Seminar Report

Security Issues in MANETs

Abhishek Seth
04329001

November12 ,2004

Abstract

Mobile Ad hoc Networks (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. A mobile adhoc network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a Mobile Adhoc Network usually seek the help of other intermediate nodes to establish communication channels. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes. The security experience from the Wired Network world is of little use in Wireless Mobile Ad hoc networks, due to some basic differences between the two Networks. Therefore, some novel solutions are required to make Mobile Adhoc Network secure.

1 Introduction

A *Mobile Adhoc Network* is a group of wireless mobile computers in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. Application such as military excercises, disaster relief, and mine site operation may benefit from adhoc networking, but secure and reliable communication is a necessary prerequisite for such applications.
MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense.
Security is a process that is as secure as its weakest link. So, in order to make MANETs secure, all its weak points are to be identified and solutions to make all those weak points safe, are to be considered. Some of the weak points and solutions to strengthen them are considered in this article. However the list is possibly incomplete, and some more weak points of MANETs are likely to be discovered in near future. So Security issues in MANETs will remain a potential research area in near future.
The rest of the paper is organized as follows. Section 2 will illustrate about MANETs. Section 4 will raise the problems of secuirity in MANETs. Further sections deals with some of the solutions to these problems. Finally Section 10 concludes this article.

2 Mobile Adhoc Networks

2.1 Introduction

Mobile Adhoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robost.
The characteristics of these networks are summarized as follows:

- Communication via wireless means.
- Nodes can perform the roles of both hosts and routers.
- No centralized controller and infrastructure.
- Intrinsic mutual trust.
- Dynamic network topology.
- Frequent routing updates.

2.2 Advantages and Applications

The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.

Some of the applications of MANETs are

- Military or police exercises.
- Disaster relief operations.

- Mine cite operations.
- Urgent Business meetings.

2.3 Disadvantages

Some of the disadvantages of MANETs are:

- Limited resources.
- Limited physical security.
- Intrinsic mutual trust vulnerable to attacks.
- Lack of authorization facilities.
- Volatile network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

2.4 Routing

The knowledge of routing protocols of MANETs is important to understand the security problems in MANETs. The routing procols used in MANETs are different from routing protocols of traditional wired world. Some of the reasons are listed below:

- Frequent Route updates.
- Mobility.
- Limited transmission range.

The performance criteria of nodes in MANETs are different than that of wired networks. Some of the performance metrics of MANET routing protocols are listed below:

- Energy consumption.
- Route Stability despite mobility.

Routing protocols in Mobile Adhoc Networks are majorly of two categories:

- Proactive Protocols
- Reactive Protocols

Reactive Routing protocols are based on finding routes between two nodes , when it is required. This is different from traditional Proactive Routing Protocols in which nodes periodically sends messages to each other in order to maintain routes. Only Reactive Protocols are considered in this article, as they are extensively studied and used in MANETs. Among many Reactive Routing Protocols, only two of them are described below as they are mostly studied.

2.4.1 Dynamic Source Routing

Dynamic Source Routing (DSR) uses source routing to deliver packets from one node in the network to some other node. The source node adds the full path to the destination in terms of intermediate nodes in every packet . This information is used by intermediate node to determine whether to accept the packet and to whom to forward it. DSR operates on two mechanisms: Route Discovery and Route Maintainance. Route Discovery is used when the sender does not know the path upto the destination. In this mechanism, the sender broadcasts a `ROUTE REQUEST` message which contains Source Address, Destination Address , Identifier. Each intermediate node adds its address in `ROUTE REQUEST` message and rebroadcast it, unless it has not rebroadcasted earlier. With this controlled broadcast, the `ROUTE REQUEST` will ultimately reaches the destination. The destination then sends a unicast `ROUTE REPLY` message in reverse direction whose information is obtained from list of intermediate nodes in `ROUTE REQUEST` message.
When the `ROUTE REPLY` packet reaches the source, it records the route contained in it and saves in its cache for the specific destination. For better performance, intermediate nodes also records this route information from the two route messages. All nodes overhearing these packet adds meaningfull route entries in their caches.
Finally, Route Maintainance Mechanism is used to notify souce and potentially trigger new route discovery events when changes in the network topology invalidates a cached route.

2.4.2 Adhoc On-demand Distance Vector Routing

Adhoc On demand Distance Vector rouing (AODV) is another on-demand protocol. It has similar mechanism of `ROUTE REQUEST` and `ROUTE REPLY` as that in DSR. However, it does not rely on source routing, rather it makes use of routing tables at intermediate nodes. The nodes maintain routing table entries of all reachable nodes in the network. The entries in routing tables are of the form: $<$ *Destination, Next Hop, No. of hops, Sequence Number*$>$. Sequence number is used to maintain freshness. The route table is used to route data packets destined for a particular node and to respond to `ROUTE REQUEST`. The advantage of AODV over DSR is that, a data packet does not need to contain whole route to the destination.

