International Journal of communication and computer Technologies, ISSN: 2278-9723

Available at http://www.ijccts.org

A Research Study On Packet Forwarding Attacks In Mobile Ad-Hoc Networks

(*MANET*)

Bhaskar Kumawat, Dev Kumar

Computer Science & Information Communication, Suresh Gyan Vihar University, India

Received: 18-07-2012, **Revised:** 16-10-2012, **Accepted:** 30-11-2012, **Published online:** 28-12-2012

Abstract— **In this thesis we analyzed selective packet dropping where malicious node drops packets based on packet destinations or some other characteristics ,this type of attacks called packet forwarding attacks. The MANET requires a careful and security-oriented approach for designing communicational protocol .For this we study the DSR and AODV protocols .The information also needed for this is topology information, such as node moving speed , local routing information , such as route cache entries and route updates; and traffic information, all incoming and outgoing traffic statistics, including inter-arrival periods and frequencies. The intuition here is that there should be correlation between node movements and routing table changes, and between routing changes and traffic changes under normal conditions, and that such information can be used to detect anomalies caused by attacks.**

Keywords- Packet dropping ,DSR ,AODV,Routing information.

I. INTRODUCTION

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be desktops/laptops with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Figure1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them.[1][2][8]

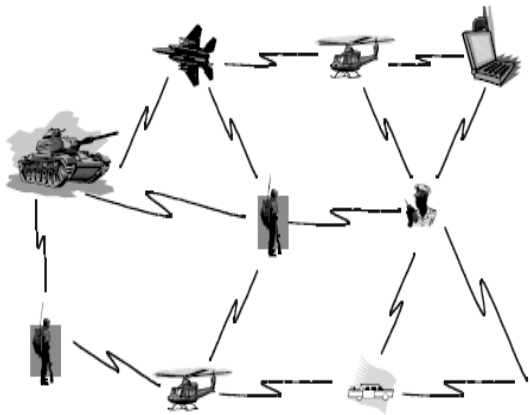

Figure 1 Overview of Mobile Ad-hoc Network

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

II. ROUTING PROTOCOLS IN MANET

The special structure of Ad-hoc networks requires the routing mechanisms to be dynamic and on-demand. Routes have to be adapted to the constantly changing network topology .Moreover, routing is not only performed by special nodes, but by every member of the network. Before we introduce the vulnerabilities of ad-hoc networks in the following section, let us brief present two commonly used routing protocols for ad-hoc networks ,namely DSR and AODV.[7]

A. Dynamic Source Routing Protocol (DSR)

DSR is an on-demand source routing protocol. It is referred to as "on-demand" because route paths are

discovered at the time a source sends a packet tɵ a destination for which the source has no path .How is a route discovered? Suppose a node S wishes to communicate with a node D but does not know any path to D. It initiates a route discovery by sending a route request broadcast to its neighbors. This packet contains the destination address D. The neighbors append their own address to the route request packet and rebroadcast it. The process continues until the route request reaches D. D now sends back a route reply packet to S to inform it about the discovered route. D may choose the reverse path (all nodes on the path the route request packet traveled have been appended to the packet) or initiate a new route discovery back to S. A source may receive multiple route replies from a destination, because there may be many routes from S to D. These routes are cached for future use .

B. Ad-hoc On-demand Distance Vector Routing Protocol (AODV)

The AODV protocol is a table-driven routing protocol and it is based on the classical Bellman-Ford routing algorithm .How is a route discovered? When a source node S wants to send a packet to a destination D and does not already have a route, it broadcasts a route request packet across the network. Nodes that receive this packet update their information for the source node and their routing tables. If the node is either the destination S or knows a recent path to S, it may send a route reply back to the source. Otherwise, the route request is rebroadcasted. Security in Ad-hoc Networks As the route reply propagates back to the source, the nodes on the way update their routing tables with the information about the route to D. Routes are maintained as long as data packets are traveling periodically from the source to the destination. Once the source stops sending packets, the link will time out and eventually be deleted from the routing tables of the intermediate nodes. If a link break is detected by an intermediate node, a route error message is propagated back to S. If it still desires the route, it has to reinitiate a route discovery .AODV typically minimizes the number of required broadcasts, i.e. nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges.

