Security in Mobile Ad Hoc Networks (MANETs)

Farid Zafar Sheikh[1], M. Ali Akbar[2], M. Zulkifl Khalid[3], Wasif Mehmood[4]

Electrical Department, College of Electrical & Mechanical Engineering, National University of Sciences and Technology, Rawalpindi, Pakistan

{[1]farid.zafar, [2]aliakbar386}@hotmail.com, {[3]zulkifl, [4]mwasifmehmood}@gmail.com

ABSTRACT

In this paper, we describe the security issues in Mobile Ad Hoc networks. A malicious attack by nodes in networks significantly affects the Quality of Service delivered by the network and disrupts the route discovery process. This problem is especially serious in mobile ad hoc networks (MANETs) as traditional methods created to prevent such attacks on wired networks are only partially successful when applied to mobile networks. We present some techniques to secure Mobile Ad Hoc Networks from these attacks. We take AODV as an example and develop a security mechanism to protect its routing information.

Categories and Subject Descriptors

C.2.2 [**Computer-Communication Networks**]: Network Protocols—Routing protocols. [1]

General Terms

Algorithms, Reliability, Security

Keywords

Mobile Ad hoc Networks, Digital Signatures, Hash Chains, SAODV

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructureless" network. Such as military battle field, emergency rescue, vehicular communication, mining operation, etc. These networks are subject to frequent link breaks which also lead to a constantly changing network topology. In MANETs every node can perform the role of host as well as router, thus nodes which are out of transmission range can be accessed by routing through the intermediate nodes. The network topology of MANETs is always changing as their mobile nodes are free to move around and can freely leave or join the networks. This makes Mobile Ad Hoc Networks more vulnerable to external attacks because any attacker node can easily enter the network. In addition, the constantly changing topology makes it hard to determine which node really left the network, just changed the location, or has been intercepted or blocked. Some of the characteristics of mobile Adhoc networks are described as follows: [2]

- MANET's constitute dynamic topology, which means that the nodes making up the network can move arbitrarily, making it very hard to predict the topology of the network at any instant of future time. Also, the optimum paths between nodes or groups of nodes (multicasting) may change continuously.
- Most of the nodes constituting a MANET may have limited power supplies and power constraints, limiting their effectiveness in routing and forwarding applications.
- Due to shared nature of the MANET networks, they are much more prone to security threats than regular fixed topology networks. Risks may include, spoofing, worm holes, denial of service attacks and many more.[3,4]
- Also, the wireless medium of transmission has limited bandwidth capacity as well as higher rates of errors.

The paper is organized as into various sections. The section 2 deals with related work done in the field of Adhoc networks. Section 3 explains the various functional Adhoc protocols that have been implemented including AODV and DSR, and the various classifications of Adhoc networks. Section 4 defines the various security considerations for a wireless Adhoc network and the various attack schemes possible. Section 5 explains the security extensions that need to be incorporated into an Adhoc network, with the implementation model of SAODV secure routing protocol.

2. RELATED WORK

Mobile Adhoc Network development is in its initial stages with work going on to enhance, optimize and secure proposed designs and protocols. Enhancements include efficient utilization of bandwidth, higher throughputs, lesser per packet overheads, power consumption optimization, security against potential threats, e.g., eaves dropping, impersonations et , and others.

Quite a number of protocol designs have been proposed and implemented for MANET's for example; Dynamic Source Routing (DSR), Ad Hoc On-Demand Distance Vector Routing (AODV), Destination-Sequenced Distance-Vector (DSDV) and Temporally Ordered Routing Algorithm (TORA) have been implemented.

W4A2007, May 07–08, 2007, Banff, Canada. Co-Located with the 16th International World Wide Web Conference.

All of these approaches have a number of advantages and disadvantages, e.g., AODV establishes routes as and when required rather than proactively searching for routes to remote hosts, therefore utilizing bandwidth for path discovery when required. Apart from throughput, power consumption issues , overheads ,optimum path discovery, and other similar routing issues, security is a very important issue and integral part of reliable efficient packet routing. So, in order to address the issue of security, a number of advanced protocols have also been proposed, which solve the security problem to some extent.

