International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 4– No.10, December 2012 – www.ijais.org

Securing AODV against Wormhole Attack using Token based Approach

Mohit Kumar
Computer Science & Engineering
Amity University, Lucknow

Nidhi Shalya
Computer Science & Engineering
Amity University, Lucknow

ABSTRACT
In present scenario, ad hoc network become the prominent mode of communication for mobile devices. Hence, becoming a elementary field of research. Since ad hoc networks are infrastructure less networks and the nodes in ad hoc networks are connected by a wireless links. As nodes are connected by wireless links, its becomes easier for attacker to disrupt in the ad hoc networks. Therefore security is the major issue in ad hoc networks as compared to wired network. In this paper, we are discussing the various attacks which are possible in MANET due to fabrication and worm hole attack in AODV and how to secure AODV against wormhole attack using token based approach. The propose method reduces the packet loss due to malicious nodes to a considerable extent and hence enhance the performance.

Keywords
Ad hoc, AODV, MANET

1. INTRODUCTION
Opposed to the infrastructure wireless networks where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET is a kind of wireless ad hoc network [1][3]. Multi hop paths are used for communication in MANET[1][2]. Mobile ad hoc networks uses radio waves to transmit signals. Mobility, an advantage of wireless communication, gives a freedom of moving around while being connected to a network environment. Mobile ad hoc networks are so flexible that nodes can join and leave a network easily. But this flexibility of mobile nodes, results in a dynamic topology that makes it very difficult in developing secure ad hoc routing protocol. Security being a serious issue, the nature of mobile ad hoc network makes them extremely vulnerable to adversaries malicious attacks. First of all the use of wireless links renders a mobile ad hoc network to be vulnerable to attacks of various types worm hole attack is one of them. A worm hole attack[4] is particularly a severe attack on MANET routing where two attackers, connected by a high speed off-channel, are strategically placed at different ends of a network. These attacker overhear the packets at one end and replay them at other end using high speed off-channel link.

2. TYPES OF ATTACK
There are various attacks which are possible in MANET. Some of the intense attacks on MANET are discussed here:

1. Black hole attack: In black hole attack [4][5], a node acts as a malicious node, this malicious node advertise itself that it is having a fresh route to destination node, even though the route is suspicious. It exploits the mobile ad hoc network routing protocol. It receives all the packets from the source and drop them, or either change information and forward it to a destination. It is a kind of Denial of Service(DOS) attack.
2. Gray hole attack[6]: It is a deviation of black hole attack in which malicious node[7] broadcasts itself as having a valid route to the destination. It then receives all packets from the source node, forwards most of them but drops only few packets which are to be forwarded to some specific destination. This malicious behaviour can be exhibited by the node for some time and later it may behave normally. Hence, this type of attack is difficult to detect.
3. Byzantine attack: The malicious nodes in the type of attack may work collectively or in isolation. They may create routing loops, or drop the packets selectively. Also they can route the packets on non-optimal routes. Byzantine failures[6] are difficult to detect as it seems to the user that the network is operating properly.
4. Worm hole attack: In worm hole attack, an attacker records the packet from one location and disrupts the flow of packet by transferring it to another location. In this type of attack, generally two or more attackers are connected by high speed off-channel link which is known as wormhole link. It is very difficult to detect worm hole attack in MANET. It is a kind of replay based attack.

3. WORM HOLE ATTACK IN AODV
Worm hole attack [2][8][9] is a kind of replay attack which is severe attack that disrupt the normal flow of the packet in the network. In worm hole attack two attackers are connected by high speed off- channel link which is known as wormhole link.

