Providing of Secure Routing against Attacks in MANETs

A.Vani
Assistant professor
ECE Department
CBIT-Hyderabad, A.P

D.Sreenivasa Rao
Professor
ECE Department
JNTUH —Hyderabad,A.P.

ABSTRACT
A collection of wireless nodes which exchange various information among each other through wireless links as per the coverage boundary, directly or with the support of midway nodes as routers called infrastructure less in ADHOC networks. The Mac 802.11 wireless standard supports multiple data rates at the physical layer. Wireless network is dynamic because of frequent changes take place inside the topology due to mobility or energy loss. Accordingly any node can join or else leave the network in order to that changes in membership causes trust relationship among nodes is a big issue. During this circumstances security is the main concern in AD HOC networks. The existing protocols are inadequate to discover various types of threats. To overcome this problem designing a new routing protocol to provide solution for detecting and preventing nodes from security threats. Our proposed network security protocol includes with Intrusion detection system. It observe the network traffics and trying to investigate the misbehave activities like attackers, wormhole, anomalies, failure, channel blocked success plus other anonymous behavior in network and maintenance. We implement this algorithm using network simulator [ns-2].The performance of the protocol is measured using packet delivery ratio, Avg end- to- end delay, routing overhead and throughput

General Terms
Secure protocol, attacks, malicious and wireless nodes

Keywords
Ad hoc network, Blackhole, DOS, Flooding, Intruder, MIM, Security,

1. INTRODUCTION

Ad Hoc means tempory.Ad hoc network some times called as mobile ad hoc network. These networks are used for disaster condition like military, flooding etc. In theses nodes can can join and leave the network and acts as router/host or both at a same time Depending on their connectivity they can form arbitrary topologies with each other in the network and nodes have self configuration capability because of this they can be deployed without any infrastructure. Internet engineering task force (IETF) has MANET working, group (WG) that is devoted for developing IP routing protocols. Security is the main issue in MANETS. Different routing protocols have been developed for Ad hoc wireless networks, i.e., AODV, OLSR, DSR etc.

MANET can be defined as a distributed infrastructure less network [1] and mainly relies on individual security solutions from each mobile node and therefore centralized security control is hard to implement [2]. Securing an ad hoc wireless network is a big problem because of the conjunction of different several factors:

- **Vulnerabilities:** The absence of physical security causes as the ease of eavesdropping and spoofing takes place by intruders that leaves much gap between the security in standard wire line and standard wire line communication.
- **Lack of infrastructure:** MANETS cannot use any Security solutions comprising of dedicated secure components with predefined roles (such as trusted third party and key servers.
- **Requirement for cooperation**: Due to absence of dedicated components such as servers and routers. The set of ordinary nodes carry basic network functions and services in a distributed fashion. Thus, the secure routing is affected by the presence of intruders or malicious node or the absence of cooperation among the nodes.

Security in an adhoc wireless network is the most important concern for the basic functionality of network. The confidentiality availability of network services, availability and integrity of the data can be obtained by assuring that security issues have been met. Adhoc wireless networks often suffer from security threats or attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperation algorithms and no clear defense mechanism. These factors have changed the battle field situations for the adhoc wireless networks against the security threats. The adhoc wireless networks the nodes communicate with each other on the base of mutual trust without any a centralized administration. These characteristic makes adhoc wireless networks more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the adhoc wireless networks more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [3, 4]. Mobile nodes can overhear and even participate in the network because these nodes present within the range of wireless link .Adhoc wireless networks must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attacks on the wireless networks. Security is the cry of the day. In order to provide secure communications and transmissions, the engineers must understand different types of attacks and their effects on the ad hoc wireless networks. wormhole attack black hole attack, flooding attack, routing table overflow attack, denial of service (DOS), selfish node misbehaving, impersonality attack are kind of attacks that can adhoc wireless network can suffer from .And adhoc wireless network is more open to these kinds of attacks because communications is based on mutual trust between the nodes, there is no central point for networks management, no

authorization facility, vigorously changing topology and limited resource.