Security issues for routing algorithms have been addressed in the form of extensions to existing protocol designs. These extensions work on the concept of detecting mischievous and malicious activity. But the problem is that it is likely to confuse transmission errors with malicious activity and there are no real means to guarantee the integrity and authentication of the routing messages.

For example , ARAN routing protocol uses authentication and requires the use of a trusted certificates .Every forwarding node must sign the control packet ,which takes computing power consuming and the size of the routing message increases with each hop.

Secondly we have the SRP extension that can be used with many existing routing protocols. SRP requires that, for every route discovery, source and destination must have a security association between them.

Ariadne is based on DSR .It requires clock synchronization. There are some other extensions as well which require time synchronization between the nodes of network.

In SEAD hash chains are used in combination with DSDV. At every given time each node has its own has chain. The hash chain is divided into segments; elements in a segment are used to secure hop counts. SEAD can be used with any suitable authentication and key distribution mechanism.

Keeping the various requirements of a secure routing protocol in mind, we have worked on the implementations of a security features inside existing routing protocol, namely AODV. We have implemented a secure version of the AODV routing protocol , SAODV. In SAODV , the main focus is on authentication and security of mutable fields, e.g., Hop Count which has to be modified by every intermediate node. AODV requires a sound key distributing system and user authentication mechanism as well as hash chains management.

3. PRACTICAL IMPLEMENTATIONS OF MANET DESIGNS:

Mobile Adhoc Networks can be practically classified into two major categories , [3]

- Table-Driven (Proactive)
- On-Demand (Reactive)

3.1 Table-Driven Routing Protocol:

Table Driven, or otherwise known as Proactive Routing protocols perform route discoveries automatically and periodically, so as to buildup a table of the network topology. [4] Therefore, routes are discovered for every mobile node of the network, with out any requests for communications by the hosts.

Some examples of table driven or proactive routing protocols include DSDV, WRP, CGSR and STAR.

3.2 On-Demand Routing Protocols:

Apart from table driven routing protocols, there are also some reactive routing protocols, in which route discovery is performed when communication between hosts of a mobile network is required. Reactive protocols perform route discovery and path establishment by using specialized sets of packets known as **control packets.**

Examples of Reactive routing protocols include AODV, DSR, and TORA.

3.3 Dynamic Source Routing Protocol:

Dynamic source routing protocol utilizes the concept of source routing i.e. the packet is provided with entire journey path before it is put on the link, in other words, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a routing cache called the **routing table**. The data packets carry the source route in the packet header. The routing procedure consists of the following control packets.

- When a node in the ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a route discovery process to dynamically determine such a route. Route discovery works by flooding the network **with route request (RREQ)** packets.
- Each node receiving an RREQ rebroadcasts it, unless it is the destination or it has a route to the destination in its routing table. Such a node replies to the RREQ with a **route reply (RREP)** packet that is routed back to the original source. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed across the network.
- The RREP routes itself back to the source by traversing this path backward. The route carried back by the RREP packet is cached at the source for future use.
- If any link on a source route is broken, the source node is notified using a **route error (RERR)** packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source if this route is still needed.

DSR makes very aggressive use of source routing and route caching. No special mechanism to detect routing loops is needed. Also, any forwarding node caches the source route in a packet it forwards for possible future use.

3.4 Adhoc On-Demand Distance Vector Routing:

AODV is a practical implementation of the Reactive route discovery mechanism [5]. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers.

3.4.1 Route Discovery/Estb. In AODV:

[6]AODV utilizes control packets such as Route Request (RREQ), Route Reply (RREP), and Route Error (RERROR) to manage routes between communicating nodes. The formats for AODV messages is given in **Appendix A**

3.4.1.1 Route Request (RREQ)

When a node needs to determine a route to a destination node, it floods the network with a **Route Request (RREQ)** message. The originating node broadcasts a RREQ message to its neighboring nodes, which broadcast the message to their neighbors, and so on. To prevent cycles, each node remembers recently forwarded route requests in a route request buffer. As these requests spread through the network, intermediate nodes store reverse routes back to the originating node. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop count.

