International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Volume 1,Issue 1 : Page No.17-20 , May –June 2012
https://www.mnkpublication.com/journal/ijlrst/index.php

SECURITY ISSUE RELATED TO THE ADHOC NETWORK - A REVIEW

Sonu Kumar[1], Ajay Kumar Singh[2], Seema Rani[3]
[1,2,3]Assistant ProfessorCSE Deptt. Ambala College of Engineeing and Applied research
India

Abstract - Adhoc network ai type of warless network that is used for mobile computing. Mobile ad hoc networks (MANET) have been generally regarded as the most popular network model for group communication. However, the security deployment for MANET operations is knotty. The traditional system not provide the solution that can be applied to work as adhoc network. These are mostly due to resource poorness of these networks. For temporary establishment of network adhoc network is used. We first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it easier to suffer from attacks than traditional wired network. Many type of attack can be deployed on this network. wormhole is the type of attack that can be break the security of the adhoc network. The paper deal with the wormhole attack on the adhoc network.

Keywords- Ad hoc network, leashes, routing, wormhole

I. INTRODUCTION

In recent years there has been exponential growth of Mobile Computing Devices (MCDs). MCDs mainly include laptops, Personal Digital Assistants (PDAs) and handheld digital devices. This has impelled a revolutionary change in the world of computing. The concept of omnipresent MANETs emerges. The concept of MANETs has become one of the research hotspots in the society of computer science and engineering. A mobile ad hoc network consists of a set of mobile hosts. They carry out basic networking functions like packet forwarding, routing and service discovery without the help of an established infrastructure. Such networks are frequently viewed as key communication technology enabler for network centric warfare and disaster relief operations. As the technology is burgeoning MANETs are increasingly reaching many other applications in areas like intelligent transportation systems and fault tolerant mobile sensor grids. Unlike conventional networks ad hoc networks do not depend upon any kind of preset infrastructure to operate. Communication is generally done via wireless links. In this nodes within radio range coordinate to create an implicit and momentary infrastructure for data routing and dissemination. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges. The nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. This suppleness, along with their self organizing capabilities are biggest strengths of MANETs. But it poses their biggest security weaknesses.

II. SECURITY WOES

Ad hoc networks are among the most challenging research problems from the security viewpoint. Resembling their wired counterparts MANET nodes are autonomous computer systems. They are susceptible to the same vulnerabilities. They are prone to the same types of failures as their wired counterparts. In addition they have following specific issues:-

1) No central control exists in MANET: In a pure ad hoc environment, there is no trusted third party in the network. All the nodes are equally likely. The absence of third party causes major difficulty in our security deployment. The public key cryptography which provide authentication has to be constructed with the help of certification centre or Certification Authority (CA). CA is a trusted third party. Without a CA, there is no way to authenticate the linkage between the public key and key holder. In this sense, integrity and non repudiation are compromised.

2) Unreliability of wireless links between nodes: Due to the limited energy supply for the wireless nodes, the wireless links between mobile nodes are unreliable.

3) *Constantly changing topology*: Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly. The nodes can continuously move in and out of radio range of other nodes in ad hoc network and this movement will eventually result in change in routing tables all the time.

Publication History
Manuscript Received : 15 May 2012
Manuscript Accepted : 16 June 2012
Revision Received : 25 June 2012
Manuscript Published : 30 June 2012