In adhoc wireless networks most challenging attacks to defend against is wormhole attack, black hole attack, denial of service attack and flooding attack. The worm hole and black hole attacks disclose the confidentiality security service and DOS, flooding attacks reduce the availability of the network service. The primary objectives of this paper is to propose protocol which will protect adhoc network security services like confendiality,availability ,authentication and nonrupudiation from wormhole attacks, black hole attacks, DOS and flooding attacks. These are the most divesting security attacks and to improve the network stability, confidentiality and availability on the network. These attacks are simulated using Adhoc-On demand distance vector (AODV) routing protocol. Finally, we develop a simple protocol to defend against the attacks for secure routing in adhoc wireless networks.

The remaining of the paper is organized as follows. The Related work is described in section 2. The issues and challenges in are described in section 3. Classification of attacks in section 4. Proposed solution section 5. Simulation environment and results are analyzed in section 6. The last conclusion is in 7.

2. RELATED WORK

MANET is very much popular and applicable due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much affected by the attacks [4, 5]. In MANETS Wireless links also causes more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [4, 3]. Different kinds of attacks have been analyzed in MANET and their effect can be measured on the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [6]. The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail

2.1 Wormhole attack

In any network, the sender wants its data to be sent as soon as possible in a secure and fast way, many attackers advertise themselves to have the shortest and high bandwidth available for the transmission such as in wormhole attack, and the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes. One of the most arising issues in MANET is the limited battery, attackers take an advantage of this flaw and tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep .

Several approaches have been developed to defend against wormhole attacks in mobile adhoc networks. In [7] packet leashes are used to protect reactive routing protocols against wormhole attacks. A leash is defined as any information appended to a packet to restrict the maximum transmission distance of the packet. Two kinds of leashes have been proposed: *geographical* and *temporal*. In the geographical leash, the sender appends its location and the sending time to a packet. Based on this information, the receiving node computes an upper bound on the distance to the sender. This solution in fact requires location information and coarse synchronization of all nodes in the network. In the temporal leash, the sender appends the sending time to the packet, and the receiving node computes a traveling distance of that packet assuming propagation at the speed of light, and using the difference between the packet sending time and packet receiving time. This solution requires fine-grained synchronization among all nodes. In [8] directional antennas are used to prevent against wormhole attacks. Each node in the network shares a secret key with every other node and broadcasts HELLO messages to discover its neighbors using directional antennas in each direction

The SECTOR protocol [9] presents a countermeasure against wormhole attacks by allowing nodes to prove their encounters with other nodes. However, several hypotheses are needed for this protocol to work correctly. Among these are the necessity for coarse synchronization, the ability of nodes to measure their local timing with nanosecond precision, the pre-establishment of security associations between each pair of nodes, and the presence of a central authority that controls the network membership. So-called disjoint-path-based approaches have been adopted recently.

In [10] introduce a simple delay analysis approach It calculates mean delay per hop of every possible route. To do so, a sender initiates a detection packet like RREQ, and receiver responds to every received detection packet. After collecting all response, the sender computes mean delay per hop of each route. Then, it arranges computed delays, and finds whether there is a large difference between two adjacent values. However, it does not use any confidentiality and authentication service, so attacker can disguise the sender easily. There are also some other methods proposed in the literature to defend against wormhole attacks. However, most of these methods require fine-grained time synchronization between nodes in the network or special hardware to prevent against the wormhole attack.

2.2 Black hole Attacks

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it There indeed have been numerous attempts published in the literature that aim at countering the Black attacks. We survey them in the following.

In [11, the authors discuss an approach in which the requesting node waits for the responses including the next hop details, from other neighboring nodes for a predetermined time value. After the timeout value, it first checks in the CRRT (Collect Route Reply Table) table, whether there is any repeated *next-hop-node* or not. If any repeated *next-hop-node* is present in the reply paths, it assumes the paths are correct or the chance of malicious paths is limited. The solution adds a delay and the process of finding repeated next hop is an additional overhead.

In [12], the authors discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source nodes get this information, it sends a RREQ to the next hop to verify that the target node (i.e.

the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a *FurtherRequest*, it sends a*FurtherReply* which includes the check result to the source node. Based on information in *FurtherReply*, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. Obviously, this increases the routing overhead and end-to-end delay. In addition, the intermediate node needs to send RREP message twice for a single route request.

In [13], the authors describe a protocol in which the source node verifies the authenticity of a node that initiates RREP by finding more than one route to the destination. When source node receives RREPs, if routes to destination shared hops, source node can recognize a safe route to destination puts some overhead in one or either/both intermediate and destination nodes in one or other way.