3 Security basics

Before proceeding further, the reader should have the knowledge of following terminologies of Network Security:

- Symmetric Key Cryptograpy.
- Public Key Cryptograpy.
- Authentication and Digital Signatures.
- Hash and Message Authentication Codes (MAC)
- Man-in-the-middle attack, Denial of Service Attack

4 Security Problems in MANETs

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons :

- Open Medium - Eavesdropping is more easier than in wired network.
- Dynamically Changing Network Topology - Mobile Nodes comes and goes from the network, thereby allowing any malicious node to join the network without being detected.
- Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
- Lack of Centralized Monitoring - Absence of any centralized infrastructure prohibits any monitoring agent in the system.
- Lack of Clear Line of Defense - The only use of I line of defense - *attack prevention* may not suffice. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process that is as secure as its weakest link . In addition to *prevention*, we need II line of defense - *detection and response*.

The possible security attacks in MANETs can be divided into two categories:

- **Route Logic Compromise**: Incorrect routing control messages are injected into the network to damage routing logic.
- **Traffic Distortion Attack**: All attacks that prohibits data packets to transfer from the source to the destination, either selectively or collectively comes under the category of Traffic Distortion Attack. This type of attack can snoop network traffic, manipulate or corrupt packet header or contents, block or reply transmissions for some malicious purposes.

The list of some of the attacks in MANETs is as follows:

- Jamming.
- Snooping.
- Flood Storm attack.
- Packet Modifications and Dropping.
- Repeater attack.
- Identity Impersonation.
- BlackHole attack.
- Wormhole attack.
- Rushing attack.

All these attacks are discussed in further subsections:

4.1 Jamming

Accidentally or Intentionally, interference can happen with radio waves of MANETs, because WLANs[1] use unlicensed radio frequencies (ISM band[2]). Other electromagnetic devices operating in the infrared or 2.4 GHz radio frequency can overlap with WLAN traffic. If attacker has a powerfull transmitter, he/she can generate a radio signal strong enough to overwhelm weaker signals, disrupting communications. This condition is called jamming. Jammers can be of two types:

- High power pulsed full band jammers.
- Low power partial-band jammers.

Jamming attacks can be mounted from a location remote from the targeted network. This makes this attack extremely inevitable.

4.1.1 Countermeasures

The solution to jamming is to use Spread-Spectrum technology to transmit data. Spread - Spectrum consumer more bandwidth than do narrowband transmission. It is designed to resist eavesdropping, interference, and noise. Spreading codes are used to broaden the narrow band signal. The receiver uses the same spreading code used by the transmitter to narrow down the spread signal to its original form. The 802.11 Wireless standard already uses these techniques to resist these attacks.

- Frequency-Hopping Spread Spectrum(FHSS): In this technique , a radio signal is sent over a number of channels. At a time only one channel is used, and the hopping sequence of using different channels is determined by a pseudo-random code sequence. Only receiver, who knows the code can narrow down the signal.

[1] Wireless Local Area Network
[2] Industrial, Scientific and Military band

- Direct-Sequence Spread Spectrum(DSSS): Under these technique, each data bit in the signal is transmitted as 11 bit chipping sequence (if 11 bit chip code is used), which are converted into a waveform. The waveforms are then transmitted over a wide range of frequencies. The receiver unspreads the chip to recover the original data.

Although MANETs uses spread -spectrum techniques to minimize jamming, still the problem is not solved completely because of the inherent characterisrtics of radio waves.

4.2 Snooping

Due to broadcast nature of radio signals from transmitter, it is possible to eavesdrop packets. Due to inherent trust between mobile nodes, they are allowed to look at the whole packet data. Two types of information can be obtained from snooping:

- Packet Payload data: The actual data that the packets are carrying can be eavesdrop if proper encryptions are not used. The resource constraint nature of mobile nodes generally prevent them from using strong encryptions.
- Routing information: The source and destination information from the packets may reveal the nature of communication & relationship between them. These destroys some privacy of their conversation.

4.3 Flood Storm Attack

This is a Denial of Service Attack. Malicious node deliberately floods the whole network with meaningless *Route Request*(RREQ) and *Route Reply* (RREP)messages. The purpose of doing so is two fold:

- Paralyze the network by destroying its routing logic.
- Exhaust the network bandwidth.

Such attacks are possible only because RREQ and RREP packets are not authenticated. Any body can forge such messages. The only solution for these attacks is to authenticate route control messages.

4.4 Packet Modifications and Dropping

It is possbile for intermediate nodes to modify the packet content, if proper integrity checks are not maintained. Also it is possible to change the header information including source and destination address. Any node can take the role of router, which is not the case in wired network, where dedicated machines are routers. The malicious intermediate nodes can also simply drops data or route packets. Some Variations of packet dropping based on frequency and selectiveness are given below:

- Selective dropping
- Constant dropping
- Periodic dropping
- Random dropping

4.5 Repeater attack

In this attack, a malicious node I simply replays packets of one of its neighbour A. This will result in other side neighbour (say one of them is B) assuming that the A is its neighbour, infact it is not. Two nodes are said to be neighbour if they are in transmission range of each other. Now the malicious node I can selectively replay packets between A and B, while dropping other packets. This would cause a Denial of Service for the nodes A and B. This scenerio is difficult to detect as nodes can assume that this periodic dropping is because of noisy channel. Such types of attacks can be detected by Secure Neighbour Detection Techniques discussed in further sections.