3.4.1.2 Route Reply (RREP)

When a node receiving the request either knows of a fresh route to the destination or is itself the destination, the node generates a **Route Reply (RREP)** message, and sends this message along the reverse path back towards the originating node. As the RREP message passes through intermediate nodes, these nodes update their routing tables, so that in the future, messages can be routed though these nodes to the destination.

3.4.1.3 Route Error (RERR)

Each node periodically sends HELLO messages to its neighbors. Each node expects to periodically receive messages from each of its outgoing nodes. If a node has received no messages from some outgoing node for an extended period of time, then that node is presumed to be no longer reachable. Whenever a node determines one of its next-hops to be unreachable, it removes all affected route entries, and generates a **Route Error (RERR)** message. This RERR message contains a list of all destinations that have become unreachable as a result of the broken link. The node sends the RERR to each member of its precursor list. They update their routing tables, and in turn forward the RERR to their precursors, and so on. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs.

3.4.1.4 Route Request Buffers

To prevent nodes from resending the same RREQs repeatedly, each node maintains a **route request buffer**, which contains a list of recently broadcasted route requests. Before forwarding a RREQ message, a node always checks the buffer to make sure it has not already forwarded the request .RREQ messages are also stored in the buffer by a node that originates a RREP message, so that a node does not send multiple RREPs for duplicate RREQs that may have arrived from different paths.

3.4.1.5 Sequence Numbering

Each node maintains an increasing sequence number , and every route entry includes a destination sequence number. The protocol uses sequence numbers to ensure that nodes only update routes with “newer” ones. This also ensures loop- freedom for all routes to a destination. All RREQ messages include the originator’s sequence number, and its destination sequence number. Nodes receiving the RREQ update routes to the originator with the originator sequence number. If the node receives an identical RREQ message through another path, the originator sequence numbers would be the same, so the node would pick the route with the smaller hop count. If a node receiving the RREQ message has a route to the desired destination, then we use sequence numbers to determine whether this route is fresh to be used as a reply to the route request, by check if this node’s destination sequence number is at least as great as the maximum destination sequence number of all nodes through which the RREQ message has passed. If this is the case, an RREP is sent back to the originator. As with RREQ messages, RREP messages also include destination sequence numbers.

3.4.1.6 Multicast Routes

Multicast routes are set up in a similar manner. A node wishing to join a multicast group broadcasts a RREQ with the destination IP address set to that of the multicast group and with the **JOIN** flag set to indicate that it would like to join the group. Any node receiving this RREQ that is a member of the multicast group that has a fresh enough sequence number for the multicast group may send a RREP. As the RREPs propagate back to the source, the nodes forwarding the message set up pointers in their multicast route tables. As the source node receives the RREPs, it keeps track of the route with the freshest sequence number, and beyond that the smallest hop count to the next multicast group member. After the specified discovery period, the source node will unicast **a Multicast Activation (MACT)** message to its selected next hop. This message serves the purpose of activating the route. A node that does not receive this message that had set up a multicast route pointer will timeout and delete the pointer.

3.4.1.7 Precursor And Outgoing Lists

Each node of the network keeps track of a **precursor list**, and **an outgoing list**. A precursor list is a set of nodes that route through the given node. The outgoing list is the set of next-hops that this node routes through. In networks where all routes are bi-directional, these lists are essentially the same.

4. SECURITY REQUIREMENTS IN MANET's

One of the most distinct feature of MANET's from other static networks is the fact that each node of the networks contributes in making up routes from various sources to destinations or groups of nodes acting as destination. However, this distinct feature poses a number of serious threats to the security and privacy of the overall network as well as the individual nodes making up the network. [7]

The openness of Adhoc networks offers greater flexibility in terms of functionality, but it also provides an open path for any malicious node or intruder to gain access to the network and perform activities such as eaves dropping, spoofing, Denial of service attacks, flooding, link failure and many more.

To ensure safe operation of an Adhoc network, the following minimum constraints should be met

- Authentication of a node is very important so that the node can be trusted as a valid and trusted node , and malicious, eavesdropping nodes are denied access into the network.
- Data integrity is an important issue, so as to ensure the data communicated between nodes has not been tempered or altered by any malicious node.
- Privacy is also necessary, to ensure that no intermediate node can access the data that is meant for the destination of that message.

