SECURITY IN AD-HOC NETWORKS

Raja Iswary[1], Rohit Kumar Das[2]

[1]*Department of Information Technology, Assam University, Silchar*
[2]*Department of Information Technology, Assam University, Silchar*

Abstract

On wireless computer networks, ad-hoc mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicated in peer-to-peer fashion. One main challenge in design of these networks is their vulnerability to security attacks. The growing popularity and widespread applications of wireless networks are directly proportionate to their propensity for security exploitation. In this paper we have discussed about the potential attacks and security issues of routing protocols face by ad-hoc network.

Keywords: *Ad-hoc network, Network Attacks, Routing Protocols*

--***--

1. INTRODUCTION

An ad hoc network is made up of multiple “nodes” connected by “links”. An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. Basically, an ad hoc network is a temporary network connection created for a specific purpose (such as transferring data from one computer to another). An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. As the medium of transmission is wireless the security aspect for this type of transmission is very high and is one of the major concerned issues. In this paper, for the first section we will see some of the security aspects for the ad-hoc network, the second section is be consisting of the vulnerable attacks and then the routing protocols.

2. SECURITY IN AD-HOC NETWORK

2.1 Network Availability

Services should be available whenever required. Availability is a key concern in wireless network security. It relates to the survivability and operability of a wireless network.

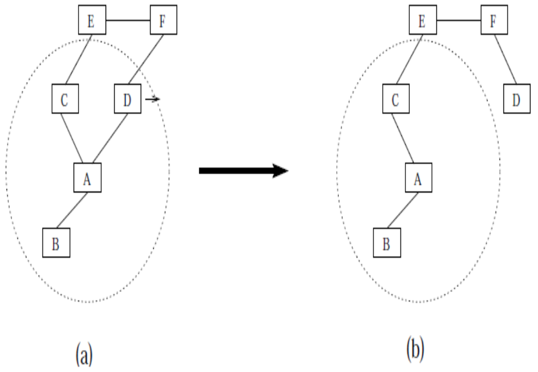

Fig 1: Topology change in ad hoc networks: nodes A, B, C, D, E, and F constitute an ad hoc network.

The circle represents the radio range of node A. The network initially has the topology in (a). When node D moves out of the radio range of A, the network topology changes to the one in (b) Availability ensures not only operational efficiency, but also data delivery. This is usually done by the routing protocol. [2]

2.2 Integrity

Data which are being transmitted over the wireless ad-hoc network are integrated in such a way that they cannot be corrupted.

2.3 Authentication

Authentication is the ability of a node to identify the node with which it is communicating. If authentication process is not enabling then the attacker could gain unauthorized access to resource and can get sensitive information of other nodes.

2.4 Confidentiality

It ensures that some sensitive information is never disclosed to any unauthorized users.

2.5 Non-repudiation

Non-repudiation states that the sender of the message cannot deny having sent it. Non-repudiation is useful for detection and isolation of compromised nodes. [4]

3. ATTACK ON AD HOC NETWORK

3.1 Denial of Service Attacks

A denial of service attack is the most common attack to deny network availability. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. As Wireless devices use CSMA/CA protocol to transmit data. If a user wants to transmit data must first listen to the channel to check for activity. If the channel is idle, the user can begin transmission. Otherwise, the user must wait until the channel is free. By design most wireless devices share the communication medium. However, it is possible for a device to constantly transmit energy on the frequency of a wireless network, making the channel unavailable. This effectively denies all service (data transmission) on the network. There is no realistic protection against such an attack. If a node has the appropriate hardware, a DoS attacked can be mitigated. If the channel remains unavailable for a predetermined amount of time, an alternative channel (RF) may be used.

3.2 Passive Attack

The passive attacks only intercept the message transmitted in the network without disturbing the transmission. The attacker will be able to analyze the valuable information like network topology to perform further attacks. Unfortunately, this kind of attack in wireless network is impossible to detect due to the nature of wireless network that its medium is air which is widely open to every user within the domain. Passive attacks threaten confidentiality of data.

3.3 Active Attack

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. This threat violates the security of the system. Some examples of active attacks are data interruption, interception, modification and fabrication.

3.4 Wormhole Attack

This is a network layer attack where the attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. There are several variations to the wormhole attack. Such as Wormhole using Out-of-Band Channel, Wormhole with High Power Transmission, Wormhole using Packet Relay, Wormhole using Protocol Deviations. [3]

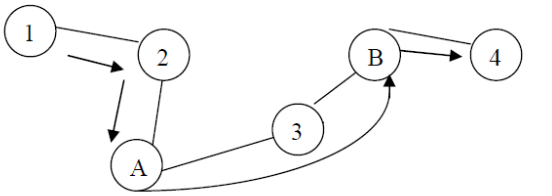

Fig 2: Wormhole attack

3.5 Blackhole attack

Here a node provides an arbitrary false shortest path route replies to the route requests it receives. These fake replies can be use simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets. The attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing.

