A Comparative study on secure routing algorithms SAODV and A-SAODV in Mobile AdHoc Networks (MANET) – The Enhancements of AODV

J RAJESHWAR
Research Scholar, Dept. of Computer Science & Engineering, JNTUH College of Engineering, JNTUH, Kukatpally, Hyderabad A.P, INDIA.
E-Mail: prof.rajeshwar@gmail.com

Dr G NARSIMHA
Assistant Professor, Department of Information Technology, JNTUH College of Engineering, Kondagattu, Jagityal, Karim Nagar, A.P, INDIA,
E-Mail: narsimha06@gmail.com

ABSTRACT
A freely moving nodes forming as group to communicate among themselves are called as Mobile AdHoc Networks (MANET). Many applications are choosing this MANET for effective commutation due to its flexible nature in forming a network. But due to its openness characteristics it is posing many security challenges. As it has highly dynamic network topology security for routing is playing a major role. We have very good routing protocols for route discovery as well as for transporting data packers but most of them lack the feature of security like AODV. In this paper we are studying the basic protocol AODV and identify how it can be made secure. We are studying a protocol S-AODV which is a security extension of AODV which is called Secure AODV (S-AODV) and we are studying enhanced version of S-AODV routing protocol a Adaptive Secure AODV (A-SAODV). Finally we have described about the parameter to be taken for performance evaluation of different secure routing protocols.

Keywords: MANET, AODV, Secure Routing Protocols SAODV, A-SAODV, Performance evaluation parameters.

1. INTRODUCTION:
A self configured moving nodes forming as a group to communicate each other is called as Mobile Ad Hoc Networks (MANET). Now a day's MANET's became very much popular and they have been used in most of the systems due to its flexibility in forming a network with less infrastructure requirement, its speed of configuration and they can be easily deployable.

MANETs became very much popular due to their wide variety applications, they are Law of enforcement operations automated military applications like Battlefield communications, Rescue & disaster recovery operations, Interactive lectures and Data sharing in classrooms, Meeting events and conferences, intelligent building and logistics etc.

MANETs are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load).

Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. Besides the general security objectives like authentication, confidentiality, integrity, availability and non-repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion.

During the last few years, we have all witnessed a continuously increasing growth in the deployment of wireless and mobile communication networks. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not exist. Therefore, a network layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols [1]. Unfortunately all of the widely used ad hoc routing protocols have no security considerations and trust all the participants to correctly forward routing and data traffic. This assumption can prove to be disastrous for an ad hoc network that relies on intermediate nodes for packet forwarding.

Researchers found many protocols to secure the AODV protocol, they have added few security features to the existing AODV protocol and it is one of the most efficient routing protocols into which security measures can be included. It is observed that complete belief of the network on nodes can lead to many routing attacks. To avoid this, security measures are added to AODV to make it Secure. In this paper we are studying the extension of AODV protocols like S-AODV,
A-SAODV, this study is made to compare the performance between these routing protocols, original AODV (Ad hoc On Demand Distance Vector), Secure AODV, Adaptive (A-SAODV).

The paper is organized in the following way section 1 introduces about MANET, section 2 describes about AODV, section 3 tells about secure routing protocols, section 4 briefs about the parameters for performance evaluation for secure routing protocols, section 5 with conclusion.

2. RELATED WORK
2.1. Ad hoc On demand Distance Vector Routing (AODV) [2] protocol:
2.1.1 Mechanism of AODV protocol: AODV is perhaps the most well-known routing protocol for a MANET. It is a *reactive* protocol it is proved to be an efficient routing protocol for implementation in Ad hoc networks.

It is a Source-Initiated On-Demand or Reactive Routing Protocol. When a source node desires to send a packet to the destination node for which it does not have a valid route, it initiates a route discovery process.