4.1 Classification Of Attacks In MANETs :

Attacks on Adhoc networks can be broadly classified on the basis of their origin, either external , or internal. [8]

- External attacks are the attacks launched by parties that are not part of the network. External attackers are not necessarily disconnected from the network, though. The targeted network might be a self-contained
- Internal attacks are sourced from inside a particular network. A network with internal attacker nodes is more vulnerable because a malicious node inside a network is already past the basic defence lines of a network, hence the malicious activity is very difficult to detect and curtail.

The attacks on networks can also be classified as follows,

- Passive attacks are those attacks in which a malicious node does not actively try to disrupt the network; instead, it sits silently, eavesdropping on communication and data traffic, as well as collection information about the various communicating nodes of a network.
- Active attacks are those in which a node proactively searches for flaws in the network and tries to disrupt the topology of the network by overloading it or breaking existing paths between network nodes.

4.2 Attack Types In MANET's:

4.2.1 Spoofing

[9]In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network. This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node. A malicious node with this goal will most likely try to impersonate a node within the path of the data flow it requires. It could be done by modifying routing data or implying itself as a trustworthy communication partner to neighboring nodes in parallel. Usually, exploiting MAC layer protocol malicious nodes could place their node between two other nodes communicating with each other (man-in-the-middle attack).

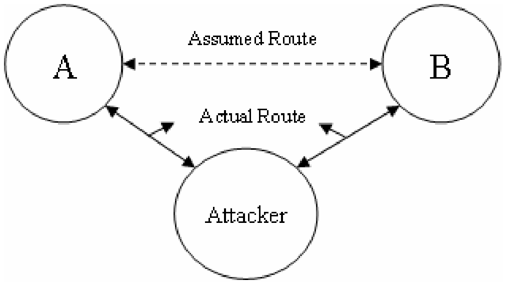


Figure 1. Spoofing (Man in the middle)

4.2.2 Denial Of Service Attack

In a denial of service attack, a malicious node may become the bottle-neck for paths that are passing through it, by denying service to those paths. In this type of attack, a particular node, that has a single or multiple paths passing through it may stop forwarding packets, while still maintaining its presence in the networks (replying to **hello** packets of precursors), hence acting as a sink for data in the network.

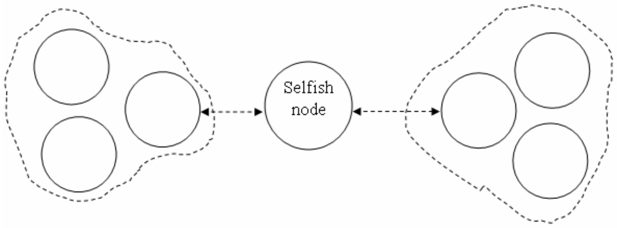


Figure 2. Denial of Service Attack

4.2.3 Sinkholes

In a sinkhole attack, a compromised node tries to attract the data to itself from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be implemented on Adhoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate. The problem of sinkhole attack can be much amplified if the malicious node exists within or around the centre of the network so that it hears every communication happening inside the network. However, in the case of Multipath protocols which send data redundantly, not relying on one path only, the problem of sinkholes can be reduced. Probabilistic protocols which measure the trustworthiness of a network can help detecting sinkholes within the network.

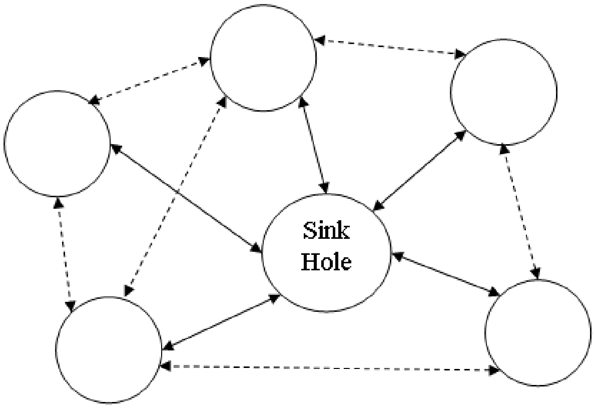


Figure 3. Sink Hole

4.2.4 Wormhole

In a wormhole attack, a malicious node uses a path outside the network to route messages to another node at some other location in the. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. A wormhole itself does not have to be harmful; for it usually lowers the time it takes for a package to reach its destination. But even this behavior could already damage the operation, since wormholes fake a route that is shorter than the according one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes.