2.3 Denial of Service Attacks

A DOS attack [14] is any event that diminishes or eliminates a network's capacity to perform its expected function. These attacks are launched against server resources or network bandwidth by preventing authorized users from accessing resources. The effect of these attacks varies from temporarily blocking service availability to permanently distorting information in the network. Recently proposed incentive mechanisms for enforcing cooperation among nodes can be classified into trade-based and trust-based mechanisms. Trade-based mechanisms assume market models for providing virtual currency incentives for motivating cooperation among nodes. In the trust-based models, trust is created and the service provider is stimulated by these trust values. Each scheme can be deployed in different application scenarios. The trade-based models are not applicable in cooperative networks where no financial incentives are needed to run the network. However, trust-based schemes can still be used to improve network performance.

Existing incentive mechanisms for enforcing cooperation can be classified into trade-based [15, 16 17] and reputation-based [18, 19, 20,21the former uses a payment-based incentive, the latter uses mutual ratings based on services provided among the nodes.

While extensive work has been carried out on confidentiality, integrity, and privacy attacks [22], the threat to network availability has received less attention. Availability is an important requirement for improving network performance. Existing studies on DoS attacks concentrate on the analysis of various attack scenarios targeting a specific layer [23] or propose a probing mechanism to detect misbehaving nodes that target a specific network layer function [24] while using a probing mechanism can help in detecting DoS attacks, probing packets may introduce communication overhead in the larger network. Reputation rating coupled with localized probing mechanisms can alleviate this problem.

2.4 Flooding Attack

Many denial of service type of attacks are possible in the MANET and one of these type attacks is flooding attack in which malicious node sends the useless packets to consume the valuable network resources. Flooding attack is possible in all most all on demand routing protocol. Significant works have been done in securing the ad hoc network. Some researches defined the method for secure routing but secure routing also can not able to handle the flooding attack.

The first flooding attack prevention (FAP) method was proposed in [25] In their paper, first they described RREQ flooding and data flooding. This was the first paper that addressed the prevention of flooding attack in ad hoc network. The authors proposed the separate approach for RREQ flooding and data flooding. To resist the RREQ flooding, they defined the neighbor suppression method which prioritizes the node based on the number of RREQreceived. A node gets higher priority if it sends less numbers ofRREQ packets and defined the threshold value. To deal with data

Flooding they used path cutoff method. In this method when node identifies that sender is originating data flooding then it cutoff the path and sends the route error message. In this way attack is prevented up to some extent but the disadvantage of this method is flooding packet still exists in the network.

This limitation of FAP is eliminated by [26] presented threshold prevention. In this method they defined the fixed threshold value for every node in the network. If any node receives the RREQflooding packet more than the threshold value then the sender is assumed as a attacker and all the packets from attacker is discarded by the receiver node. This method eliminates the flooding packet but if the intruder has the idea about the threshold value then it can bypass the TP mechanism. Normal node with high mobility is treated as the malicious node.

In [27] the author proposed the distributive approach to resist the flooding attack. In this method they have used the two threshold value; RATE_LIMIT and BLACKLIST_LIMIT. If RREQ count of any node is less then RATE_LIMIT then the request is processed otherwise check whether it is less thenBLACKLIST_LIMIT, if yes then black list the node but if the count is greater than RREQ_LIMIT and less thanBLACKLIST_LIMIT then put the RREQ in the delay queue and process after queue time out occurs. These methods can Handel the network with high mobility.

In [28] the author analyzed the flooding attack in anonymous communication. They used the threshold tuple which consist of three components: transmission threshold, blacklist threshold and white listing threshold. if any node generates RREQ packet more than transmission threshold then its neighbor discards the packet if it crosses the transmission threshold more than blacklist threshold then it black list the node. But to deal with accidental blacklisting they defined white listing threshold. If any node performs good for number of intervals equal to white listing threshold then it again start treating as a normal node.