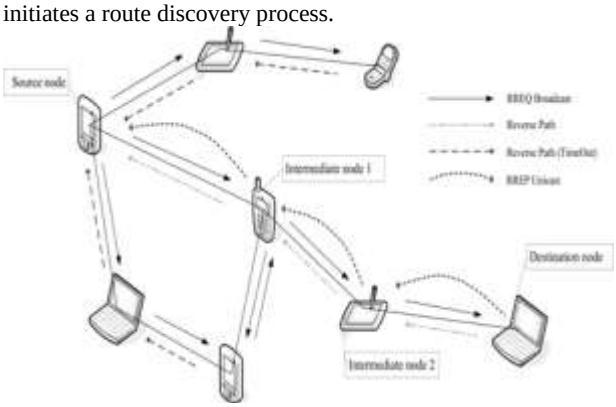

Figure 1: Route Discovery Procedure of AODV Protocol

There are three kinds of routing messages which are generated by this routing protocol during the establishment of route from source to destination they are:

-RREQ (Route Request).
-RREP (Route Reply).
-RERR (Route Error).

The source node broadcasts an RREQ (Route Request) message to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a route to the destination in its routing table is reached. During the process of forwarding the RREQ, an intermediate node record in its routing table (i.e., precursor list) the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. Additional copies of the same RREQ received later are discarded.

Once the RREQ reaches the destination or an intermediate node with a route, the respective node responds by RREP (Route Reply) message back to the neighbor from which it first received the RREQ, which relays the RREP backward via the precursor nodes to the source node. Routes are maintained as follows: HELLO beacons are sent periodically via broadcast to the neighboring nodes. When a source node moves, it has to re-initiate the route discovery protocol to find a new route to the destination.

On the other hand, when an intermediate node along the route moves, its upstream neighbor will notice route breakage due to the movement and propagate an RERR (Route Error) message to each of its active upstream neighbors. These nodes in turn propagate the RERR packet to their upstream neighbors, and so on until the source node is reached. The source node may then choose to re-initiate the route discovery for that destination if a route is still desired. Every routing table entry at every node must include the latest information available about the sequence number for the IP address of the destination node for which the route table entry is maintained. This sequence number is called the "destination sequence number". It is updated whenever a node receives new information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination.

AODV depends on each node in the network to own and maintain its destination sequence number to guarantee the loop-freedom of all the routes towards that node. A destination node increments its own sequence number under two circumstances:

(a) Immediately before a node originates a route discovery; it must increment its own sequence number. This prevents problems with deleted reverse routes to the originator of a RREQ.

(b) Immediately before a destination node originates a RREP in response to a RREQ, it must update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet.

2.2. Attacks on AODV protocol during the establishment of route.

AODV depends on each node in the network to establish a network (route), here comes the problem, the node what AODV believes to establish a network may be a malicious or compromised node. These malicious nodes can attack routing protocols in several ways. These attacks can be categorized as passive attacks and active attacks.

***Passive attacks*:** A passive routing attack does not disrupt the operation of a routing protocol, but only attempts to discover valuable information by listening to the routing traffic. Hence such attacks are difficult to detect.

Active attacks: An active attack attempts to improperly modify data, gain authentication, or procure authorization by inserting false packets into the data steam or modifying packets transition through the network. Active attacks are of two types: external and internal. An external attack is one caused by nodes that do not belong to the network. An internal attack is one from compromised or hijacked nodes that belong to the network. As malicious nodes already belong to the network as authorized parties, and hence are protected with network security mechanisms and services, therefore, internal attacks are more severe.

The attacks on the AODV routing protocol [2, 3] are:

***(a).Message tampering attack*:** An attacker can alter the content of routing messages and forward them with falsified information. For example, by reducing the hop-count field in either an RREQ or RREP packet, an attacker can increase its chance to be an intermediate node of the route. A selfish node can relieve the burden of forwarding messages for others by setting the hop-count field of the RREQ to infinity.

(b).Message dropping attack: Both attackers and selfish nodes can intentionally drop some (or all) routing and data messages. Since all the mobile nodes within a MANET function as both end hosts and routers, this attack can paralyze the network completely as the number of message dropping increases.

(c).Message replay (or wormhole) attack: Attackers can retransmit eavesdropped messages again later in a different place. One type of replay attacks is the wormhole attack. A wormhole attacker can tunnel an RREQ directly to a destination node. Since a wormhole attacker may not increase the hop-count field value, it prevents any other routes from being discovered. The wormhole attack can be combined with the message dropping attack to prevent the destination node from receiving packets.