III. Attacks On Packets In Manet

In this type of attacks, some of the protocol fields of the packets passed among the nodes are modified, thereby resulting in traffic subversion, redirection or Denial of Service (DoS) attacks. The following sections discuss some of these attacks.[7][4][5]

Modification of route sequence numbers: This attack is possible against the AODV protocol. The malicious node can change the sequence number in the route request packets or route reply packets in order to make the route fresh. In this malicious node M receives a route request RREQ from neighbor node B that originates from node S and is destined for node X.M unicasts a RREP to B with a higher destination sequence number for X than the value last advertised by X. The node S accepts the RREP and then sends the data to X through M. When the legitimate RREP from X gets to S, if the destination number is less than the one advertised by M, then it will be discarded as a stale route. The situation will not be corrected until a valid RREP with higher sequence number than that of M gets to S.

- **Modification of hop count:** This type of attacks is possible against the AODV protocol in which a malicious node can increase the chance that they are included in a newly created route by resetting the hop count field of a RREQ packet to a lower number or even zero. Similar to route modification attack with sequence number, the hop count field in the routing packets is modified to attract data traffic.
- **Modification of source route:** This attack is possible against DSR which uses source routes and works as follows .It is assumed that the shortest path exists from S to X. It is also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to X with the source route S-A-B-C-D-X. If M intercepts this packet, it removes D from the list and forwards it to C. C will attempt to forward this packet to X which is not possible since C cannot hear X. Thus M has successfully launched a DoS attack on X.

IV. Security Aware Routing Peotocols In Manet

There were various protocols designed for security of Mobile Ad-hoc networks are[3][7][6]:-

A. Ariadne

Ariadne is a reactive secure ad hoc network routing protocol based on DSR .In the route discovery Ariadne includes the source and destination addresses, a request ID and a time interval used for TESLA. In the packet header a field for a hash chain is included and also two lists, one is the node list as in the original DSR and the other is a MAC list. The hash chain is initialized by the initiator of the request by making a

secure MAC using a symmetric secret key. The input for the MAC calculation is the source, destination, request id, and the time interval value. The request is broadcast to all the initiators neighbours.When a node receives a route request that is not destined for itself it calculates the next hash chain value using a one-way hash function with its own address and the previous, incoming, hash chain value. It also calculates the next field in the MAC list using its TESLA key for the specified time interval. Before forwarding the request message the fields are updated with the newly computed information .The hash chain value is replaced while the address and MAC values are appended to their respective lists .The target of the request checks the validity of the request by verifying that the intermediate nodes' TESLA keys have not been disclosed for the time interval yet. It also makes certain that the hash chain is correct by computing the whole chain;since it shares the secret key with the initiator it can do this. If these checks certify that the request was valid a route reply is constructed and sent back to the initiator. The reply packet consists of the target and initiator addresses, time interval, node list, MAC list, target MAC, and a key list. All the fields prior to target MAC correspond to the fields in the incoming request. The target MAC is computed by the target on these fields using the shared key that it shares with the initiator. For each intermediate node on the return path the nodes add their disclosed key that was used to create the MAC they appended to the MAC list as the request went towards the destination.Using the key list and the target MAC the initiator can verify the route and conclude that there were no forgeries of routing data.

B. Authenticated Routing for Ad hoc Networks

The Authenticated Routing for Ad hoc Networks (ARAN) protocol is based on the assumption that every node has a valid public key to a trusted key server. Also, this key server must prior to use in the network sign each node's public key after secure authentication of the node.Each certificate contains the node's IP address, the public key, the creation time, and an expiration time.The source node that wants to contact a destination node broadcasts a route discovery packet containing the destination IP, the source node's certificate, a sequence number, and a time stamp. All this information is also signed using the node's private key. Each intermediate node that receives such a message checks the signature and if valid signs the data using its own private key and attaching the certificate of the node. If a node already has attached its certificate the next node in the path removes the certificate, signs the remaining data, and finally concatenates its own certificate in place of the previous one. For each valid route request an intermediate node sets up a reverse path back to the node from which it received the request. When the request finally arrives at the destination it can validate the source. It can also choose from among different routes one which it seams most appropriate and unicast back a route reply, often the first route discovery packet is replied to .The chosen route may not be the shortest but the quickest. The route reply is signed by the destination node and the packet consists of the reply header, the IP address of the initial source node, the destination's certificate, the request sequence number, and the time stamp. The nodes along the path to the source verifies the previous hop node's signature and certificate, removes them and signs the data using its own private key and concatenates its certificate .During the communication links may fail due to movement or otherwise. In this case, when a node on the path discovers a down link it informs the initiator of this by sending out an error packet which it signs. The packet consists of the error header, IP addresses of both the source and the destination, its certificate, a sequence number, and a time stamp.The need for a trusted key server might also be a single point of failure for this.

