ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (311-318), Month: April-June 2014, Available at: www.researchpublish.com

Secured Routing in MANETs

[1]G.Anandhi, [2]Dr.S.K.Srivatsa

[1]Research Scholar, [2]Senior Professor
[1]Vels University , [2]St.Joseph's College of Engineering, Chennai – 117

Abstract: **The existing ad hoc routing protocols do not accommodate any security and are highly vulnerable to attacks. We discuss threats and attacks against ad hoc routing under several areas of application. A mobile ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. The assumption of a trusted environment is not one that can be realistically expected; hence, several efforts have been made toward the design of a secure and robust routing protocol for ad hoc networks. We formulate the threat model for ad hoc routing and present several specific attacks that can target the operation of a protocol. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In this article we study the routing security issues of MANETs, and analyze in detail one type of attack — the "black hole" problem — that can easily be employed against the MANETs. We also propose a solution for the black hole problem for ad hoc on-demand distance vector routing protocol. Reason for this increased attention is the wide range of multimedia applications running in an infrastructure less environment. Because of the infrastructure less environment, limited power and dynamic topology it becomes very difficult to provide a secure environment in MANET. In this paper we are providing a detailed survey of different kind of attacks and proposed solutions for handling those attacks. This paper also gives a brief comparison of various protocols available for secured routing in MANET.**

Keywords: **DOS attack, ARAN (Authenticated Routing for Ad hoc Network), Secure Ad-hoc On-demand Distance Vector Routing Protocol (SAODV), Security-Aware ad hoc Routing (SAR), Secure Efficient Ad-hoc Distance Vector Routing (SEAD)**

I. INTRODUCTION

Mobile ad hoc networks remove this dependence on a fixed network infrastructure by treating every available mobile node as an intermediate switch, thereby extending the range of mobile nodes well beyond that of their base transceivers. Other advantages of manets include easy installation and upgrade, low cost and maintenance, more flexibility, and the ability to employ new and efficient routing protocols for wireless communication.[1]

An ad hoc network is an infrastructureless network where the nodes themselves are responsible for routing the packets. The links are usually wireless, any security that was gained because of the difficulty of tapping into a network is lost. The routing protocol sets an upper limit to security in any packet network. If routing can be misdirected, the entire network can be paralyzed. It is hard to distinguish compromised nodes from nodes that are suffering from bad links. The main objective of this paper is to discuss ad hoc routing security with respect to the area of application. We limit our study to IP based networks.[1] 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 as do 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 following section presents a brief introduction to the general problem of ad hoc routing, which is required since several of the surveyed proposed solutions secure existing protocols. We present

the possible attacks that a malicious node can use for disrupting the operation of a routing protocol in a self-organized network.[2]

Two basic system models have been developed for the wireless network paradigm. The fixed backbone wireless system model consists of a large number of mobile nodes and relatively fewer, but more powerful, fixed nodes. These fixed nodes are hard wired using landlines. [3] The communication between a fixed node and a mobile node within its range occurs via the wireless medium. However, this requires a fixed permanent infrastructure. Another system model, the *mobile ad hoc network* (MANET) has been proposed to set up a network when needed; however, the transmission range of each low-power node is limited to each other's proximity, and out-of-range nodes are routed through intermediate nodes. We describe the black hole problem in AODV protocol in detail. To mitigate the attacks, one feasible solution to the black hole problem is presented. Some special characteristics of MANET like dynamic topology, fast deployment, robustness make this technology an interesting research area. Each node in MANET can work as a

sender, receiver as well as router . Communication in the network depends upon the trust on each other. Communication can work properly if each node co-operate for data transmission.[4]

The following algorithm depicts the communication in any ad hoc network:

1. Sender node sends the signal to the neighboring nodes within the vicinity.

2. Neighboring nodes communicate with the sender node

3. Sender node sends the message to the destination node.

4. If destination node is within the vicinity then message received by the destination node else an intermediate node receives the message.

5. Restart the process of forwarding the message from step no 1 till the destination node is reached.

This paper provides a survey on the various security issues, attacks and various proposed routing protocols against these attacks.