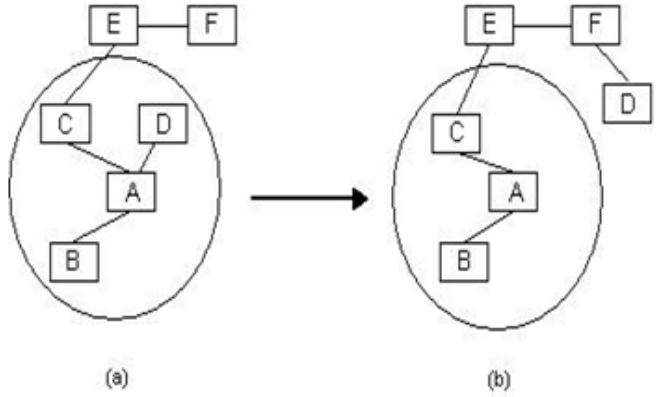

Fig. 1. Changes in topology of MANETs

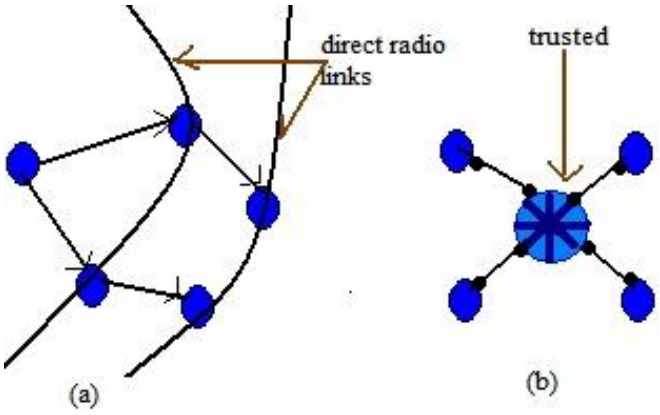

Fig. 2. (a) Routing in ad hoc networks, (b) Routing in conventional networks

4) ***Routing protocols are distinct:*** Survey of literature shows that there are more than a dozen different routing protocols. Protocols of these are based on different routing algorithms. They share no common attributes. Therefore, an authentication scheme designed for certain types of routing protocol will not be applicable to others. On the other hand, a general authentication scheme designed without considering the nature of protocols will result in huge waste in routing operation overhead.

III. SECURITY GOALS

These are defined as follows;

1) ***Availability:*** Ensures continued existence despite Denial Of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to meddle with communication on physical channel. On network layer the attacker can disrupt the routing protocol.

2) ***Confidentiality:*** Ensures certain information is never disclosed to illicit entities.

3) ***Integrity:*** Message being transmitted is never sullied.

4) ***Authentication:*** Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node. Thus, it gains unauthorized access to resource and sensitive information. It interfers with operation of other nodes.

5) ***Non repudiation:*** Ensures that the original sender of a message cannot deny

IV. KEY MANAGEMENT AND ROADMAP

In general, security goals in ad hoc networks are achieved through cryptographic mechanisms such as public key encryption or digital signature. These mechanisms are supported through centralized key management. In this CA provides public key certificate to mobile nodes. These nodes can develop mutual trust between one another. Any tampering with CA can easily compromise the security of the entire network. The proposed mechanisms used for identification such as shared secret, public key cryptography, third party authentication provide partial solution, as they are vulnerable or unable to scale. All proposed solutions require that the mobile users make proper usage of cryptographic keys. However, these mechanisms are not sufficient by themselves. There can be two major approaches.

(i) Take advantage of redundancies in the network topology (i.e., multiple routes between nodes) to achieve availability. Nodes will unlikely be all compromised. Consensus of at least (t+1) nodes is trustworthy.

V. TYPES OF ATTACKS

Use of wireless links renders MANETs susceptible to link attacks ranging from passive eavesdropping to active impersonation .Security exposures of ad hoc routing protocols are due to two different types of attacks: Active attacks: Through this the misbehaving node has to bear some energy costs in order to perform some harmful operation. Active attacks could range from deleting messages, injecting flawed messages etc. Thus, they violate availability, integrity, authentication and non repudiation.

Passive attacks: These mainly consist of lack of cooperation with the purpose of energy saving.

Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish. A more subtle type of active attack is the creation of a tunnel (or wormhole) in the network between two colluding malicious nodes linked through a private connection bypassing the network. There are various types of attacks in ad hoc networks .One of the most threatening type is wormhole attack.