Wormholes are dangerous because they can do damage without even knowing the network. The wormhole attack can be detected by marking each packet with timestamps and location stamps in order to detect wormhole intrusions in a system. Each packet is tagged with very precise time information of the sender node, which is then compared by the destination node to its own time and location stamps. If the comparison reveals an unrealistic distance the data took within an unrealistic amount of time, it can be assumed that there is a wormhole within the network.

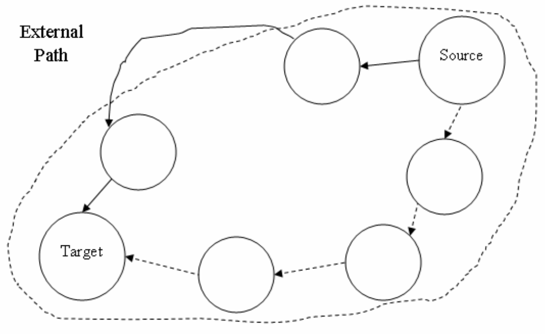


Figure 4. Wormholes

4.2.5 Sybil Attack

Malicious nodes in a network may not only impersonate one node, they could take up the identity of a group of nodes, this attack is called the Sybil attack. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point A to point B. A consequence of this is that attackers have a harder time to destroy the integrity of information. However, if a single malicious node is able to represent several other nodes, the effectiveness of these measures is significantly degraded. The attacker may get access to all the data or may alter all packets in the same transmission so that the destination node/s cannot detect the change in packets anymore. In trust-based routing environments, representing multiple identities can be used to deliver fake recommendations about the trustworthiness of a certain party, hereby attracting more traffic to it; in ideal starting point for further attacks.

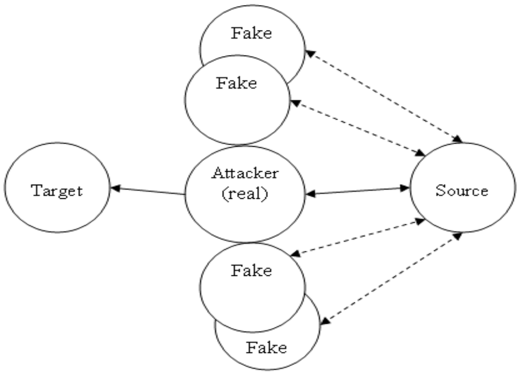


Figure 5. The Sybil Attack

4.2.6 Flooding

Malicious nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way. This has especially serious effects on ad hoc networks, since the nodes of these usually possess only limited resources in terms of battery and computational power. Traffic may also be a monetary factor, depending on the services provided, so any flooding which blows up the traffic statistics of the network or a certain node can lead to considerable damage costs.

4.2.7 RERR Generation

[10]Malicious nodes can prevent communications between any two nodes by sending RERR messages to some node along the path. The RERR messages when flooded into the network, may cause the breakdown of multiple paths between various nodes of the network, hence causing a no. of link failures.

4.2.8 Attack On Mutable Fields

In mobile Adhoc networks, there are a no. of fields in control and data packets that are altered along their path form one node to another. For example , the hop count field is incremented each time a node receives a RREQ control packet .So, a malicious node can attack by modifying this mutable information e.g., by diverting all traffic through itself or by not forwarding requests, or by simply setting these fields to an infinitely high value.

5. SECURING MANETS

There are some basic requirements for securing wireless networks. The primary security service is *authorization*. It is required in two cases. Firstly when a node receives routing update another node it has to decide whether to modify its local routing information accordingly. This is import authorization and it is a critical service. Secondly when a router receives a request for routing information it may carry out export authorization. In traditional routing systems, authorization is a matter of policy.
Authorization in addition requires other security services such as authentication and integrity. Authentication means a node should be able to verify that it is getting messages from the source which is what it claims to be and integrity means the routing information it is receiving is not altered by any of the intermediate nodes. Data authentication also requires authentication of source and integrity of message.