3. ISSUES AND CHALLENGES IN SECURITY PROVISOINING

Due to unique characteristics such as, shared radio channel, insecure operational environment, absence of central authority and association rules among nodes and limited availability of resources it is very difficult and challenging task to designing a fool pro of security protocol for ad hoc routing. A brief discussions on how each of the above mentioned characteristics causes difficulty in providing security in ad hoc wireless network is given below

- **Shared radio channel:** Unlike the wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc networks is broadcast in nature and shared by all nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So a malicious node can easily obtain data being transmitted in the network.
- **Insecure operational environment**: the operational environment in which MANET's are generally used may not be always securing, for example, a battle filed. In such environment, nodes may be moving in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.
- **Lack of central authority:** In wired networks or infrastructure based wireless networks it would be possible to monitor the network traffic through routers or base stations and implement security mechanism at those points. Since MANET's don't have any such central points, these mechanisms can't be applicable to them.
- **Lack of association rules**: In MANET, since nodes can join or leave the network at any point of time, if no proper authentication mechanism is used for associating nodes with the network intrudes can easily join the network and carry out attacks.
- **Limited availability of resources:** Resources such as bandwidth, battery power and computational power are limited in ad hoc networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

3 .1 Flaws in MANETs

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weakness of MANET's make it vulnerable to attacks and these are discussed below.

3.1.1 Non Secure Boundaries

MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. The links are compromised and are open to various link attacks. Attacks on the link interfere between the nodes and then invading the link, destroying the link after performing malicious behavior. There is no protection against attacks like firewalls or access control, which result the vulnerability of MANET to attacks. Spoofing of node's identity, data tempering, confidential information leakage and impersonating node are the results of such attacks when security is compromised.

3.1.2 Compromised Node:

Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous. Due to this autonomous feature for mobile nodes it is very difficult for the nodes to prevent malicious activity it is communicating with. Ad-Hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. It can be seen that these threats from compromised nodes inside the network is more dangerous than attacking threats from outside the network.

3.1.3 No Central Management:

MANET is a self-configurable network, which consists of Mobile nodes where the communication among these mobile nodes is done without a central control. Each and every node act as router and can forward and receive packets. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management. When there is a central entity taking care of the network by applying proper security, authentication which nodes can join and which can't. The node connect which each other on the basis of blind mutual trust on each other, a central entity can manage this by applying a filter on the nodes to find out the suspicious one, and let the other nodes know which node is suspicious.

3.1.4 Problem of Scalability:

In traditional networks, where the network is built and each machine is connected to the other machine with help of wire. The network topology and scale of the network, while designing it is defined and it do not change much during its life. In other words we can say that the scalability of the network is defined in the beginning phase of the designing of the network. The case is quite opposite in MANET's because the nodes are mobile and due to their mobility in MANET's the scale of the MANETs is changing. It is too hard to know and predict the numbers of nodes in the MANETs in the future. The nodes are free to move in and out of the Ad-Hoc network which makes the Ad-Hoc network very much scalable and shrinkable. Keeping this property of the MANET, the protocols and all the services that a MANET provides must be adaptable to such changes.

4. CLASSIFICATION OF ATTACKS

The attacks can be categorized on the basis of the source of the attacks i.e. internal or external and on the behavior of the attack i.e. passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or as well as active or passive attack against the network.

4.1 External and Internal Attack

External attackers are mainly outside the networks who get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network.

These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks.

4.2 Active and Passive Attacks

In active attack the attacker disrupt the performance of the network, steal important information and try to destroy the data during the exchange in the network. Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is east for the node to exploit and hijack any internal node to use it is introduce bogus packets injection or denial of service. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network. In Passive attack, the attacker listen to network in order to get information, what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

4.3 Security threats

4.3.1 Security flaws and attacks on routing protocol service

The mobile ad hoc networks allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix infrastructure in such a network. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other had, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that execute active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. In this paper, our focus is on vulnerabilities and exposures in the current as hoc network. We have classified the attacks as modification, impersonation, fabrication, wormhole and lack of cooperation.

In fact we consider AODV as the default routing protocol as it is presently going to be the acceptable standard for ad hoc network. So, we will highlight the major attacks on AODV or major flaws of this protocol. It is to be noted that it is not hard to transform similar type of attacks on other protocols, DSR for example known attacks on AODV are as follows:

4.3.2 Wormhole Attack

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are Tunnelled.This tunnel between two colluding attacks is known as a wormhole .In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

4.3.3 Black hole Attack

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. [9] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

4.3.4 Denial of service attack

Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc Network.

4.3.5Flooding Attack

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 adhoc 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 cost.