II. MANETs

Manets are useful for disaster management. A communications infrastructure is designed to survive common short-term problems, such as overloading, but not to sustain major physical damage. In most cases, the collapse of a single system will cause many dependent devices to fail. If a fire, earthquake, or other natural catastrophe disables a subset of base stations, every mobile phone within range of those stations automatically becomes unreachable. In such situations, rescue workers can use the nodes in manets to create a network "on the fly." [1]

Small-scale manets are also effective for emergency search and rescue, battlefield surveillance, and other communication applications in hazardous environments. For example, robots or autonomous sensors deployed in an area inaccessible to humans could use simple manet routing protocols to transmit data to a control center. Even if many robots or sensors are disabled or destroyed, the remaining ones would be able to reconfigure themselves and continue transmitting information.

Routing in MANETs

Manets use multihop rather than single-hop routing to deliver packets to their destination. There are several well known protocols in the literature that have been specifically developed to cope with the limitations imposed by ad hoc networking environments. The problem of routing in such environments is aggravated by limiting factors such as rapidly changing topologies, high power consumption, low bandwidth, and high error rates.[3]

Routing Protocols of MANETS

Many different routing protocols have been developed for MANETs. They can be classified into two categories:

Table-driven: Table driven routing protocols essentially use proactive schemes. They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

On demand: A different approach from table-driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined.

III. ATTACKS

In a passive attack, the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routing traffic. The major advantage for the attacker in passive attacks is that in a wireless environment the attack is usually impossible to detect. This also makes defending against such attacks difficult. To perform an active attack the attacker must be able to inject arbitrary packets into the network. The goal may be to attract packets destined to other nodes to the attacker for analysis or just to disable the network. A major difference in comparison with passive attacks is that an active attack can sometimes be detected. This makes active attacks a less inviting option for most attackers.[2]

Here are some of the active attacks in ad hoc network.

Black hole. In the attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In a flooding based protocol such as AODV the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply where an extremely short route is advertised. If the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

Routing table overflow. In a routing table overflow attack the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing algorithms attempt to discover routing information even before it is needed while a reactive algorithm creates a route only once it is needed. This property appears to make proactive algorithms more vulnerable to table overflow attacks. An attacker can simply send excessive route advertisements to the routers in a network. Reactive protocols, on the other hand, do not collect routing data in advance. For example in AODV, two or more malicious nodes would need to cooperate to create false data efficiently: The other node requests routes and the other one replies with forged addresses.

Sleep deprevation. Usually, this attack is practical only in ad hoc networks, where battery life is a critical parameter. Battery powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes, or by forwarding unnecessary packets to the node using, for example, a black hole attack. This attack is especially suitable against devices that do not offer any services to the network or offer services only to those who have some special credentials. Regardless of the properties of the services, a node must participate in the routing process unless it is willing to risk becoming unreachable to the network.

Location disclosure. A location disclosure attack can reveal something about the locations of nodes or the structure of the network. The information gained might reveal which other nodes are adjacent to the target, or the physical location of a node. The attack can be as simple as using an equivalent of the trace route command on Unix systems. Routing messages are sent with inadequate hop-limit values and the addresses of the devices sending the ICMP error-messages are recorded. In the end, the attacker knows which nodes are situated on the route to the target node. If the locations of some of the intermediary nodes are known, one can gain information about the location of the target as well.

Replay : An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

Wormhole : The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunnelled traffic back into the network . The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers.

Blackmail : This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender.

An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated .

Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the *routing table overflow* and the *sleep deprivation torture* . In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

Routing Table Poisoning: Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even partitioning certain parts of the network.

Routing table overflow: The attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.

Impersonation: A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table.

Energy consummation: Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.

Information disclosure: The malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route.