C. Secure Ad Hoc On Demand Distance Vector Routing

The basic AODV protocol has built in capabilities for extension headers. The Secure Ad hoc Distance Vector (SAODV) protocol is a proposal by Zapata for such extension headers. The extensions are used to send signatures and hash values that are later used for verification of the routing packets. The SAODV is not meant to yield any confidentiality since this is usually not needed or desired in general ad hoc networks. The protocol does provide means to get authentication, integrity, and non-repudiation of the routing control packets.The protocol extensions use asymmetric cryptography to achieve authentication by signing the data packets with the private key. This allows for the destination node, and all intermediate nodes, to validate the request. Also, this allows for the nodes to be certain that no one has altered the packets. However, some fields of the packets must change and these are signed as if they were zeroed out.To allow for verification of the hop count field a one-way hash chain is utilised. The initiator of the route request decides a max hop count, such as ten or fifteen.It also generates a random value which is sent as the hash for the first hop count.The value is also hashed the max hop number of times producing a so called top hash. Each node can verify the hop count by checking that the incoming hash value hashed max hop count minus the current hop count number of times is equal

to the top hash. Since the top hash value is not changed, and thus signed, this provides the means to authenticate even the mutable hop count.The SAODV extensions allow for two different ways for nodes to reply to a route request. The destination node creates a route reply and signs it using its own secret key. The route reply is sent according to the usual AODV and each intermediate node can verify the reply and discard it if not valid. This approach does not consider the possibility of having intermediate nodes reply directly if they do have a valid route already.To add the ability for route discovery optimisation a double signature scheme is devised. For each route request a second signature is added to the packet. This signature is stored in each intermediate node when they set up the reverse route.Later on, when a new route is needed because of node movement between the two peers an intermediate node that still has a route can reply directly by also including the second signature and the original signature. In addition to this, the actual life time is also sent in the reply which is signed by the intermediate node that sends the reply .This method only allows malicious hosts to build a larger hop count or the same. That is, it is vulnerable to a partly replay attack which would let the hop count to be unchanged for one hop. This in turn could cause the route via the malicious node to be chosen as the shortest one. For this possibility to continue over time the adversary must be close to the actual shortest path and also move along while the intended peers move. Using more nodes in the attack would of course ease the attack at the cost of more attackers, which makes them easier to descry.

D.Secure Efficient Ad hoc Distance Vector Routing

The secure efficient ad hoc distance vector (SEAD) routing protocol is a security aware modification of DSDV. SEAD is proposed by Hu, Johnson, and Perrig .Most of the original operations of the DSDV are still used with some modifications.In addition, the distance vector updates are authenticated using an efficiently computable one-way hash function.SEAD uses one-way hash chains to authenticate the distance vector updates from each node. These values are used in a way that disables malicious nodes to forge distance vector values with lower distance than the correct one. They are, however, free to add a larger distance if they see fit. In these situations the route is discarded in favour of a shorter path.Each node creates a one-way hash chain that is later used for authentication of the node. The chain is split up into a number of parts each consisting of m subsequent entries. When a node sends out a distance vector update it adds the entry to itself with the distance metric equal to zero. Together with the routing table entries sent the hash value is also sent out. For each entry to other destinations it copies the current values it holds in the routing table and applies the hash function to the hash value it received for that entry. A node that receives the distance update can easily authenticate the correctness of the shortest route by checking the hash value against the authenticated hash value for that node. In addition, the source of each routing update message must be authenticated. This can be accomplished using TESLA or some other broadcast authentication algorithm available .