4.3.6 Man-in-the-middle attack

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

5. PROPOSED SOLUTION

For the developing a common Intrusion detection security protocol ultimate aim is to provide more security among wireless network nodes. The wormhole node or attacker can present in any manner, our protocol capable to detect those unauthorized activities and can eliminate such kind of nodes or activities. Likewise this protocol can distinguish dissimilar attacks cause minimize the losses and damages. Here Intrusion detection takes part in four methods.

1. Observation level: Herein this phase actions of the destination is represented as per the pre allocation of network and it decided by the source node.

2. Preparation level: standard performance topology studied and corresponding model built. This can be equipped using various methods to set up a network in this paper

3. Detection level : Once the network created as per the parameter specified by this paper the protocol starts to monitor the traffic, depends on the threshold deviation, it can be more or less, according to the variation in network the wormhole node detect by using Hybrid Intrusion detection security protocol.

4. Isolation level: After detection process completed using hybrid technology such kind of misbehavior nodes or packets should eliminate from the entire network action. This paper presents overall solution against presence of attacks in ADHOC network.

IDS Detection procedures:

ALGORITHM

1. Fix data_rate_thresh to monitor the traffic. When RREQ broadcast to its neighbour's data_rate_thresh also includes along with it. Then observe gap between each packet. This technique used to eliminate excess of control packets.

2. This could happen with the objective of create congestion in physical layer which can produce more number of packet so that the channel can be blocked for further transmission. If there are no any massive changes in data rate then there is no any worm hole.

3. If it is a attacker it will transmit huge number of packets.

4Attacker send false connection request frequently.

Apply sorting method

a-scheme. record first sync packet of each connection

If any new packet comes

B. if sync packet completed 3 –way handshaking pass the packet

We pass the packet with a certain probability.

To record the other SYNC packets. connection is new, and then we drop this SYN packet

5. Send joins req to distributed server

Recv join req from new node by server

Send membership msg to node

Nodes send an ack msg to server

while recv ack msg server generates hash_key and send to nodes

recvr nodes storeits hash key

While data transmits src node send req to dst and server for hash key

if blackhole node presents it sends malicious key or wrong key to source

else

normal destination send its hash key to src node

if(hash key from server == hash key from destination)

no bh

else

routereply sender is bh node

6. RREQ packet contains as we saw already, destination address and sequence number and at present with data_rate_thresh along with source address. Sequence number provides the freshness of route. Fix theshold value for sequence number.

tx rreq (da_address, sequence number, data_rate_thresh)

fix seq_thresh

7. Once the destination node receives RREQ message from neighboring nodes, initially it will verify data_rate_thresh

If (rx_ctrl_pkt rate is > data_rate_thresh)

then (check gap between each packet)

if (rx_ctrl_pkt time , next_pkt_time)

pkt_count++

if (count is more)

{

wormhole node sends more number of packets

}

8. At the time of receive RREQ ensure senders sequence number also and compare it with its own sequence number. If the difference between both sequence numbers is more can declare RREQ received from wormhole node

If (SA seq_no > seq_thresh DA seq_no)

{

Due to more difference in sequence no sender is a wormhole node

}

9. Then unicasts the RREP (route_reply) back to the source node.

10. Each Node sends Hello message to its entire neighbor periodically to ensure the neighbors presence. Transmit hello message along with its transmission power.

11. During the time of send hello message fix pwr_thresh value for hello message

12. Then check pwr_thresh while receiving hello message. If power is greater than the threshold

Sender may be a wormhole node. Before declaring the state transmits another packet and start timer. Within the time period it receives hello message within the limit of threshold value declare it is a normal node. If the reverse response received from sender confirm it is a wormhole node

If (rx pwr_thresh > tx_ pwr_thresh}

{

Sender maybe a wormhole node

}

tx_next_hello_msg and wait for reply

if (rx_pwr is <= pwr_thresh)

{

declare normal node

}

else

{

confirm sender as wormhole node

}

13. Then classify sum of queue_delay between hops and end_end_delay. When it sends hello message include max_delay time and start the timer. When it reaches the destination measure the queuing delay as the duration of time left from the start time of the packet. By the way each node maintains average queue_delay.

14. If it reaches the destination within very short period there may be a wormhole node. Since the number of hops may be less due the character of wormhole, so it can broadcast a message during less duration, so that the receiving node can be a focus for the short queuing_delay . Whereas the normal node contains the real hop count with average queuing delay.