4.6 Identity impersonation

The attacker can achieve various malicious goals by impersonating another user. This is because of lack of any authentication scheme in MANETs. The IP address and MAC based identity are easy to impersonate, if underlying communication channel is not secured.

4.7 BlackHole Attack

A black hole[3] is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since a black hole does not have to check its routing table, it is the first to respond to the RREQ in most cases. When the data packets routed by the source node reach the black hole node, it drops the packets rather than forwarding them to the destination node. Such malicious node also advertises itself as having shortest path to requested node. The situation can become worse if the blackhole node declares itself as having shorter path to almost all nodes, causing the whole data traffic to end up on this node, and finally the blackhole drops all data packets. This would result in complete Denial of Service.

4.8 Wormhole attack

This attack is a generalized form of repeater attack. In this attack, an attacker records a packet, at one

[3]The word blackhole refers to black hole star which is so dense that it absorbs all light and hence appear to be black.

location in the network, tunnels the packet to another location in the network, and replays the packet from the second location. This requires the attacker to have just two nodes, connected by private tunnel. Tunneling of packet can be done either by using single long-range directional wireless link or through a direct wired link. If the distance between two end points of tunnel is greater than the radio coverage of nodes, the tunneling can always be faster than the normal multihop route between the end points of tunnel. This tunnel is refered to as *wormhole*.
Various issues are:

- Either all or selected packets are tunneled.
- Apart from packets destined to this node, other packets obtained by eaves-dropping can also be tunneled.

The wormhole between two nodes can make some distance nodes to believe that they are neighbours. Many exploits can be possible after this fraud. One powerfull exploit is to tunnel the RREQ packets from a node near the sender to some node near the destination. This prevents any routes other than through the wormhole from being discovered. This is because, tunneling of RREQ can always be done faster than the normal multihop trasnmission of RREQ. The attacker then exploit the wormhole by discarding, rather than forwarding data packets, thereby creaing a Permanent Denial of Service. No other route can be discovered as long as the wormhole is active and *first come first select* strategy is used for RREQ forwarding. This attack is always possible if distance between the sender and receiver is greater than two hops.
The thing that makes this attack very strong is that, this attack is possible even if all communication provides authenticity and confidentiality and even if attacker has no keys.

4.8.1 Power of wormhole attack

Let A and B are far apart nodes, and believe that they are neighbours because of a wormhole between them. If best existing route from A to B is atleast $2N + 2$ hops long, then any node C within N hops of A would be unable to communicate with B. This is because C would find a shortest path to B through A, with maximum hop count of $N + 1$(hop count between A and B is one because of wormhole). The other path from C to B would have a length of atleast $N + 2$ hop counts, which is less than the hop count of route selected through A, and hence rejected.

4.9 Rushing attack

In rushing attack, a malicious node wants a route to be established through it. For this purpose, a malicious M node waits for route request RREQ of sources either selectively or collectively . Whenever the RREQ arrives, the malicious node M *rushes* the request to the next intermediate node, in a hope to get a route through it. The probability of getting a route through M is higher, because of the property of all nodes to select the first RREQ and forward it, and discarding the duplicate RREQ.
If the RREQ forwarded by the attacker are the first to reach each neighbour of the target, then any route discovered by this Route Discovery will include a hop through the attacker. Note that even if secure routing is used, this attack is possible. The malicious node can achieve various malicious purposes, after a route is established through it. It includes eavesdropping (if proper encryptions not used),Packet Dropping ,and other possible attacks.
The Rushing attack acts as an effective denial-of-service attack against all currently proposed on-demand ad hoc network routing protocols, including secure routing protcols.
Some of the techniques that the attacker can use for rushing attack:

- Quickly forward the packet without following contention protocol. Contention protocols require to wait for some time before transmitting packets in order to prevent packet collisions.
- Keep the network interfaces of neighbour interfaces full by some DOS attack. This will lower the chances that the neighbours will forward RREQ packet first. One way of doing this, is to send them bogus authetication requests and keep them busy in verifying these requests.
- Attacker can employ a wormhole to rush the RREQ to the destination.

5 Ariadne - Secure routing protocol

Ariadne is a secure On-Demand Routing Protocol for MANETs. It prevents an attacker to tamper with uncompromised routes and large number of types of DOS attacks. Ariadne can authenticate routing messages using either shared secrets between each pair of nodes, or shared secrets between communicating nodes combined with broadcast authentication, or digital signatures. Ariadne appreciates use of TESLA , an efficient broadcast authentication scheme. The next subsection introduces TESLA.