Strategic Routing Attacks

Encyclopedia Britannica defines strategy as “the science and art of military command exercised to meet the enemy in combat under advantageous conditions.” The definition covers areas such as intelligence gathering. It might also cover destruction of enemy networks in preparation for battle. However, once a routing attack has ended, the network can usually be brought back into use in a short amount of time. Additionally, because of the attack, the target could gain some information about where the enemy is about to strike next. Thus, active attacks are probably best suited to tactical use while passive attacks can be effective in gathering information. Passive routing attacks have a wide range of use. One can deduce things about the location of nodes, and the roles of each node in the network. Obvious targets include command and control nodes. They may be distinguishable from other nodes by traffic analysis targeted at the routing protocol, since routes to them are likely to be needed more often than to a typical node in a network.[2]

Tactical Routing Attacks

Tactics is the science of disposing and maneuvering forces in combat. Tactical routing attacks could be used most effectively during battle. The attacks might use information about the network topology or relationships between nodes as well as other information that has been collected earlier using passive attacks. The main goal could be to temporarily disable some important part of a network using denial-of-service attacks.[2]

IV. SECURITY IN MANETs

Although no single node in a manet is trustworthy,threshold cryptography can distribute trust to an aggregation of nodes. This scheme lets n parties share the ability to perform a cryptographic operation such that any t parties can do it together, while up to $t - 1$ parties cannot perform the operation. However, dividing a private key into n shares and constructing t partial signatures is nontrivial given that traditional key distribution schemes either do not apply to the ad hoc scenario or are not efficient for resource-constrained devices. Combining identity-based techniques with threshold cryptography can achieve flexible and efficient key distribution. After distribution, a combiner can verify the t signatures and compute the final signature for the certificate. In this way, up to $t - 1$ compromised nodes cannot generate a valid certificate by themselves. If a large number of nodes are compromised, attributing fault to a specific malicious node is impossible. A proposed algorithm addresses this problem by limiting the possible fault location to the link between two adjacent nodes; as long as a fault-free path exists between two nodes, they can establish a secure communication link even if most nodes in the network are compromised. In addition, this algorithm can detect selfish nodes that refuse to cooperate with other nodes. If their behaviour is the result of a denial-of-service attack rather than power-savings activity, the algorithm can isolate the selfish nodes.[1]

Security protocols for MANET's can be mainly categorized in two major categories:

Prevention: This mechanism involves protocols which prohibit the attacking node to initiate any action. This approach requires encryption technique to authenticate the confidentiality, integrity, non-repudiation of routing packet information.

Detection and Reaction: Detection and Reaction mechanism as the name suggest will identify any malicious node or activity in the network and take proper action to maintain the proper routing in the network.[5]

A Proposed Solution to the Black Hole Problem

One possible solution to the black hole problem is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense we avoid the black hole problem and implement a secured AODV protocol. But there are two associated disadvantages. First, the routing delay is greatly increased, especially for a large network. Second, a malicious node can take further action such as fabricate a reply message on behalf of the destination node. The source node cannot identify if the reply message is really from the destination node or fabricated by the malicious node. In this case, the method may not be adequate. We propose another solution using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it exists, we can trust the intermediate node and send out the data packets. If not, we just discard the reply message from the intermediate node and send out alarm message to the network and isolate the node from the network.[4]

1. Prevention Using Asymmetric Cryptography

a) Authenticated Routing for Ad-hoc Network (ARAN) : Authenticated Routing for Ad-hoc Network (ARAN) is an On-Demand routing protocol which uses the cryptographic certification. This protocol consists of the following steps:

preliminary certification step which requires of a trusted certification authority, who distributes its public key to all the nodes in the network. It is necessary for each node to certify its address and to have the public key before connecting to the network.

Second step is the route discovery for end-to-end authentication. The goal of end-to-end authentication is for the source to verify that the intended destination was reached. The source begins route instantiation by broadcasting a digitally signed

Route Discovery Packet(RDP). The RDP includes the certificate of the initiating node, a nonce, a timestamp and the address of the destination node. Nonce and timestamp are present to prevent replay attacks and to detect looping and appends its signature on the packet. All subsequent intermediate nodes remove the signature of the previous node, verify it and append their signature on the packet. Similarly, along the reply packet (REP) each node appends its signature before forwarding it to the next hop. In order to maintain the route, nodes keep track of whether routes are active or not. An error message is generated and forwarded to the source node if the data is received from an inactive or broken node.