If

Define queue_delay_ thresh

Rx_pkt for forwarding

Update queue_delay and forward pkt

Rx node update queue_delay

? queue_delay+hop_count

If path queue_delay > queue_delay

Declare no wormhole

Else

Wormhole node

15. Man in the middle attack:

Like black hole node, mim attacker generates route reply to corresponding route request packet, and also it find path to destination, it capture the packet and change the data contents. And forwards to destination nodes

16. With the difference of seqno and thr_value and contents of malicious data the mim attacker will be detected by trusted nodes

If (SA seq_no > seq_thresh DA seq_no)

{

Due to more difference in sequence no sender is a malicious node

}

if (data_contents are not valid)

{

Immediate node is malicious node.

}

17. Intruder detection and isolation enabled when the routing protocol sense the wormhole node. Misbehave; suspicious nodes

can be detected using our protocol and information distributed to the topology.

18. Though good quality node marked as wormhole node, to reduce the false detection, after the wormhole node discovery, apply the monitoring process continuously for certain period of time.

19. All nodes maintain a log of recently forwarded Traffic

Upon receiving the query, a device consults its traffic log

If seen, will implement a filter blocking further attack activity for a short period. They then forward the same attack query to their immediate neighbors.

We observe the performance of the complete network and the maximum nodes are protected by our new routing Security protocol.

20. The aspect of security in ADOC network a lot different attacks and wormhole detection have been investigated and simulated using network simulator

In this manner, the attack is quickly traced back to its true origin, with filters in place at each device along its path, preventing attack completion. To improve this problem, the network components also forward their reports and activity to a centralized Discovery Coordinator (DC). The IDS operates on a global level, include information from multiple IDS reports and sources.

6. SIMULATION RESULTS

6.1 The simulation parameters

parameter	value
Simulator	NS-2[ver 2.32]
Simulation time	600s
No. of nodes	20-100
Routing protocol	AODV
Traffic model	CBR
Pause time	20-100s
Terrain area	1200m x1200m
Transmission range	250m
No. of malicious nodes	2-6
Node mobility	1-5 mtrs