5.1 Security flaws of AODV

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not following the protocol design and implementation. The following attacks are very straight forward to implement on AODV:

- Impersonating a node by forging a RREQ with its address as the originator address.
- When forwarding a RREQ generated, reduce the hop count field to increase the chances of being in the route path so it can analyze the communication between them.
- Also, when forwarding a RREQ, increment the destination sequence number to make the other nodes believe that this is a ‘fresher’ route.
- Impersonating a destination node by forging a RREP with its address as a destination address.
- Impersonating a node by forging a RREP that claims that the node is the destination and, to increase the impact of the attack, claims to be a network leader of the subnet and send it to its neighbors. In this way it will it will become a black hole for all traffic belonging to the subnet.
- Selectively, not forward certain RREQs and RREPs, certain RREPs and not forward certain data messages. This kind of attack is especially hard to detect, as it has the same features as a transmission error.
- Forge a RERR message. The RERR message has a very high destination sequence number for one of the unreachable destinations.
- The originator of a RREQ can put a much bigger destination sequence number than the real one. In addition, sequence numbers wraparound when they reach the maximum value allowed by the field size. This allows a very easy attack in where an attacker is able to set the sequence number of a node to any desired value by just sending two RREQ messages to the node.

5.2 Securing AODV Protocol:

There are two basic mechanisms used to secure the AODV routing protocol:

- **Digital Signatures** (to authenticate the non-mutable fields of the messages).
- **Hash Chains** to secure the hop count information (mutable information in the messages).

The digital signatures of non-mutable fields are verified end-to-end, whereas, the hash chains are to be used at each and every next hop along a path to the destination. The various packet header extensions required to add security to AODV are given in **Appendix B**

5.3 Digital Signatures:

Digital signatures are used to protect the integrity of the non-mutable data in RREQ and RREP messages. Meaning that they sign everything but the Hop Count (mutable field) of the AODV message and the hash from the SAODV extension. Thus the verification of destination through digital signatures would validate it as the legitimate destination.

The problem in applying digital signatures is that AODV allows intermediate nodes to reply RREQ messages if they have a fresh enough route to the destination, meaning that they have a sequence number for the destination greater than that enclosed in the RREQ packet. While this makes the protocol more efficient it also makes it more complicated to secure. The problem is that a RREP message generated by an intermediate node should be able to sign it on behalf of the final destination. And, in addition, it is possible that the route stored in the intermediate node would be created as a reverse route after receiving a RREQ message. Hence, the intermediate node replying on behalf of the destination does not have the signature for the RREP.

To solve this problem, there can be two independent approaches:

- The first is that, if an intermediate node cannot reply to a RREQ message because it cannot properly sign its RREP message, it just behaves as if it didn't have the route and forwards the RREQ message. Hence an intermediate node cannot reply on behalf of the destination.
- The second is that, every time a node generates a RREQ message, it includes the RREP flags, the prefix size and the signature that can be used by any intermediate node that creates a reverse route to the originator of the RREQ, to reply a RREQ that asks for the node that originated the first RREQ. Also, when an intermediate node generates a RREP message, the lifetime of the route has changed from the original one. Therefore, the intermediate node should include both lifetimes, and sign the new lifetime. In this way, the original information of the route is signed by the final destination and the lifetime is signed by the intermediate node.

5.4 SAODV Extension Messages:

5.4.1 Double Signature Extensions:

[11]To differentiate between different SAODV extensions messages, the ones that have two signatures are called RREQ and RREP Double Signature Extension. When a node receives a RREQ, it first verifies the signature before creating or updating a reverse route to that host. Only if the signature is verified, will it store the route. If the RREQ was received with a Double Signature Extension, then the node will also store the signature for the RREP and the lifetime in the routing table entry. An intermediate node will reply to a RREQ with a RREP only if it fulfills the AODV's requirements to do so and the node has the corresponding signature and old lifetime to put into the Signature and Old Lifetime fields of the RREP Double Signature Extension. Otherwise, it will rebroadcast the RREQ.

5.4.2 Single Signature Extensions:

When a RREQ is received by the destination itself it will send an RREP with Single Signature Extension. When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. Only if the signature is verified, will it store the route with the signature of the RREP and the lifetime.