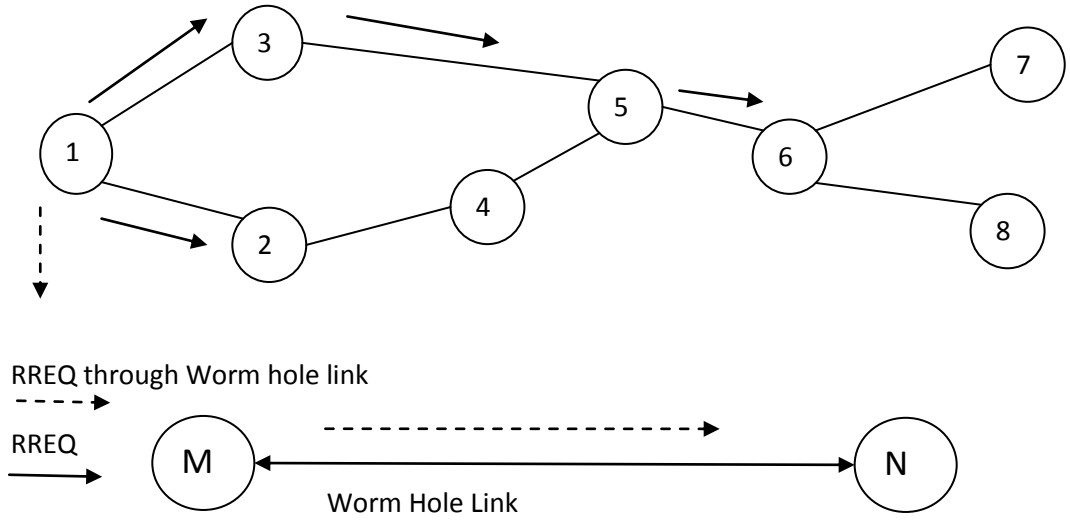

Fig 1: Worm Hole Attack

In fig1 , M and N are two remote malicious nodes. M and N are connected via wormhole link and these attackers target to attack the source which is node 1. In the route discovery process, node 1 advertise RREQ to a destination which is node 6 in this case. Here, node 3 and node 2 are neighbours of node 1, they receives RREQ from node 1 and forwards the RREQ to their neighbours. Here the malicious node M records the RREQ from node 1, and then malicious node M forwards the RREQ via wormhole link to its partner N. Malicious node N then forwards RREQ to its neighbour node 6 which is a destination node. RREQ packet is also forwarded through node 3 and node 5 to the destination node 6. But, M and N are connected by high speed wormhole link, RREQ reaches first to node 6 from N. Hence, node 6 discards the RREQ packet that reach later and choose the route through M and N which are malicious nodes. To set up a worm hole attack is not difficult and is harmful for MANET routing protocols. Once the worm hole attackers have control of link, they can do many things to disrupt the network. Attacker can forward packets out of order. Attackers can also drop packets, their link is supposed to be forwarding.

4. TOKEN BASED APPROACH TO SECURE AODV

In AODV the route is discovered in two phases, firstly the source node advertises the RREQ packet in the whole network and each intermediate node readvertises the packets. Secondly, when the destination node receives the RREQ packet, it sends the RREP packet in the reverse path of RREQ.

Once the route is defined in between source node and destination node, the next step is to authenticate the sender and receiver. To authenticate the sender and receiver, here we use the double encryption technique to increase the security level against the wormhole attack. The term we use here is :

PU_a & PU_b = Public key of Sender and Receiver

PR_a & PR_b = Private key of Sender and receiver

S_k = Session key

G_t = Generated time

Double Encryption:-

Double Encryption[10] use two keys, say K1 and K2. It does perform the encryption on the original Plain text using K1 to get the encrypted text. It again performs encryption on the encrypted text, but this time with the other key K2. The final output is the encryption of encrypted text (i.e. the original plain text encrypted twice with two different keys). This is shown in the fig2.

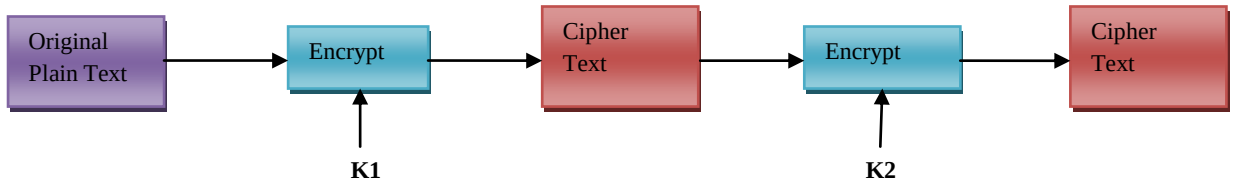

Fig 2: Double Encryption on Original Plain Text

In proposed technique, session key and generated time will be stored in the token. This token is issued by the issuer, if issuer is convinced about the security level of sender or subject node. This token is encrypted with the Receiver's public key and the whole token is encrypted with Sender's Private key, if the sender's private key is authorized that token will be decrypted by the sender's public key. Now the whole token is decrypted by the receiver's private key.

$$D_{PUa}\ [\ E_{PRa}\ [D_{PRb}\ [PU_b\ ,\ S_k\ ,\ G_t]]]$$

Session Key[10] is one time Key, if there is any delay in the transmission that key will be expired and packet will be loosed. At that time the subject node will record the activity of next node, if the RREQ is hold by the node more than the time interval, session key is expired at that node, that node is treated as suspicious node. The response of expire token is automatically generated and received by the receiver with the suspected id.

The Token will be encrypted by the private key of sender so that we called token as digital signature certificate.