2. Prevention Using Symmetric Cryptography

a) Security Aware Ad-hoc Routing : Security-Aware ad hoc Routing (SAR) makes use of security attributes to take the routing decision. In SAR, security metric is embedded into the RREQ packet. Nodes are required to have keys for decryption of data while forwarding or receiving the data. If a path with the required security attributes is found a RREP is sent from an intermediate node or the destination node to the source node. In case of more than one route the shortest route is selected for data forwarding.

b) Secure Routing Protocol : Secure Routing Protocol (SRP) is another routing protocol which uses symmetric cryptography. The protocol is based on route querying method. SRP Requires a Security Association (SA) between source and destination node. Key generated by the SA is used to encrypt and decrypt the data by the two nodes. A SRP Header is added to the base header. The RREQ packet consists of a *query sequence number (QSEQ), query identifier (QID),* and the out put of a key hashed function. The key hash function takes IP header, header of the basic routing protocol, and the shared key.

The intermediate nodes broadcast the query to the neighboring nodes and update their routing table. If receiving node has the same QID in their routing table, query is dropped. When the destination is reached, destination node checks for the security metrics by calculating the key hash function ―*message authentication code (MAC)"*. After verifying the secret key it generates reply packet for source node consisting of path from source to destination, QID, QSEQ. After receiving the reply packet source node again calculates its MAC. There can be multiple routes from source to destination. Route maintenance in this protocol is also done through route error message.

3. Prevention Using one-way hash chains

a) Secure Efficient Ad-hoc Distance Vector Routing : Secure Efficient Ad-hoc Distance Vector Routing (SEAD) protocol is a proactive routing protocol based on the design of DSDV protocol. This protocol is used against the modification attacks. This protocol makes use of hash chain method for checking the authenticity of the data packet. This hash chain value is used for transmitting a routing update. A node that receives a routing update, verifies the authentication of each entry of the message. SEAD make use of destination sequence number in order to remove looping. To avoid loops, SEAD protocol also authenticates the source of routing update message. This can be done with any one of the following two mechanisms:

i) make use clock synchronization between the nodes that participate in the ad hoc network, and employs broadcast authentication mechanisms.

ii) By providing a shared secret Key between pair of nodes for *message authentication code* (MAC) between the nodes for the authentication of a routing update message.

b) Ariadne : Ariadne is an on-demand secure ad-hoc routing protocol based on DSR with symmetric cryptography. This protocol makes use of a shared key between the nodes for authentication (MAC). Ariadne protocol can be carried out in 3 steps which are as follows:

When source node wants to communicate with other node, it sends a route request (RREQ) containing source address, destination address, an Identifier that identifies the current route discovery, a TESLA time interval denoting the expected arrival time of the request to the destination, a hash chain. On receiving the RREQ the intermediate node checks for the validity of the TESLA time interval. In order to check the authentication a one-way hash function is used. If data packet is a valid packet then the node appends its own address in the node list, replaces the hash chain with a new one consisting of

its address plus the old one, and appends a MAC of the entire packet to the MAC list. The destination node verifies each hop of the path by comparing the received hash and the computed hash of the MAC.

4. Hybrid approach

a) Secure Link State Routing Protocol : The Secure Link State Routing Protocol (SLSP) is used to secure the discovery and the distribution of link state information. This protocol makes use of asymmetric key for the security purpose. Participating nodes are identified by the IP addresses of their interfaces. SLSP can be logically divided into three major steps which are as follows:

Public key distribution: SLSP do not make use of any central server for key distribution. Distribution of public key is done by the node to the nodes within its own vicinity. This distribution of the key is known as public key distribution (PKD). Neighbor discovery: Link state information of the node is broadcast periodically using Neighbor Lookup Protocol (NLP). Hello message contains sender's MAC address and IP address of the network. These messages are also signed. NLP can be used for identifying the discrepancies or the malicious node. Link state updates. Link state update (LSU) packets are identified by the IP address of the initiating node and include a 32-bit sequence number for providing updates. Intermediate nodes LSU verify the attached signature using a public key they have previously cached in the pubic key distribution phase of the protocol. The hops_traversed field of the LSU is set to hashed hops_traversed, the TTL is decremented and finally the packet is broadcasted again. To protect against denial of service attacks, SLSP nodes maintain a priority ranking of their neighboring nodes based on the rate of control traffic they have observed. High priorities are given to nodes that generate LSU packets with the lowest rate. This functionality enables the neighbors of malicious nodes that flood control packets at very high rates to limit the effectiveness of the attack. .