2.3. The features required for [4] AODV routing protocol to provide security:

(a) *Source authentication*: The receiver should be able to confirm that the identity of the source is indeed who or what it claims to be.

(b) *Neighbor authentication*: The receiver should be able to confirm that the identity of the sender (i.e., one hop previous node) is indeed who or what it claims to be.

(c) *Message integrity*: The receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit.
(d)*Access control*: It is necessary to ensure that mobile nodes seeking to gain access to the network have the appropriate access rights.

3. SECURE ROUTING PROTOCOLS

3.1. Secure AODV (S-AODV) [5]:

SAODV is a security extension of AODV protocol based on public key cryptography. SAODV routing messages (RREQs, RREPs, and RERRs) are digitally signed to guarantee their integrity and authenticity. It avoids active external attacks by not forwarding route requests to the external nodes. This is done by authenticating all the nodes of the network by issuing the same passwords to all the nodes. Before forwarding route request to a neighbor, a node first checks the authenticity of the neighboring node by verifying its password. If it is found legal, then only route request is forwarded. In this way, external nodes are excluded from entry into the network.
In SAODV, (i).**digital signatures** are used to authenticate RREQ and RREP messages and (ii).**hash chain**s are used to authenticate the hop-count fields within the RREQ and RREP messages.

A node that generates a routing message signs it with its private key and the nodes that receive this message verify the signature using the sender's public key. The hop count cannot be signed by the sender, because it must be incremented at every hop, to protect it hash chain a mechanism is used. In this way malicious node cannot increment the hop count only destination node can give RREP reply, because the RREP message must be signed by the destination node.

S-AODV also includes a mechanism called "double signature" by which intermediate node can reply to RREQ messages. When a node N1 generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on RREP message towards N1 itself. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node N1. If one of these nodes then receives a RREQ towards node N1, it can reply on behalf of N1 with a RREP message, similarly to what happens with regular AODV. To do so, the intermediate node generates the RREP message, includes the signature of node N1 that it previously cached, and signs the message with its own private key. SAODV does not require additional messages when compared to AODV. Due to digital signatures SAODV messages are bigger. Moreover, SAODV requires heavy weight asymmetric cryptographic operations, every time a node generates a routing message, it must generate a signature, and every time it receives a routing message (also as an intermediate node), it must verify a signature. This gets worse when the double signature mechanism is used, because this may require the generation or verification of two signatures for a single message. The major operations of SAODV to authenticate routing data are hash chains and signatures.

3.1.1. SAODV Signatures

To calculate signatures, Hop Count field is set to zero, as it is a mutable field. In the case of the Signature for RREP field of the RREQ Double Signature Extension, what is signed is the future RREP message that nodes might send back in response to the RREQ.
To construct this message it uses the values of the RREQ and the Prefix Size (the RREP field that is not derivable from the RREQ but not zeroed when computing the signature. In the case of RREPs, R and A flags are set to zero. SAODV is not designed taking into account AODV multicast ('R' flag is used in multicast) and 'A' flag is mutable and, if an attacker alters it, it can only lead to some sort of denial of service. Every time a node generates a RREQ it decides if it should be signed with a Single Signature Extension or with a Double Signature Extension. All implementations MUST support RREQ Single Signature Extension, and SHOULD support RREQ Double Signature Extension. A node that generates a RREQ with the gratuitous RREP flag set SHOULD sign the RREQ with a Double Signature Extension. A node SHOULD never generate a RREQ without adding a Signature Extension.

When a node receives a RREQ, first verify the signature before creating or updating a reverse route to that host. Only if the signature is verified, it will store the route. If the RREQ was received with a Double Signature Extension, then the node will also store the signature, the lifetime and the Destination IP address for the RREP in the route entry. If a node receives a RREQ without a Signature Extension it SHOULD drop it. An intermediate node will reply a RREQ with a RREP only if fulfills the AODV requirements to do so, and the node has the corresponding signature and the old lifetime and old originator IP address to put into the 'Signature', 'Old Lifetime' and 'Old Originator IP address' fields of the RREP Double signature Extension. Otherwise, it will rebroadcast the RREQ. When a RREQ is received by the destination itself, it will reply with a RREP only if fulfills the AODV requirements to do so. This RREP will be sent with a RREP Single Signature Extension.