Wormhole attacks are one of most easy to deploy for such an adversary. It can cause great damage to the network. In this paper wormhole attack is presented. Efforts will be made to find solution to the problem.

VI. WORMHOLE ATTACK

In wormhole attack an adversary establishes a low latency link between two points in the network. The adversary eavesdrops on messages at one end of the link, referred to as the origin point, tunnels them through the wormhole ink and replays them at the other end of the link, referred to as the destination point. In a wormhole attack, the devices and wormhole links deployed by the adversary do not become part of the network. Hence, they do not need to hold any valid network Ids and cryptographic quantities to perform the attack. The lack of key compromise makes the wormhole attack invisible to the upper layers of the network.

(i) Wormhole Threats against Network Protocols: The Wormhole attacks disrupt various network protocols and applications including routing protocols such as DSDV or ADV. The Fig. 3 shows a 10 node ad hoc network and a wormhole link between node s4 and s8.

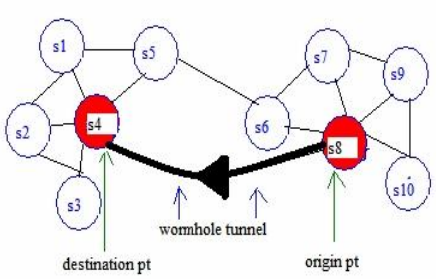

Fig. 3 10 node ad hoc network and a wormhole link between node s4 and s8.

If the routing table of node S8 is tunnelled through the wormhole link, node s4will assume that node s9 is a one hop neighbour. Node s2 will update its routing table entries for one hop neighbour node s8, and nodes {s7, s9, s10} are now reachable via two hops. Similarly, other neighbours of s4 will adjust their own routing tables. Node s2 will update its routing table entries for one-hop neighbour node s8, and nodes {s7, s9, s10} are now reachable via two hops. Similarly, other neighbours of s4 will adjust their own routing tables.

Note: Nodes {s1, s2, s3, s5} will now route via s4 to reach any of the nodes {s6, s7, s9, s10}. Hence, with nominal resources, an attacker can redirect and observe a large amount of traffic as desired. Furthermore, by simply switching the wormhole link on and off, the attacker can trigger a route oscillation within the network. Thus, it leads to a DoS attack.

These examples show that a wormhole in essence creates a communication link between an origin and a destination point that could not exist with the use of the regular communication channel.

(ii) Detecting Wormhole Attack: The most widespread method to detect wormholes is to employ the notion of packet leash. A leash is the information that is added to a packet designed to restrict the maximum allowed transmission distance of the packet. Leashes are designed to protect against wormholes over a single wireless transmission; when packets are sent over multiple hops, each transmission requires the use of a new leash. When packet leashes are used, the first node to receive the packet after it leaves the wormhole detects that the packet has travelled too far. Hence, the wormhole is detected. Leashes are classified under two categories. These are geographical and temporal. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. The sender includes its location and the current time in each packet.

At the receiving end, the timestamp is compared to the current time. If the sender and receiver are synchronized to within the required range and the maximum velocity of any node is known then the receiver can calculate the upper bound on the distance between the sender and any valid receiver. If the receiver is valid, the packet is accepted, otherwise it is dropped. An attacker who pretends to reside at multiple locations can be caught and blacklisted when geographical packet leashes are used in conjunction with digital signatures. A legitimate node overhears the attacker claiming to be in different locations that would only be possible if the attacker could travel faster than the maximum node velocity. The evidence can then be presented to other nodes. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed of light. The sender includes a packet expiration time in each packet. The expiration time is calculated based on the desired length of the packet leash and the speed of light. This value is compared to the current time at the receiving node. If the expiration time has passed the packet is dropped. Tight synchronization can be provided by a number of currently available technologies including GPS. One issue arises when contention based MAC protocols, such as IEEE 802.11, are used. In this case the user cannot know the exact transmission time far enough in advance to generate digital signatures. A very efficient signature must be used in this case. Either type of leash can prevent the wormhole attack.