5.1 TESLA

TESLA is an asymmetric broadcast authentication protocol. It is different than the traditional asymmetric protocol such as RSA. RSA operations are computa-

tionally expensive and very costly if carried on resource constrained mobile nodes. Authentication is provided using MAC[4]. MAC alone cannot be used for broadcast authentication because the receiver(s) (who know the secret key of MAC) also can forge message on behalf of sender. TESLA makes use of loose clock synchronization and delayed key disclosure for achieving its purpose.
In brief, MAC function is a many to one function, that takes message M and secret key K as arguements and produces a number called MAC. This MAC is appended to the message being transmitted. Authentication is carried out at the receiver by recalculating MAC of the message, if secret key is known and compare it with the MAC appended in message. If both MAC are same, message is authenticated.
MAC = F (M , K)
The procedure of TESLA is given below:

- Sender computes one way key chain $[K_0, K_1, ..., K_n]$ as follows

$$\begin{aligned} K_n &= Randomkey \\ K_{j-1} &= H[K_j] \end{aligned}$$

  Here K_0 to K_n are keys and H is the hash function.

- The order of publishing keys is: $K_1, K_2..., K_n$. This keys stream can be verified to come from single source by calculating hash of the key K_i and comparing it with previously published key K_{i-1}.

- Before disclosing key K_i , sender sends its packet authenticated with $MAC(K_i)$.

- The receiver, when receives packet, need to verify that its MAC key is not yet published. Loose time synchronization is required for this verification. After some time when sender publishes its key, the receiver can authenticate previously received data message.

- The sender has to publish its first key of the key chain, subsequently after which, it can be authenticated based on remaining keys of the key stream.

Thus, this mechanism provides broadcast authentication, without employing any public key operations.

5.2 Route Discovery Mechanism

This subsection describes a secure route discovery mechanism that make use of TESLA authentication. In this mechanism, the source sends a RREQ packet for the destination, which contains following : *<RREQ, initiator, target, id, time-interaval, hash-chain , node-list, MAC-list >*. Each of these parameters are explained below:

[4]MAC - Message Authentication Codes

- *Initiator* = Sender address
- *target* = Destination address
- *id* = Unique id for RREQ by sender
- *time-interval* = TESLA time interval at the pessimistic expected arrival time of the REQ at the target.
- *hash-chain* = Initialized to $MAC_{K_{SD}}$ (*initiator,target,id,time-interval*), where K_{SD} is the shared secret key between source and destination.
- *node-list* and *MAC-list* = Empty list.

Any intermediate node A when receives the RREQ checks for its validation and forwards the packet after doing following steps:

- Appending its own address, A, to the node-list.
- Replace hash-chain field with $H[A, hash-chain]$.
- Appending the MAC of entire RREQ, calculated by its TESLA key K_{A_i},corresponding to *time-interval* to the MAC-list.

Finally the target node when receives the RREQ do the following, before replying with RREP.

- Check if TESLA keys are not disclosed yet.
- Verify the *hash-chain* equal to $H[A_n, H[A_{n-1}, H[..., H[A_1, MAC_{K_{SD}}$ $(Initiator, target, id, time-interval)]...]]]$.

After verification, the target returns a RREP to the initiator, containing two new field apart from RREQ fields: *target-MAC* is MAC on preceeding fields of RREP with key K_{DS} , *key-list* is initialized to empty list.
The RREP is returned to initiator along the route obtained by reversing the node-list. Each intermediate node appends its TESLA key to the *key-list* . Finally at the initiator, it checks for validity of TESLA keys in *key-list* of each intermediate node, verifies the *target-MAC*.
The following reasoning shows that this protocol is secure

- Any malicious node cannot change node list, because of *hash-chain* is updated at each node appropriately taking into account the new node.
- Nobody can forge RREQ message as it is appended by MAC, calculated by shared secret keys between sender and receiver.
- Intermediate nodes verifies themselves by appending disclosed TESLA keys in RREP, which gurantees that they had added their entry in node-list.

- Initiator can safely believe that RREP comes from target, as the target appends the MAC of RREP containing node-list, calculated with secret key shared with initiator.

6 Prevention against Rushing Attack

This section will describe some set of techniques that can be combinely used to prevent *Rushing Attacks*. The assumption of securely distribute the public keys amoung various nodes, holds here. Each node is assumed to have sufficient computational resources, to carry out public key operations. Following are the mechanisms used to prevent Rushing Attack.