5.5 Hash Chains:

SAODV uses hash chains to authenticate the mutable field in control packets, namely hop count of RREQ and RREP messages, in such a way that allows every node that receives the message to verify that the hop count has not been decremented by an attacker. [12]

5.6 Hash Chain Calculations:

A hash chain is formed by applying a one-way hash function repeatedly to a seed.

5.6.1 Hash Chain Generation:

Every time a node originates a RREQ or a RREP message, it performs the following operations:

• Generates a random number also known as **seed value,** through random number generation functions (rnd) .

• Sets the Max Hop Count field to the maximum **TimeToLive** value for an AODV request packet.

Max Hop Count = TimeToLive

• Sets the Hash field to the seed value.

Hash field= seed value generated.

• Sets the Hash Function field to the identifier of the hash function.

• Calculates Top Hash by hashing seed Max Hop Count times.

Top Hash = **h [**Max Hop Count (seed)**]**

h represents a hash function.

5.6.2 Hop Count Verification:

Every time a node receives a RREQ or a RREP message, it performs the following operations in order to verify the hop count:

• Applies the hash function h Maximum Hop Count minus Hop Count times to the value in the Hash field, and verifies that the resultant value is equal to the value contained in the Top Hash field.

IF [Top Hash**]** = **h [**Max Hop Count− Hop Count (Hash)**]**

• Before rebroadcast a RREQ or forwarding a RREP, a node applies the hash function to the Hash value in the Signature Extension to account for the new hop.

Hash = **h** [Hash]

The Hash Function field indicates which hash function has to be used to compute the hash. Hash Function, Max Hop Count, Top Hash, and Hash fields are transmitted with the AODV message, in the Signature Extension.

5.7 RERR Verification In SAODV:

For RERR messages, one approach to securing them would be to secure them in the same manner other RERR messages are secured ,i.e., utilizing digital signatures to secure the non-mutable information and applying hash chains to secure the mutable information.

RERR messages have a big amount of mutable information. In addition, it is not relevant which node started the RERR and which nodes are just forwarding it. The only relevant information is that a neighbor node is informing another node that it is not going to be able to route messages to certain destinations anymore. So the mechanism adopted should be as follows,

- Every node generating or forwarding a RERR message will use digital signatures to sign the whole message and that any neighbor that receives it will verify the signature. In this way it can verify that the sender of the RERR message is really the one that it claims to be.

- A node should never update any destination sequence number of its routing table based on a RERR message The nodes will not trust destination sequence numbers in a RERR message, they will use them to decide whether they should invalidate a route or not.

5.8 Key Management And Distribution:

Generally, the approach for solving the key-management problem is to assume that each node carries a list of legitimate public keys. This approach is by far the most straightforward .However, it assumes that all nodes trust a common set of authorities and that each node can download a list of legitimate nodes before deployment. [13]

One mechanism of key management in Adhoc networks can be the mechanism of incremental deployment in which keys are assigned to nodes as the boot up from a central authority. But, the issue with this approach concerns incremental deployment. If network nodes are not deployed nearly simultaneously, then one node might be deployed before a future node can provide its keys to the authority. In this case, the authority would need to generate keys for future nodes. When a new node wants to join the network, it receives both the list of legitimate nodes as well as its own private key. In this case, the channel over which it receives the private key must be secure against eavesdropping.

Ordinarily, the channel over which it receives the list of legitimate nodes would need to be secure against attacks. But in this approach, we have kept key management as a separate issue and focused on the security issues of AODV.

6. ACKNOWLEDGMENTS

We will like to thank Dr. Mudassar Farooq for his support. Also we will like to thank Wing Cmdr. Nauman for his guidance and expertise in the field of Mobile Adhoc networking.

7. REFERENCES

[1] http://www.acm.org/class/1998/

[2] **Securing Ad Hoc Routing Protocols,** M. Guerrero Zapata and N. Asokan**,**. Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002.