6.2 Simulation screenshots

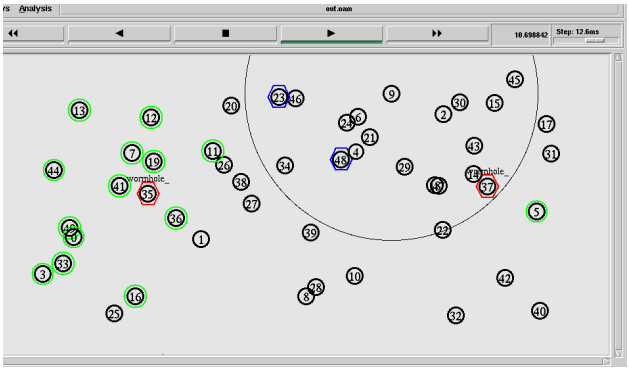


Fig 1.Sending of RREQ

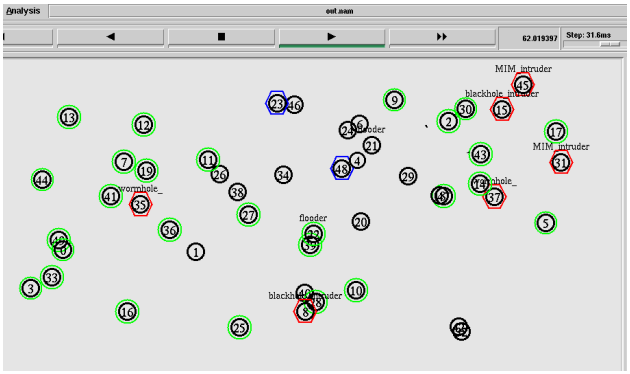


Fig 2.Different attack scenario

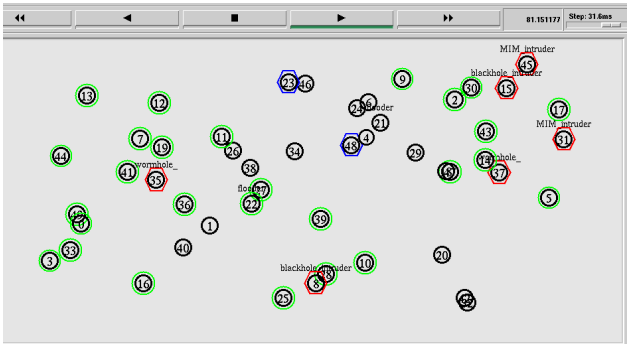
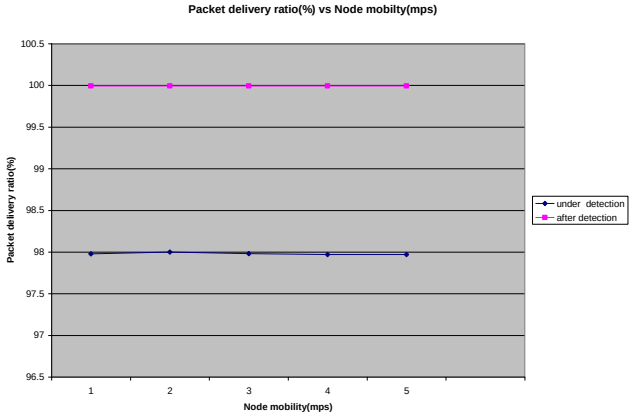
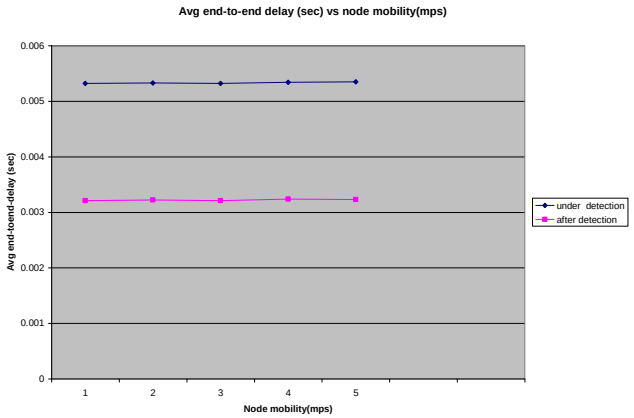
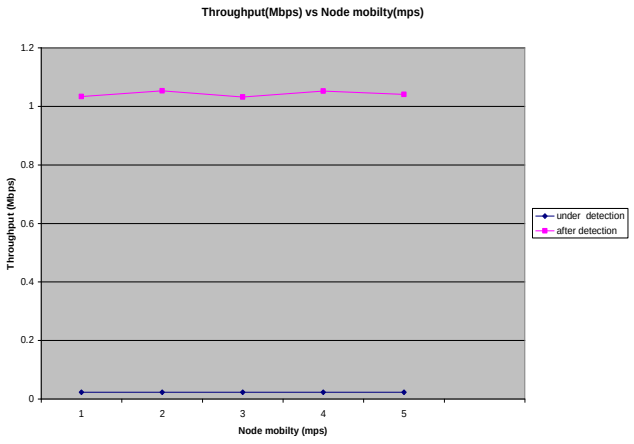


Fig 3.Different attack moving scenario

6.3 Simulation results







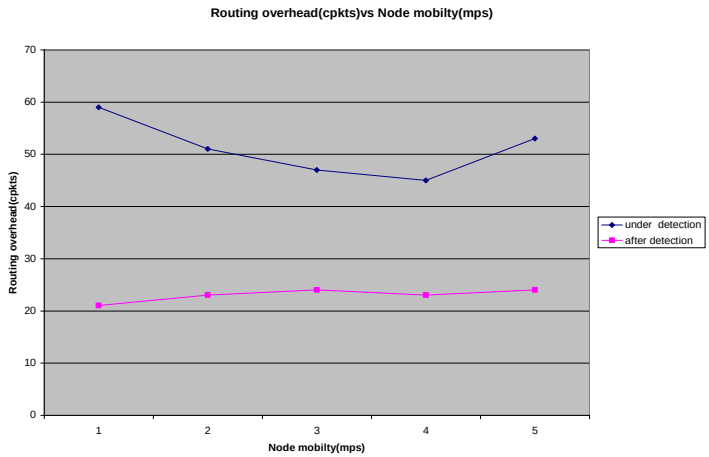


Fig 3 Impact of node mobility (m/s) on PDR (%), Avg end-to-end delay (sec), Throughput (Mbps), Routing overhead