6.1 Secure Neighbour Detection

The implicit neighbour detection techniques used by routing procols, based on periodic broadcast of hello messages by a node, allowing neighbours to detect it. However this simple mechanism can be attacked simply by replaying messages between nodes. Two nodes that are at two hop distance can be made to believe that they are neighbours, by simply replaying their messages by the middle node. Few technique of Rushing attack, as discussed in section 4, involves overhopping the RREQ. So correct neighbour detection is required to prevent such situations.
The secure neighbour detection requires to verify that the neighbour is in normal transmission range. A simple three way mutual authentication protocol that uses tight delay timing can be used. For instance, the first message includes sender identity, a nonce[5] N_1, signed by sender. The second message includes sender-id, receiver-id, nonces N_1 and N_2, signed by receiver. Finally, the third message includes sender-id, receiver-id, nonce N_2. The tight delay timing ensures that the message has only gone through one MAC contention. Given the delay between sending the first message and receiving the second message be D, the neighbour is no farther than $D/2 \times C$, where C is the speed of light. This is accurate if the receiver can quickly process the first message and respond with the second message. In this way an upper bound of delay D can be obtained. This makes the secure neighbour detection job complete.

6.2 Secure Route Delegation

Each node wants to verify that all the secure Neighbour Detection steps were performed between all adjacent pair of nodes for the RREQ previously. *Secure Route Delegation* Mechanism ensures this by adding one more message in the third step of Secure Neighbour detection Protocol. This message is the delegation message contains addresses of two neighbours and addresses of ultimate source and destination of RREQ, all signed with first neighbour.

6.3 Randomized Message Forwarding

One final step in preventing rushing attack is to disallow intermediate nodes to forward first RREQ. Rather, a random selection technique can be used, in which a few number of RREQ are collected and a randomly selected RREQ is forwarded. Timesouts should be choosen appropriately, because small timeouts can prevent other RREQ to arrive, whereas large timeouts may allow very longer routes to be selected, thus increasing the end to end delay.

7 Prevention against Wormhole Attack

The problem of wormhole as described in subsection 4.8 can only be solved if two nodes can detect that they are actually in radio coverage of each other.
Using Secure Neighbour Detection approach requires public key operations that are computationally expensive. Also due to mobility, there may be cases, when at time of three way handshake the two nodes are neighbours, and immediately after that instant, they moved far away.
One approach of restricing the maximum distance the packet is allowed to travel is to use leash. A leash is any information that is added to a packet to restrict the maximun travel distance. Two types of leashes can be used:

7.1 Geographical Leashes

Each node must know its geographical position[6] and stores this in the packet and signs the packet. The receiving node simply checks the validity of packet and calculates the distance between the two nodes, by knowing its geographical position and position contained in the received packet. If calculated distance exceeds some value, then wormhole attack is detected. Some sort of loose time synchronization is required to determine the variation of the actual distance wrt the calculated distance, if maximum moving speeds of nodes are considered.
The advantage of using geographical leashes is that an attacker can be caught if pretends to reside at multiple locations. However, it has one disadvantage that, due to external disturbances, if the radio coverage area is decreased, then the two nodes which are in normal transmission range of each other can be attacked by

[5]Nonce: One time number or Random number

[6]Location information can be obtained using GPS receivers.

wormhole, because they are no longer in transmission range due to external disturbances.

7.2 Temporal Leashes

A better approach of detecting wormholes is to use temporal leashes, which ensures that the packet has an upper bound on its lifetime. In this technique, the time of trasnmission of packet is appended in the packet. The use of Temporal leashes restricts the maximum travel distance of the packet, since the packet can travel atmost at the speed of light. It requires the network to have strong time syncronization with maximum time syncronization error Δ.

Let t_s be the sender time of transmission of a packet and t_r be the time at receiver when it receives the packet. The sender send in the packet, the expiration time $t_e = t_s + L/c + \Delta$. Here c is the speed of light, L is the maximum distance the packet is allowed to transmit. The receiver will only accept the packet if $t_r < t_e$.

This mechanism also require authentication of messages contains expiration time-stamps. For this purpose TESLA or its extention can be used, to prevent any forging of time-stamps.

8 Anonymous Routing

While data encryption can protect the content exchanged between nodes, routing information may reveal valuable informatin about end-users and their relationships. The location and relationship of the communicating entities may easily be determined from traffic and data analysis of packet. A protcol is discussed in this section which provides anonymous routing between source and destination.

One of the assumption of this protcol is that the nodes have sufficient computational resources. This protocol makes use of Public key based authentication and encrption techniques.

8.1 Secure Distributed Anonymous Routing Protocol (SDAR)

During normal routing of data packets, the source and destination information is contained in the packet. which can be exploited by malicious intermediate or overhearing nodes. The SDAR protocol described in this subsection ensures anonymity of sender and receiver. In this protcol, a sender S discovers an anonymous path between itself and receiver, before transmitting any data. The three phases of this protocol is described below:

8.1.1 Path Discovery Phase

In this phase, source S sends a *path discovery message* to all its neighbours which is destined for a receiver R. This message contains following components:

- TYPE , TRUST_REQ, TPK
- $E_{PK_R}(ID_R, K_S)$
- $E_{K_S}(ID_S, PK_S, TPK, TSK, SN_{Session\_ID_S}, Sign(M_S))$

Here TPK and TSK are temporary (public,private) key pair used for this session. K_S is the session secret key used by S and ID_R is the address of receiver, both are send in this packet by encrypting with PK_R: the public key of R. The last part contains ID_S: address of sender S, PK_S: the public key of S, $SN_{Session\_ID_S}$: random number used to identify this session, all these are encrypted with session key K_S. The $Sign$ part protects the integrity of message.
The information about sender and receiver are all encrypted. Thus anonymity is maintained here.Only the receiver can decrypt the second part by its private key, obtain the session key and hence decrypt the last part. The intermediate node i process the packet as follows:

- Check if the message has already arrived , by looking at TPK, which acts as identifier of request. If yes, then discard the message, else process it further.
- Add the following information to the packet, all encrypted with TPK: $E_{TPK}(ID_i, K_i, SN_{Session\_ID_i}, Sign(M_{ID_i})$ Here , ID_i: the address of node, i, K_i: the session key used by node i for this session, $SN_{Session\_ID_i}$: random number used to identify this session by node i, $Sign(M_{ID_i})$: Signature of whole message.
- Add $(SN_{Session\_ID_i}, K_i, PreviousNode)$ to internal table. This will be used to forward data packets for this route.

  The receiver when receives this message, can identify that this is destined to itself. However for anonymity purpose, forwards it to other nodes, and it enters into Path Recovery Phase

8.1.2 Path Recovery Phase

The receiver R, after obtaining the *path discovery message* do following steps in this process:

- Form the message $E_{K_S}(SN_{Session\_ID_1}, K_1, SN_{Session\_ID_2}, K_2, ..., K_N, SN_{Session\_ID_R}), SN_{Session\_ID_S}$.
- Repeatedly encrypting the above message, each time encrypt it with key K_i and add $SN_{Session\_ID_i}$, starting from key K_1 upto key K_N.

- Send the final constructed message to the first node in the reverse path.

In the reverse direction, each intermediate node i receives this message, identifies that it belong to itself by $SN_{Session\_ID_i}$, which is appended to this message. It then finds its key correnponding to this session-id, decrypts the message and forwards it to the next intermediate node in the reverse path. The remaining intermediate node follows similar steps. Each intermediate node therefore removing one layer of encryption. Finally the sender will receive the *path recovery message* which is of the form that is prepared by the receiver in first step. It extracts the keys and session-ids of all intermediate nodes. This completes the route finding process in anonymous manner. No intermediate node and no other node knows of the full route that is evaluated. Even the sender and receiver dont know about this route. Only thing that sender and receiver knows is session-ids and keys of intermediate nodes.

8.1.3 Data Transfer Phase

In this phase, the sender S actually sends message to receiver R. Rather than filling source and destination address, it builds a layered encryption packet as follows.

- Make a packet of the form: $E_{K_S}(Data_S), SN_{Session\_ID_R}$.
- Encrypt and append session-id repeatedly, by using session key and session-id of each intermediate node in the order of reverse path of intermediate node.
- Broadcast the message, to allow neighbour intermediate node to forward it.

Each intermediate identifies the packet which is meant to be forwarded by it by appended session-id, decrypts one encrytion layer and forwards the message to next intermediate node. Finaly the receiver decrypts the inner most layer and got the message.

So, data packet is transfered from source to destination and no other node including intermediate node has any information about their route as well as their identity. This protocol does not require the source node to gather and store information about the network topology. The multicast mechanism and the layered encryption used in the protocol, ensure the anonymity of the sender and receiver nodes.

8.2 Characteristics

This protocol has following characteristics :

- Non-Source based Routing: The source does not require to have a global view of network topology and hence the knowledge of route to destination.
- Flexible and Reliable Route Selection: The route control messages described earlier cannot be modified by malicious intermediate node, without being detected by source or destination.
- Resilience against Path Hijacking: Even if some malicious node becomes intermediate node, it cannot break the anonymity of route discovery.

8.3 Security Analysis

- Passive attack: Malicious nodes cannot find the sender, receiver and other intermediate node just by eavesdropping on *path discovery* messages.
- Active attack: Any modification of the *path discovery* messages will be detected by receiver because of signatures appended, which preserves integrity of message.
- Denial of Service Attack: The protocol is incapable of resisting DOS attack involing flooding the network with meaningless *path discovery* messages. It is because verification of these messages involves complex computations which is resource consuming. Also it consumes network bandwidth. In fact DOS attack is very difficult to resist in any protcol.

9 Intrusion Detection in MANETs

Intrusion Detection systems (IDS) serves as second line of defence, after first line of defense by *prevention* techniques.
The two major analytical techniques in intrusion detection are

- Misuse detection: It uses signature of known attacks, to identify those attacks
- Anomaly detection: It uses established normal profiles only to identify any unreasonable deviation from them.

9.0.1 Architecture of an IDS agent

Figure 1 shows the architecture of an IDS agent that can be deployed on each mobile node. The various components are:

- *Data Collection Module* : It collects various security related data from various audit data sources and preprocess them to the input format of detection engines.
- *Detection Engine* : It determines whether a particular state of system is anomalous, based on predetermined normal profile of network created during training process.