V. PROBLEM FORMULATION

Attacks on routing layer can be grossly classified into two categories, attacks on routing protocols and attacks on packet forwarding/delivery. Attacks on routing are designed to prevent a victim from knowing the path to a destination even if such a path exists in the network .Attacks on forwarding is to disrupt the packet delivery along a predetermined path. Even if we do have secured ad-hoc routing, attacks on Packet forwarding can still disrupt the packet delivery .These attacks can affect the route sequence number ,hop count ,source route. These attacks achieve two main goals: selfishness and denial-of-service. In a selfishness scenario, a malicious participant selectively drops data packets that it is supposed to forward in order to save its own resource. In a denial-of-service scenario, a malicious node can send excessive traffic through a victim node in order to deprive its battery power.

VI. OBJECTIVES

Secure routing could be divided into two complementary parts: secure route discovery and secure data forwarding. This thesis addresses the problems on secure packet forwarding .In ad hoc networks each node functions as a router and forwards packets for other nodes .Here, we study the impact of misbehaving nodes on packet forwarding. Most existing routing protocols designed for ad hoc networks typically assume a trusted and non-adversarial environment where each node is assumed to be cooperative and well-behaving. This assumption is not true in a hostile environment. The existence of misbehaving nodes may significantly disrupt the network operation and degrade the network performance. For example, if a misbehaving node on an active route drops data packets, then a large number of packets will be lost. Simulation results show that the average packet delivery ratio of DSR degrades by 30%, when 20% nodes are misbehaving nodes .The main objective of this research is to

investigate security issues in the context of Packet forwarding in mobile ad hoc networks, analyze the benefits and weaknesses of currently existing solutions, and find new and effective solutions for the purpose of secure data forwarding in mobile ad hoc networks.

VII. METODOLOGY USED IN THE WORK

To overcome the problem of packet forwarding there are features belong to two categories, non-traffic related and traffic related. The non-traffic related features capture the basic view of network topology and routing operations. In addition, "absolute velocity" characterizes the physical movement of a node.The traffic related features are collected based on the following considerations.Packets come from different layers and different sources. For example,it can be a TCP data packet or a route control message packet (for instance, a ROUTE REQUEST message used in AODV and DSR) that is being forwarded at the observed node. We can define the first two aspects or dimensions of a traffic feature as**, packet type**, which can be data specific and route specific (including different route messages used in AODV and DSR), and **flow direction**, which can take one of the following values, received (observed at destinations),sent (observed at sources), forwarded (observed at intermediate routers) or dropped (observed at routers where no route is available for the packet). We need to evaluate both short-term and long-term traffic patterns.Finally, for each traffic pattern, we choose two typical **statistics measures** widely used in literature, namely, the packet count and the standard deviation of inter-packet intervals. Overall, a traffic feature has the following dimensions: packet type, flow direction, sampling periods, and statistics measures. An example is the feature that computes the standard deviation of inter-packet intervals of received ROUTE REQUEST packets every 5 seconds.

VIII. CONCLUSION

The Mobile ad-hoc network(MANET) has very enterprising applications in today's world. But the security is main issue in the MANET .The security depends on the routing protocols and trusted key management .Reactive protocols are active research area in the field of ad-hoc mobile network. There are still lots of simulations to be done in this promising field.

IX. REFERENCES

[1]S.Madhavi,Dr.Tai Hoon Kim,"An intrusion detection system in mobile ad hoc networks",IJSA,Vol 2,No.3,July 2008.

[2]A.Rajaram,Dr.S.Palaniswami,"A high certificate authority scheme for autentication in mobile ad hoc networks "IJCSI,Vol7,No.5.July 2010.

[3]Pankaj Sharma,Yogendra Kumar Jain,"Trust based secure AODV in MANET",JGRCS,Vol3,No.6,June 2012.

[4]Wenjia li and Anupam Joshi,"Security issues in mobile ad hoc networks-a survey".

[5]Gulshan kumar,Mritunjay Rai,"An approach to provide security in mobile ad hoc networks using counter mode of encryption on MAC layer".

[6]R.Balakrishna,U.Rajeshwar Rao,"trust based routing security in MANETS "IJCSE,Vol.2,No.3,2010.

[7]Ashwani Garg,Vikas Beniwal,"A review on security issues of routing protocols in mobile ad hoc networks"IJARCSSE,Vol.2,No.9,Sep. 2012.

[8]Pravin Ghosekar ,Girish Katkar,"Mobile ad hoc networking:imperatives and challenges"IJCA,2010.