b) Secure Ad-hoc On-demand Distance Vector Routing Protocol: Secure Ad-hoc On-demand Distance Vector Routing Protocol (SAODV) is based on AODV routing Protocol. SAODV make use of asymmetric cryptography as well as hash chaining. When a node wants to send a message it digitally signs the RREQ packet and send it to the neighboring nodes. On receiving a RREQ, intermediate nodes verifies the signature before updating or creating a reverse route to the host with the help of cryptography.

Hash chains are used in SAODV to authenticate the hop count. When a node wants to send a RREQ or a RREP it generates a random number called as seed. It Selects a Maximum Hop Count which should be set to the TTL value in the IP header. 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. Whenever an intermediate node receives a RREQ or a RREP it verifies the hop count by hashing Max Hop Count - Hop Count times the Hash field and check whether the resultant value is same as Top Hash value. If two values are different from each other, data packet will be dropped by the node. For the broken links an error message is generated by the nodes.[5]

V. CONCLUSIONS

If the security in the routing protocol is nonexistent, the network can have no security against denial-of-service attacks that can disable the entire network. Other serious threats resulting from routing protocols is the disclosure of some information about the network structure and the movement of the nodes within the network. Currently, ad hoc routing protocols are vulnerable to several kinds of attacks, and none of the available protocols make any visible attempt at reducing their vulnerability. Also, existing security enhancement techniques such as the Non-Disclosure Method and IPsec are either too expensive or ineffective to be of value. Unless protection against routing attacks can be provided by the applications that are used in the network, current routing protocols should not be used in areas of applications where the threats of denial-of-service attacks, forged routes, or location disclosure are of any significant importance. The analysis of the different proposals has demonstrated that the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. The comparison we have completed between the surveyed protocols indicates that the design of a secure ad hoc routing protocol constitutes a challenging research problem since already existing generic solutions, such as IPsec, cannot be successfully applied. A wireless MANET presents a greater security problem than conventional wired and wireless networks due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability. Routing security plays an important role in the security of

the entire network. In general, routing security in wireless networks appears to be a nontrivial problem that cannot easily be solved. It is impossible to find a general idea that can work efficiently against all kinds of attacks, since every attack has its own distinct characteristics. In this article we study the routing security issues of MANET, analyze one type of attack, the black hole, that can easily be deployed against a MANET. One limitation of the proposed method is that it works based on an assumption that malicious nodes do not work as a group, although this may happen in a real situation.

REFERENCES

[1] Routing and Security in Mobile Ad Hoc Networks, *Nikola Milanovic, Miroslaw Malek, Anthony Davidson, Veljko Milutinovic*

[2] Routing Security in Ad Hoc Networks, Janne Lundberg

[3] Secure Routing for Mobile Ad hoc Networks, Patroklos G.Argyroudis and Donal O'Mahony – IEEE Communications Surveys , The Electronic magazine of original peer reviewed survey articles.

[4] Routing Security in Wireless Ad hoc Networks, *Hongmei Deng, Wei Li, and Dharma P. Agrawal*

[5] A Comparative Study for Secure Routing in MANET , Parul Tomar, Prof. P.K. Suri, Dr. M. K. Soni - *International Journal of Computer Applications (0975 – 8887) Volume 4 – No.5, July 2010*

[6] Y. Desmedt, "Some Recent Research Aspects of Threshold Cryptography," *Proc. 1st Ann.Workshop Information Security*, LNCS 1396, Springer-Verlag, 1997, pp. 158-173.

[7] Khalili, J. Katz, and W.A. Arbaugh, "Toward Secure Key Distribution in Truly Ad-Hoc Networks,"*2003 Symp. Applications and the Internet Workshops (SAINT 03 Workshops)*, IEEE CS Press, 2003, pp. 342-346.