- *Local Aggregation and Correlation Engine (LACE)*: It aggregates and correlate various detection results and transfer them to GACE.
- *Global Aggregation and Correlation Engine(GACE)*: Its function to aggregate detection results from a number of nodes and globally make decision about any malicious event.

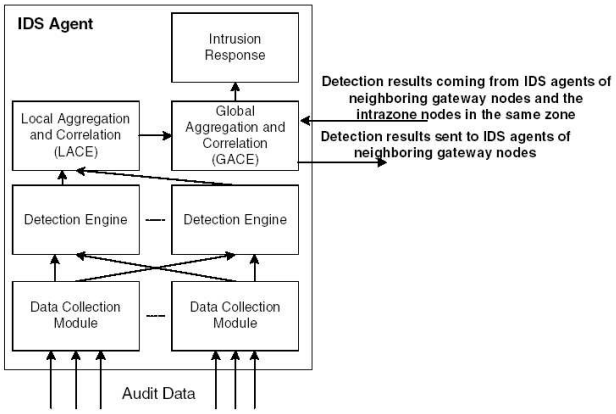

Figure 1: IDS Agent

9.1 Routing anomalies in MANETs

This subsection will describe how Routing anomalies can be detected in MANETs. One important assumption of intrusion detection is that normal and intrusive behaviours are distinguishable.
The following are the challenges in routing anomaly detection

- Due to arbitrary mobility, it is very difficult to establish a mathematical model to characterize routing disruption attack.
- Difficulty in distinguishing Routing control packets generated by attacker, and that by mobility induced error.

In this sub-section, a Markov Chain Based Anomaly Detection scheme is briefly described. The following steps are required:

9.1.1 Feature Selection

Features are the attributes of data that needs to be considered. Features associated with routing caches of mobile nodes are determined in order to characterize their normal changes. Two main features are used.

- PCR: % Change in number of routing entries in certain time periods.
- PCH: % Changes in sum of hops of all routing entries in a certain time periods.

9.1.2 Markov Chain Based Intrusion Detection

The idea of using this model is that the routing changes in mobile nodes can be considered as random process with stationary transition probabilities of Markov Chain. This statement is valid for a particular class of network, whose normal traffic follows a regular pattern. Two step process of Intrusion Detection are following:

1. **Markov Chain Model Construction**

The Markov Chain Model Construction requires some amount of traning data representing normal traffic pattern of the network. During construction process, the training data is preprocessed for discretization, and divided into set of traces. Each trace has a continuous values of statistical feature that we want to consider. A virtual window of size W slides through this trace. At each position of window the transition of W ordered states (feature values) within the window to new state, which is the feature value just on the right of window, is recorded. This process, if repeated for large number of traces. This will build a comprehensive probability model for a particular network traffic. This model can be used to calculate the probability of a given $W + 1$ number of ordered feature values.

2. **Classifier Construction**

The Classifier of Markov Chain Model is constructed after training the model. The classifier determines how anomalous is a given trace of statistical feature values. Under operational condition, the traces from the routing caches are recorded and fed to the detection engine. The detection engine runs the classifier over this trace. It involves sliding a virtual window of length W, and find out the probabilities of every continuous $W + 1$ feature value of the trace. We get a set of probabilities as $(P_0, P_1, P_2, ..., P_k)$. The lesser is the value of these probabilities, the more anomalous are the events that these probabilities are representing. Now, either we can calculate the average probability and compare it with some threshold or we can analyze individual probabilities. The later approach of analyzing individual probabilities is better because calculating average probability can suppress some of the few exceptionally low probabilities.
Some of the approach to analyze these probabilities are:

- A common approach is to indiviually compare the probabilities with some threshold value. If some probability is less than a particular threshold, then raise an alert.
- The ratio of cumulative sum of probability with number of probabilities that are summed is com-

pared with some threashold at each iteration of summation. Again if the ratio becomes less than some threshold at any stage, an alert is generated.

Selecting the threshold T determines a tradeoff. Higher value of T will increase the anomalous detection ratio, but may also increase the false alarm ratio. Lower value of T will decrease the false alarm ratio but it will also decrease detection ratio. A proper value of T can be determined empirically, with desired level of trade-off. There are some limitations of this model:

- Unexpected changes in statistical features are undesirable, as they introduces noise in the probability model.
- Overhead of training data is significant.

9.2 Crossfeature analysis in MANETs

This is another technique of detecting anomaly in MANET network. The Cross feature analysis is a data mining method to capture the inter-feature correlation patterns in normal traffic. The basic idea of cross-feature analysis framework is to explore the correlation between one feature and all other features. Anomaly detection problem can be transformed into a set of classification sub-problems, where each sub-problems choose a different feature and find out its correlation with all other features.
The same basic assumption applies here that normal and abnormal events should be able to separate from each other based on their corresponding feature vectors. The technique of cross feature can be applied in two steps as:

9.2.1 Training procedure

This phase involves training a classification model such that the model will be able to predict value of one feature when given the values of all other features. Some of the examples of features are given in subsection 9.2.3. The model is trained from normal traffic feature values and hence will be able to differentiate normal and abnormal traffic. The model building process is repeated for every feature and upto L[7] sub-models are trained.