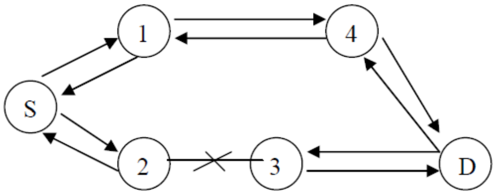

Fig 3: Blackhole attack

3.6 Location Disclosure

The actual location of a device needs to be kept hidden for reasons of privacy of the user. In this approach, an attacker is able to detect the location of nodes or may even get the entire structure of the network.

3.7 Packet Replication

This attack fall under the routing attack category where the stale packets are replicated which require additional bandwidth. This results in confusion in the routing process as it will be difficult to identify which of the packet to forward to the other nodes. [4, 5]

4. EXPLORATION OF SECURITY CONCERN IN AD-HOC NETWORK USING ROUTING PROTOCOL

A clear distinction exists between a wired and wireless when it comes to a routing protocol mechanism. Routing in traditional wired networks with fixed infrastructure when compared with a wireless faces certain problems. A limitations imposed by the Ad-hoc infrastructure as whether or not a routes records need to be created, whether or not a routing protocol should depend on a centralized entity or a routing protocol should be energy efficient imposes a serious concern. Thus, knowing the fact that this limitation are indeed serious concern so mechanisms that are operable in a most suitable ways are proposed as most existing routing protocol follow up two different approaches that deal with an Ad-hoc networks: the table driven and the source-initiated on-demand approaches. [6]

4.1 Proactive Routing Protocols (The Table Driven)

A Clear and consistent view of the network topology by propagating periodic updates and maintaining at all times routing information regarding the connectivity of every node to all other nodes that participate in the network follows a Proactive Mechanism. This provides a quick way to route data across the network which turns out to be an expensive one in a small network as minimal of activity involved in it.

Some Classification based on Proactive Routing Protocol:

4.1.1 Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)

In this approach each and every nodes that are within the network maintains a routing table information containing each destinations and the number of hops required which follows a Bellman-Ford routing algorithms. Every significant change are propagated as each node broadcasts its routing table where updates are sent in either full or incremental dumps i.e. in case of full dump the entire table is sent and in case of incremental only the routing data that has changed are sent.

4.1.2 Wireless Routing Protocol (WRP):

WRP uses an enhanced version of the distance-vector routing protocol, which uses the Bellman-Ford algorithm to calculate paths. The tables that are maintained by a node are the following: Distance table (DT), Routing table (RT), link cost table (LCT), and a message retransmission list (MRL). The protocol introduces mechanisms which reduce route loops and ensure reliable message exchange. To overcome the count-to-infinity problem and to enable faster convergence, it employs a unique method of maintaining information regarding the shortest distance to every destination node in the network and hop node on the path to every destination node.

4.1.3 Global State Routing (GAR):

In Global state routing the entire network is not flooded as is the case with Dynamic Destination-Sequence Distance-vector routing. Here three tables are maintained for each node: a neighbor list, a topology table, a next hop table and a distance table.

4.2 Reactive Routing Protocols (Source-Initiated on-Demand):

In this approach a source node initiates a rote discovery function where a route is created only when the source node requires a route to specific destinations. Being a less resource intensive as compared to Proactive routing there is no need of periodic transmission of updates as information responds are achieved when demand arises.

Some Classification based on Reactive Routing Protocol:

4.2.1 Ad Hoc on-Demand Distance Vector Routing (AODV)

DSDV is improved an enhanced by AODV. It is a Reactive routing protocol, meaning that it establishes a route to a destination only on demand. AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV. AODV is capable of both unicast and multicast routing. In AODV based on the demand for route information the Broadcast is minimized. Its simplicity is that when broadcasting RREQ packet between a source and destination an immediate node receives and forwards it to the destination.

4.2.2 Dynamic Source Routing

Dynamic Source Routing' (DSR) is a routing protocol which forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. This protocol is truly based on source routing whereby all the routing information is maintained at mobile nodes. It has only two major phases which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node.

Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach.

5. ROUTING PROTOCOL SECURITY

The determination of the flow of data from node to node can be obtained through the routing protocol. As the flow of data from source to destination passes through many intermediate nodes in a wireless environment it is prone to be intercepted. So security aspects need to be improved for secure communication. A number of security measures are undertaken to limit the risks.