All implementations MUST support RREP Single Signature Extension, and SHOULD support RREP Double Signature Extension. A node SHOULD never generate a RREP without adding a Signature Extension. This also applies to gratuitous RREPs. When a node receives a RREP, first verifies the signature before creating or updating a route to that host. Only if the signature is verified, it will store the route with the signature and the lifetime and the originator IP address of the RREP. If a node receives a RREP without a Signature Extension it SHOULD drop it. Every node, generating or forwarding a RERR message, uses digital signatures to sign the whole message and any neighbor that receives verifies the signature.

In this way it can verify that the sender of the RERR message is really the one that claims to be. And, since destination sequence numbers are not singed by the corresponding node, a node SHOULD never update any destination sequence number of its routing table based on a RRER message. Although 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.

3.1.2. SAODV Hash Chains

Hash chains are used in SAODV to authenticate the hop count of the AODV routing messages (not only by the end points, but by any node that receives one of those messages. Every time a node wants to send a RREQ or a RREP it generates a random number (seed). Select a Maximum Hop Count. Maximum Hop Count SHOULD be set to the TTL value in the IP header, and SHOULD never exceed its configuration parameter NET_DIAMETER.

The Hash field in the Signature Extension is set to the seed. The Top Hash field is set to the seed hashed Max Hop Count times. Every time a node receives a RREQ or a RREP it verifies the hop count by hashing Max Hop Count Hop Count times the Hash field, and checking that the resultant value is the same than the Top Hash. If the check

fails, the node SHOULD drop the packet. Before rebroadcasting a RREQ or forwarding a RREP, a node hashes one time the Hash field in the Signature Extension.

The function used to compute the hash is set in the Hash Function field. Since this field is signed, a forwarding node will only be able to use the same hash function that the originator of the routing message has selected. If a node cannot verify or forward a routing message because it does not support the hash function that has been used, then it drops the packet.

3.1.3. The problems addressed by SAODV.

It avoids active external attacks by not forwarding route requests to the external nodes. The problem of route table overflow is solved by updating the tables at regular intervals. SAODV solves the problem of blackhole by disabling the intermediate nodes to send route replies and there by allowing the generation of route reply only by the destination node. No malicious node can read the data in the data packet due to the encryption of the message. Every node checks password before forwarding the RREQ. All nodes on the route from source to destination are secure and fulfill security requirements of the sender.

3.2 Adaptive Secure AODV (A-SAODV)

Adaptive Secure AODV (A-SAODV) [3] is a prototype implementation of SAODV, based on the AODV-UU. It follows multi threaded application which avoids the blocking of processing of other messages. It has two execution threads: one dedicated to cryptographic operations and the other to handle the functions like routing message processing, SAODV routing table management, timeout management, SAODV message generation and data packet forwarding.

The two threads communicate via a first input first output (FIFO) queue containing all the messages that must be signed or verified. The prototype developed includes an experimental feature, the *adaptive reply decision*, to optimize SAODV performance with respect to the double signature option.

In AODV, allowing intermediate nodes to generate RREPs on behalf of the destination node has a positive impact on performance, because it does not require heavyweight operations by intermediate nodes themselves. The situation is different in SAODV, because generating such a reply requires the intermediate node to generate a cryptographic signature nodes may spend much time in computing these signatures and become overloaded.