9.2.2 Testing procedure

This phase actually test the given set of feature values for its normality. The given set of feature values for a particular event is tested under this model. Each of the L sub-models is applied to the given set of feature values. In each turn the probability of one feature value, when given other feature value, is calculated. So we are left with L probabilities . These set of probabilities can be treated in the same way as expained in previous subsection 9.1.2.

[7] L is the number of features under consideration

9.2.3 Feature Example

Some examples of features are given below:

- *Route related features*: velocity, route add count, route removal count, route find count, route repair count, total route change, average route length.
- *Traffic related features*: packet type, flow direction (sent,received,forwarded,dropped), statictical measures of timing.

9.3 Cooperative Approach

It is very hard to distinguish between intrusions and legitimate operations or conditions in MANET because of the dynamically chaning topology and volatile physical environment. However, by integrating the security related information from a wider area, the aggregation algorithm can reduce the false alarm ratio and improve the detection ratio.
Two methods of aggregating are:

- Zone-based Aggregation: This approach divides the mobile nodes into zones based on geographical division. The gateway nodes are the nodes which have physical connections to different zones. The *gateway* nodes of each zone is responsible for aggregating and correlating the locally generated alerts inside the zone.
- Cluster based Aggregation: In this approach, nodes dynamically form cluster. A cluster is a group of nodes such that all nodes in that cluster are at one hop distance from a particular node called *cluster head*. The *cluster-head* is the one who collect alerts from all other nodes of that cluster. This allows the cluster-head to take a global decision about the events happening in the cluster.

10 Conclusion

The following colclusions are made based on the study of MANET attacks and solutions:

- The mobile nodes are considered to be resource constrained. If public key operations are used, care needs to be taken to limit the frequency of these operations to prevent DOS attacks.
- The two lines of defenses(*Prevention* and *Detection*) against MANET attacks is required. However, a proper balance between these two is necessary to prevent much consumption of resources.
- Because of mobility it is very difficult for the attacker to keep a node victimized always.
- DOS attack is very difficult to resist in any protcol.

- Some solutions discussed in this article favours public key operations and some oppose it. This is because using public key encryptions in MANETs is taken as highly computational problem which is actually so. However, due to decrease in the cost of computational power in day by day technologies, MANETs will no longer believed to be resource constrained. But the problem of public key operations being expensive remain for the long time. This is because increase in computational power will also increase key sizes for appropriate level of security. This increase in key sizes will definitely increase the computational cost.

  One solution to this problem is to use Elliptic curve cryptography, which is proved to be stronger than RSA for same length of key. For now, a balance between public key operations and symmetric key operations should used in deploying security solutions in MANETs.

- Anomaly detection approaches discussed in this article are prone to change in normal traffic profile. There is tremendous research scope in this area of finding or discovering data-mining technologies that can cope up with this problem.

References

[1] Li Xu Larry Korba Azzedine Boukerche, Khalil El-Khatib. A novel solution for achieving anonymity in wireless ad hoc networks. Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, 2004 Oct.

[2] Udo W. Pooch Bo Sun, Kui Wu. Alert aggregation in mobile ad hoc networks. pages 69 – 78. Proceedings of the 2003 ACM workshop on Wireless security, 2003 Sep.

[3] A.; Johnson D.B. Hu, Y.-C.; Perrig. Packet leashes: A defense against wormhole attacks in wireless networks. pages 1976 – 1986. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE , Volume: 3, 3 April 2003.

[4] Panos C. Lekkas Randall K. Nichols. *Wireless Security - Models, Threats and Solutions.* Mc Graw Hill, 2002.

[5] K.; Pooch U.W. Sun, B.; Wu. Routing anomaly detection in mobile ad hoc networks. pages 25 – 31. Computer Communications and Networks, 2003. ICCCN 2003. Proceedings, 2003.

[6] Wenke Lee Yi-an Huang. A cooperative intrusion detection system for ad hoc networks. pages 69 – 78. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003 Oct.

[7] P.S. Yi-an Huang; Wei Fan; Wenke Lee; Yu. Cross-feature analysis for detecting ad-hoc routing anomalies. pages 478 – 487. Distributed Computing Systems, 2003. Proceedings. 23rd International Conference on , 19-22 May 2003, 2003.

[8] David B. Johnson Yih-Chun Hu, Adrian Perrig. Ariadne: A secure on-demand routing protocol for ad hoc networks. Proceedings of the 8th annual international conference on Mobile computing and networking, 2002 Sep.

[9] David B. Johnson Yih-Chun Hu, Adrian Perrig. Rushing attacks and defense in wireless ad hoc network routing protocols. Proceedings of the 2003 ACM workshop on Wireless security, 2003 Sep.