[3] **An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks**, Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer, Richard A. Kemmerer, Department of Computer Science, University of California, Santa Barbara

[4] **Secure Routing for Vehicular Networks**, SEVECOM Kickoff Workshop, 2nd February 2006, Frank Kargl

[5] **Ad hoc On-Demand Distance Vector (AODV) Routing** draft-ietf-manet-aodv-13.txt, Nokia Research Center Elizabeth M. Belding-Royer University of California, Santa Barbar ,Samir R. Das ,University of Cincinnati

[6] **Quick Guide to AODV Routing**, Luke Klein-Berndt, Wireless Communications Technologies Group, National Institute of Standards and Technology

[7] **A Survey of Secure Wireless Ad Hoc Routing** ,YIH-CHUN HU University of California Berkeley ,ADRIAN PERRIG Carnegie Mellon University

[8] **Adaptive Secure Routing in Ad Hoc Mobile Network** ,Abu Raihan Mostofa Kamal ,Department of Computer and Systems Science (DSV), Royal Institute of Technology (KTH),Stockholm, Sweden

[9] **Ad hoc network specific attacks**,Adam Burg,Technische Universität München, 2003

[10] **Study of Secure Reactive Routing Protocols in ,Mobile Ad Hoc Networks**, Lim Sher Ee Dennis, Ee Xianhe

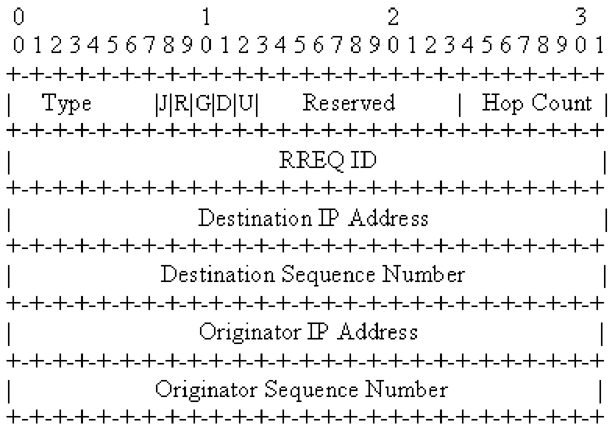
[11] **Secure Ad hoc On-Demand Distance Vector (SAODV) Routing**, draft-guerrero-manet-saodv-06.txt, Manel Guerrero Zapata, Technical University of Catalonia (UPC)

[12] **Introduction to Modern Cryptography**, Mihir Bellare Department of Computer Science and Engineering ,University of California at San Diego , La Jolla, CA 92093, USA. mihir@cs.ucsd.edu

[13] **A Survey of Secure Wireless Ad Hoc Routing** ,YIH-CHUN HU University of California Berkeley ,ADRIAN PERRIG Carnegie Mellon University

APPENDIX

A. AODV Message Formats



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|D|U|   Reserved          |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

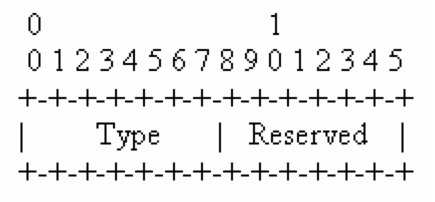
Figure 6. RREQ Message Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |R|A|    Reserved     |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination IP Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Life Time                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7. RREP Message Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |N|          Reserved           |   DestCount   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Unreachable Destination IP Address (1)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Unreachable Destination Sequence Number (1)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Additional Unreachable Dest. IP Addresses (if needed)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Additional Unreachable Dest. Sequence No.'s (if needed)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 8. RERR Message Format



```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9. RERR-ACK Message Format

B. SAODV Message-Extension Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  Hash Func.| Max Hop Count|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                        Top Hash                         ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                        Signature                        ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                          Hash                           ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 10. RREQ ,RREP (Single) Signature Extension

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |Hash Function|Max Hop Count |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|R|A|                    Reserved                  | Prefix Sz |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                        Top Hash                         ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                        Signature                        ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                   Signature for RREP                    ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                          Hash                           ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 11. RREQ Double Signature Extension

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |Hash Function|Max Hop Count |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                        Top Hash                         ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                        Signature                        ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Old Lifetime                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...               Signature of the new Lifetime             ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                          Hash                           ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 12. RREP Double Signature Extension

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|...                        Signature                        ...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 13. RERR ,RREP-ACK Signature Extension