Moreover, if intermediate nodes have a long queue of routing messages that must be cryptographically processed, the resulting delay may be longer than if the request reaches the destination node. If the double signature mechanism removed, an uncollaborative protocol created, in which only the destination node is allowed to reply to a RREQ message. This is possible, the A-SAODV approach makes the double signature feature adaptive: intermediate nodes reply to RREQs only if they are not overloaded. Each node has a queue of routing messages to be signed or verified

When a node receives a RREQ message and has the information to generate a RREP on behalf of the destination, it checks the queue length and compares it with a threshold. If the queue length is lower than the threshold, the node generates a RREP (collaborative behavior); otherwise it forwards the RREQ without replying (uncollaborative behavior). The same mechanism can be applied when generating a RREQ message in order to decide between a single signature and a double signature. In the simplest case, the threshold can be a fixed value; however, this would not be very flexible because the value maybe adjustable, depending on external factors (e.g., battery state). In the A-SAODV prototype, the threshold value can be changed during execution (two special values allow always *reply* behavior and *never reply* behavior). Other, more elaborate strategies could be defined to estimate the crypto queue delay and consequently decide whether to reply or forward the message.

For example, a fixed threshold (based on the timeouts defined by the routing protocol) and a predictor of queuing times could be used. In this way, the algorithm could adapt itself to the situation and the computing power of the node. An additional external parameter could be used to take into account the previously mentioned external factors (how much a node is willing to collaborate, e.g., depending on its battery state). Another little optimization included in the A-SAODV prototype is a cache of latest signed and verified messages, in order to avoid signing or verifying the same message twice.

Each of the above mentioned protocols have their own merits and demerits upon the user requirement a particular protocol may be selected, but no protocol is perfect many researches are going in this field to extend the features of protocols.

4. PARAMETERS OF PERFORMACE EVALUTION

The following parameters are generally used to evaluate the performance of secure routing protocols during establishment of a route and packet delivery.

(a). No. of data packets Vs No. of nodes in the network **:** It describes the number of data packets reaching to the nodes in a legitimate network

(b). No. of data packets Vs No. of malicious nodes: It describes the number of data packets reaching to the nodes in a malicious environment

(c). Packet Delivery Ratio (PDR) Vs No. of malicious nodes: PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source.

(d).The average end to end delay: The delay experienced by packet from the time it was sent by a source till the time it reached the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation and transfer times. For each packet sent, calculate the send time and receive time, then average it.

(e) Number of Dropped Packets: This shows the total number of dropped packets.

(f). Routing Control Overhead: The amount of overhead during the transportation of data packet (in bytes)

(g). Routing Overhead: The number of routing packets transmitted for every data packet sent. Each hop of the routing packet is treated as a packet. *Normalized routing load* are used as the ratio of routing packets to the data packets.

Normalized Routing Load = routing packets sent / packet received

(h). Routing Packets: It shows the amount of routing packets (i.e. RREQ, RREP and RERR) generated during one transmission.

5. CONCLUSION

In this paper we have introduced the MANET and the importance of securing a routing protocol like AODV. We have focused on the drawbacks of AODV and pointed out what features can be added to make AODV secure, there are other features what can be still added to make AODV more secure. We have discussed S- AODV which is a security extension of AODV. S-AODV can be further explored to add more features which is a future work. We have discussed A-SAODV which is an extension of S-AODV into which can also future extensions can be done. We have to further explore deep into the various approaches of providing security on the basic mechanism of routing.

REFERENCES:

[1] Jane Zhen and Sampalli Srinivas, "*Preventing Replay Attacks for Secure Routing in Ad HocNetworks*", Dalhousie University, Halifax, NS, Canada, Springer-Verlag Berlin Heidelberg 2003, ADHOC-NOW 2003, LNCS 2865, pp. 140–150, 2003.

[2] Jean-Pierre Hubaux,Levente Buttyyan, Srdan Capkun, The Quest for Security in Mobile Ad-hoc Networks

[3] M. F. Juwad, and H. S. Al-Raweshidy, "*Experimental Performance Comparisons between SAODV & AODV*", IEEE Second Asia International Conference on Modelling & Simulation, 2008

[4] C. E. Perkin, E. M. Royer, "Ad-hoc on demand distance vector(AODV)routing," The Second IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999.

[5] Manel Guerrero Zapata:"Secure Ad hoc On-Demand Distance Vector (SAODV) Routing "INTERNET-DRAFT draft-guerrero-manetsaodv-06.txt. September 2006.