Encryption: Making a data secure follows the mechanism of Encryption where a data that a sender wants to sent towards its destination needs to be encrypted such that the data is not easily broken or known to the outside world. On the other side i.e. at the destination the data is easily broken down by the decryption mechanism.

Depending upon the Energy required, Memory and Computation Power the techniques like RSA and Diffie-Hellman are use for Encryption-Decryption mechanism.

Authentication: In a wireless environment a node makes itself authenticated to other available nodes by creating neighborhood tables where the various identification numbers are include in the table. The sending node enters its own identification number and sends towards the destination. Once the identification number is verified using the neighborhood table by the receiver the data is forwarded to the destination.

Authentication-Encryption: Combining the features of both Authentication and Encryption a more secure way of communication among the nodes can be achieved and prevent nodes from being intercepted. Using the similar authentication technique mentioned above, the transmitting node includes its identification number and that same number encrypted in the data header. When the receiving node receives the data, it verifies the sender's node identification and decrypts the encrypted identification number. If both identification numbers match, the data is forwarded.

These are the most basic techniques in securing the data in Ad-hoc network.

6. SECURE ROUTING PROTOCOLS:

With respect to the performance and security a secure routing protocol offers additional features in regards to security in Ad-hoc Mobile network and also their protection from different types of Attacks. Various Secure routing Protocols that provide performance and security are as follows:

6.1 Authenticated Routing for Ad Hoc Networks (ARAN)

The detection and protection against the malicious attackers by third parties and peers in Ad-hoc environment guarded by ARAN by performing Authentication, non-repudiation and Message Integrity. A Digital Signature is being used as it is an on-demand routing protocol. When communicating between node A wants and node Z, it broadcasts a route discovery packet (RDP). The IP field specifies the IP address of Z. The message includes A's certificate, a nonce that increases every time A sends an RDP along with a time stamp. The message is signed with A's private key. When intermediate node B receives the message, it verifies the authenticity by extracting A's public key from the certificate within the message. After checking to make sure the certificate has not expired, node B sets up a (reverse) route towards the originator A of the RDP. If this is the first time that node B has seen this message, it attaches its own certificate, signs the message with its private key and rebroadcasts the RDP. Once node Z finally receives the message, it signs the message with its private key, IP address and certificate and sends a route reply (RREP) message. Nodes unicast the RREP message to the originator A through the discovered path. As the REP traverses the path, the intermediate nodes remove the certificate and signature of the previous node. Finally, node A receives the RREP and verifies the authenticity of the response.

6.2 Secure Ad Hoc On-Demand Distance Vector (SAODV)

Source authentication, import authorization, integrity and data authentication services are provided by SAODV in which it assumes that there is a key management system (KMS) that assigns keys to the nodes, verifying the association of the public keys and the node identities. Hash chains are used to secure the hop count and digital signatures authenticate the message fields. Applying a one-way hash function to a random seed value a hash chain provides integrity for hop count.

6.3 Secure Efficient Ad Hoc Distance Vector (SEAD)

Taking into account the various limited resources (network bandwidth, processing capabilities, and memory and battery power) of the nodes SEAD provides secure distance vector routing. It uses a one-way Hash function and follows the way as DSDV performs. [1]

7. CONCLUSIONS

In today's world the wireless technology is growing in a repaid fashion because of their easy implementation and use. A technology with advantage also comes with certain disadvantages. As the medium of transmission in wireless technology is not secure so, in this paper, we have analyzed the security for an ad hoc network faces and presented the operation of routing protocol based on security prospective. Various attacks for the ad-hoc networks is been declared.

REFERENCES

[1]. Barbeau, M. and Kranakis, E. Principles of Ad Hoc Networking. John Wiley and Sons Publication . 2007.
[2]. Zhang, H., Olariu, S., Cao, J. Mobile Ad-hoc Sensor Networks: Third International Conference. Springer, 2007. MSN 2007. Beijing, China. December 12-14, 2007.
[3]. Das, V. and Vijaykumar, R. Information and Communication Technologies. International Conference, ICT 2010. Kochi, Kerala, India. September 2010.
[4]. Science Academy Transactions on Computer and Communication Networks, Vol. 1, No. 1, March 2011
[5]. Securing Ad Hoc Networks, Lidong Zhou Department of Computer Science, Cornell University Ithaca, NY 14853
[6]. Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balakrishnan, Member, IEEE, “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs” IEEE Transaction on Mobile Computing, VOL. 6, NO. 5, May 2007