(i) Other methods: A solution towards wormhole attacks is by the use of directional antennas. When these directional antennas are used, nodes use definite sectors of their antennas to communicate with each other. Therefore, a node receiving a message from its neighbour has some information about the location of that neighbour and hence knows the relative direction of the neighbour with respect to itself. Wormhole discovery becomes easier with this additional information in comparison to nodes with omni directional antennas. This approach does not require either location information or clock synchronization, and is more proficient with energy requirements. Neighbour verification methods can also be employed. The main drawback of this model is that it is always not possible to use nodes with directional antennas, as discussed earlier that manets are infrastructure less and dynamic.

A method similar to temporal packet leash technique is

SECTOR It is proposed by Capkun et al. It is based on the time of flight of individual packets. Wormhole attacks are feasible because an attacker can make two far apart nodes see themselves as neighbours. This method use specialized hardware that enables fast sending of one bit challenge messages as to minimize all possible processing delays. It determines distance between two communicating nodes using a distance bounding algorithm. It can be used to thwart these attacks in MANET without any clock synchronization or location information. It measures round trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determines whether the calculated distance is within the maximum possible communication range. To verify distance between the nodes, each node sends a one bit challenge to the nodes it' encounters', and waits for a response. A receiving node immediately sends a single bit reply.

Location Aware Guard Nodes (LAGNs) is another scheme to prevent the wormhole attacks. It is proposed by L.Lazes et al.. They employ the guard node to detect the message flow between nodes. A node can detect a wormhole attack using single guard property and communication range constraints property during the fractional key distribution .They consider that a node receives an identical message more than once because a malicious entity replays the message. The main consideration is the communication range. If any two guards within the area where guards heard to nodes are located and the area where guard hears at the origin point of the attack are located have a distance larger than double of radius range, there may be a malicious node. In simple, a sensor cannot hear two guards that are more than 2R apart. Their system's weak is that the guard nodes are required to know their location. Lazos's method is fine. However, it seems more apt for dense stationary networks.

N. Song et al. Proposed another detection technique called, "Statistical analysis (SAM)". This technique is mainly based on the relative frequency of each link in the set of all obtained routes. The difference between the most frequently appeared link and the second most frequently appeared link in the set of all obtained routes is calculated. The maximum relative frequency and the difference are much higher under wormhole attack than that in normal system. The two values are together to determine whether the routing protocol is under wormhole attack. This method neither requires special hardware nor any changes to existing routing protocols. These factors allow for easy integration of this method into intrusion detection systems.

VII. CONCLUSION

The emerging technology plays a vital role in bringing the new paths to fast and speedy data transfer. It also provides new ways to penetrate the security issues of vital concern for every organization. So, before opting for any technology it becomes necessary to consider its security issues. So, that the latter on the problems can be handled easily and cost effective way.

Wormhole attacks can cause great damage to the network. In this paper wormhole attack is presented. Efforts are made to find solution to the problem. The proposed solution can handle the security issue of the ad hoc network

REFERENCES

[1] Yongguang Zhang, Wenke Lee ,"Intrusion detection in Wireless Ad-hoc networks."

[2] L.Zhou ,Z.J Haas ,"Securing Ad-hoc Networks".

[3] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[4] Y.hu A. Perrig and D. Johnson , Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in Proceedings of IEEE INFOCOM'03, 2003

[5] Ad hoc networks from Wikipedia, the free encyclopedia

[6] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[7] Mehdi Khosrow, "Encyclopedia of Information Science and Technology",Second Edition, volume 5.

[8] Arun Kumar Bayya, Siddhartha Gupte ,"Security in Ad-hoc Networks".

[9] N.Asokan, Philip Ginzboorg "Key Agreement in Ad-hoc Networks". [10] Michael Steiner, Gene Tsudik, Michael Waidner, IEE Computer Society, "Key Agreement in Dynamic Peer Groups".