing). The malicious node (wormhole attacker node) when hears the Bogus RREQ, it will reply back RREP immediately offering shortest path to the target node. The malicious node have no interest in verifying whether virtual destination exists or not. In this model, RREP sent against Bogus RREQ will contain one more field called Identity field, which stores the identity of node that sends RREP. The legitimate nodes will not reply to the Bogus RREQ because they do not have route to the virtual destination

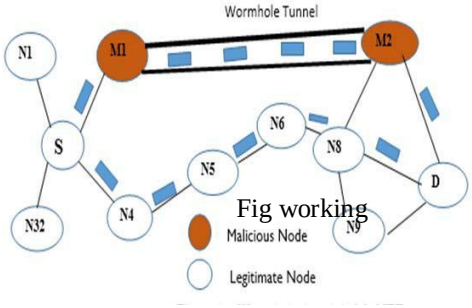
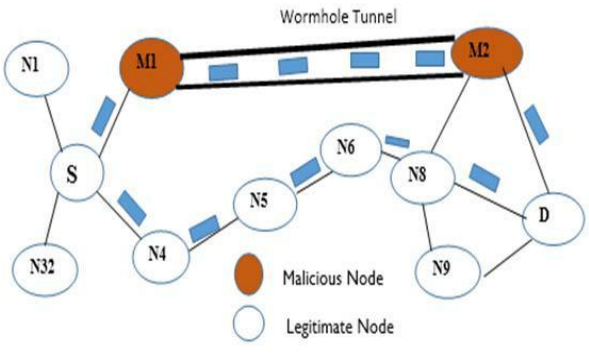


Fig working

The identity of wormhole node will be stored in identity field. if there are more than one wormhole present then their identity are put in Black list and black list containing the wormhole nodes identity will be broadcasted as an ALERT message to all the nodes in the network. So that all the nodes come to know about wormhole nodes in a network. In the Figure: 4, we have two malicious nodes that form a wormhole link i.e., M1 and M2. When the source 'S' broadcasts the Bogus RREQ to its 1-hop neighbour node M1, N1 N4, N3 are its neighbours. Here, M1 as malicious node will send back the RREP immediately without knowing anything about the destination given in the Bogus RREQ and offers the minimum the hop-count route. Legitimate nodes N!, N3, N4 will not reply because they do not have route to the virtual destination.



B. Normal AODV Route Establishment Phase

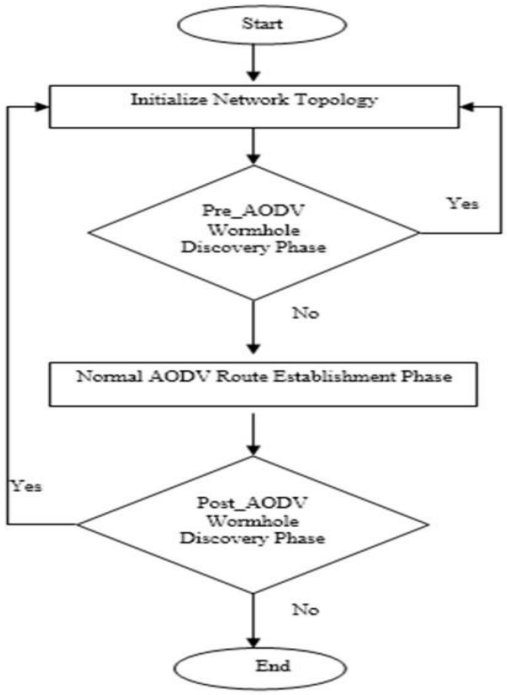
Now the network is free from wormhole attack because every node knows the **Identity** of wormhole node (malicious node)**.** When nodes will send the True RREQ to

neighbours. If the wormhole nodes sends the RREP, then its identity will be compared with the blacklist and its RREP will be rejected, hence AODV will be able to find the minimum hop count path from sender to destination which is without wormhole infected.

C. Post_AODV wormhole Discovery Phase

after making route with destination using AODV protocol, every node along the route after sending packet will also store next-node information (like delay in sending and receiving the packets) into a log file. If the delay is greater than threshold delay then wormhole is present and again phase 1 is started otherwise wormhole is not present Threshold delay can be calculated as an average delay.

Below figure Provides an overview of the security model



VII.CONCLUSION

In this research paper we consider the problems of cooperative black hole and warm hole attacks in MANET. We proposed a solution to detect and prevent these attacks. This paper reviewed several concepts, efficiency of algorithms, problems and solutions proposed by several scholars The issues and security attacks mentioned above in paper is development topic for researcher's. . As mobile ad-hoc network becoming widest area of research, lots of modifications are occurring day-by-day. As routing protocol is key concept in MANET, security solutions for this is researcher's main aim

REFERENCES

[1] Lidong Zhou and Zygmunt J.Haas "Securing Ad Hoc Networks", IEEE Network 1999

[2] Ram Ramanathan and Jason Redi, "A Brief Overview of ad hoc networks: Challenges and Directions", IEEECommunication Magazine 2002.

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing security in Wireless Ad-hoc Network" , University of Cincinnati. IEEE Communications Magazine,October 2002

[4] Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Network" The institute of Electrical Engineers.Printed and published by IEEE.2003

[5] Animesh Patcha and Amitabh Mishra "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks", 2003 IEEE

[6] Bounpadith kannhavong et al, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless
Communication, October 2007.

[7] Hesiri Weerasinghe and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Member of *IEEE* Department of Computer Science and Engineering Oakland University RochesterMI 48309 USA, July 2008.