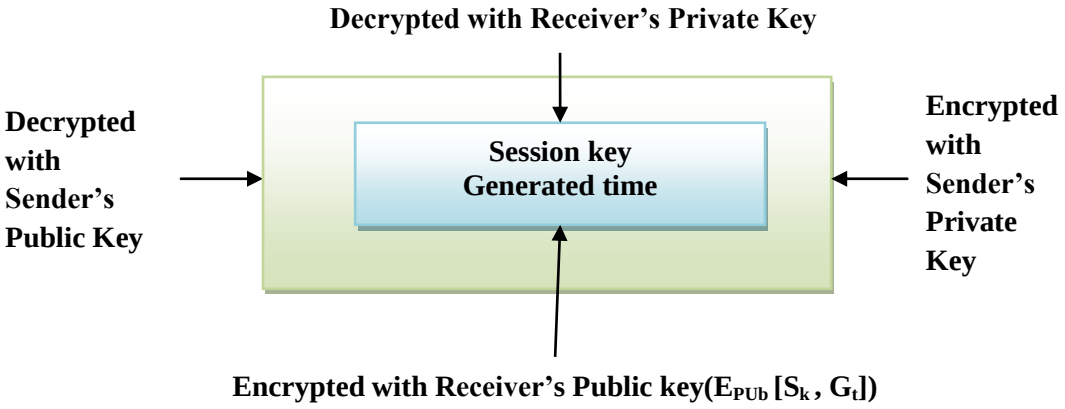

Fig 3: Digital Signature Certificate (TOKEN)

The expired Token will be generated by the issues only if it is requested by the authorized node otherwise that token will be treated as revoked and saved in the issuer's database.

After the token process, the destination node sends authenticated message append with the token received from the corresponding node. The token RREP packet will be in the form of:

[Source id, next hop id, final destination if, and the token chain]

The entire node performs the same procedure until the final source is reached. When the source receives the packet, it checks the whole token chain. If there is no problem with this chain, source node trusts the route and send the packet through this route.

5. CONCLUSION

Mobile ad hoc networks have wide applications these days. Many of these applications are vital and hence it is essential that the network operates securely even in the presence of malicious attackers. Amongst the various attacks to which the network is susceptible the wormhole attack is one of the most serious attacks which threatens the security and constancy of ad hoc networks. Also, the wormhole attack is considered as the main disruptor in the process of detection of the fellow nodes. Many basic ad hoc network functions and operations rely on accurate neighbourhood discovery, hence it is extremely important to defend ad hoc networks from wormhole attacks and ensure secure neighbourhood creation. In this paper we presented the token based approach to make

AODV routing protocol wormhole secure by using double encryption technique.

6. REFERENCES

[1] Jeoren Hoebeke, Ingrid Moeman, Bart Dhoedt and Piet Demester " An Overview of Mobile Ad hoc Networks: Applications & Challenges."

[2] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah " MANET Routing protocols & Wormhole Attack against AODV." IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010

[3] Mohit Kumar, Rashmi Mishra "An Overveiw of MANET: History, Challenges & Applications." Indian Journal of Computer Science and Engineering (IJCSE) ISSN : 0976-5166 Vol. 3 No. 1 Feb-Mar 2012

[4] Vivek Sharma, Amit Baghel "A Review of Security Attacks in MANET's." Vol-II No. 2 (58-63) : (2011) Oct-2010-Jan-2011

[5] Mehdi Medadia, M.H. Yektaie, A.M. Rahamani "Combat with Black Hole attack in AODV Routing" 978-1-4244-4570-7/09 - 2009 IEEE

[6] G.S. Mamatha, Dr. S.C. Sharma " Network Layer Attacks & Defence Mechanism in MANETS – A Survey." International Journal of Computer Science and Security, Volume (4): Issue (3)

[7] Radhika Saini, Manju Khari " Defining Malicious Behaviour of a node & its defensive methods in Ad hoc Networks." International Journal of Computer Applications(0975 – 8887) Volume 20 – No.4, April 2011.

[8] Farid Nait- Abdesselam, Brahmin Bensau "Detecting & Avoiding Wormhole attacks in Wireless Ad hoc Networks." 0163-6804/08 IEEE Communications Magazine, April 2008

[9] Ritesh Maheshwari, Jie Gao, Samir Das " Detecting wormhole attacks using Connectivity Information." 0743-166X/07 IEEE Communication Society , IEEE INFOCOM 2007.

[10] William Stallings "Cryptography and Network Security", Fourth Edition, Pearson Education. ISBN 978-81-7758-774-6, 2006