From the results we can measure the performance of the secure routing protocol. We are taking different metrics and these are measured under detection of the attack and after detection. In paper we have shown the results in terms of node mobility. As the node mobility is increases the routing overhead and increases and little delay compared to after removal. Packet delivery ratio and throughput increases after elimination of the attacks. Fig 6 Node mobility vs packet delivery ratio

7. CONSLUSION

In this paper, we have analyzed the security attacks in an ad-hoc Network faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of routing security on the other hand, adhoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust secure routing protocol to adapt to the demanding requirements of these networks. The research on MANET security is still in its little stage. The existing proposals are typically attack-oriented in that they first identify several security attacks and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many both known and unknown security threats. In paper we developed secure routing protocol that detect and eliminate different security attacks. This protocol is efficient, scable, costeffective and less cost. By using this protocol we eliminate different attacks which affect on security services

8. REFERENCES

[1] S. Corson and J. Macker, "Mobile ad hoc networking (manet): Routing protocol performance issues a evaluation considerations," *RFC 2501*,Jan. 1999.

[2] S Buchegger & J-Y Le Boudec, "Nodes Bearing Grudges: Towards Security, Fairness and Robustness in Mobile Ad hoc Networks," *In Proc.10th IEEE Euro micro Workshop on Parallel, Distributed and Network*

[3] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[4] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[5] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security, S. Huang, D. MacCallum, and D. -Z. Du (eds.), Springer, 2008.Institute of Technology Hoboken, New Jersey, USA, 8th December 2002

[6] S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".

[7] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wire- less networks," in Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1976-1986, 2003

[8] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proceedings of the Network and Distributed System Security Symposium (NDSS), pp. 131-141, 2004

[9] S. Capkun, L. Buttyan, and J. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wire- less networks," in Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21- 32, 2003

[10] H. S. Chiu and K. S. Lui. Delphi: wormhole detection mechanism for ad hoc wireless networks. 1st International Symposium on Wireless Pervasive Computing, pages 6–11, January 2006.

[11] LathaTamilselvan, Dr.V.Sankarayanan, "Prevention of Black hole Attack in MANET". The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless2007) India, 2007 IEEE

[12] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Black hole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov 2007.

[13] A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks." In: Proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr. 2004.

[14] A.D. wood and J.A. Stankovic, "Denial of Service in Sensor Networks," IEEE October 2002.

[15] L. Buttyan and J. Hubaux, "Stimulating cooperation in self organizing mobile ad hoc networks," ACM/Kluwer Mobile Networks and Applications (MONET) 8 (2003).

[16] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V.Vijayaraghavan, "Participation incentives for ad hoc Networks," http://www.stanford.edu/~yl31/adhoc (2001).

[17] Zhong, J. Chen and Y.R. Yang, "Sprite: A simple, cheatproof, cedit-based system for mobile ad-hoc networks," Technical Report 1235, Department of Computer Science, Yale University (2002).

[18 D. Barreto, Y. Liu, J. Pan and F. Wang, "Reputation-based Participation enforcement for adhoc networks," http://www.stanford.edu/~yl314/adhoc (2002).

[19]. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In: Mobile Computing and Networking. (2000) 255–265.

[20] S. Buchegger and J.Y.L Boudec, "Performance Analysis of The CONFIDANT Protocol: Cooperation of Noes — Fairness In Distributed Ad-hoc Networks," In Proc. Of IEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, IEEE (2002) 226–236.

[21] P. Michiardi and R. Molva, "Making greed work in mobile Ad hoc networks," Technical report, Institut Eur´ecom (2002).

[22] I. Aad, J.P, Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks", ACM MOBICOM 2004, Philadelphia, PA, USA.

[23] V. Gupta, S. Krishnamurthy, and M. Faloutsos, Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks. In Proc. of MILCOM, 2002.

[24] M. Just, E. Kranakis, and T. Wan, "Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks", In Proc. of ADHOCNOW'03, Montreal, Canada.

[25] YL Sun et al., "Information Theoretic Framework of Trust Modeling and Evaluation for ad hoc networks" IEEE JSAC, vol.24, no.2, Feb 2006.

[26] Guerrero Zapata, "Secure ad hoc on-demand distance vector routing, ACM SIGMOBILE Mobile Computing and Communications "Review, v.6 n3, July 2002 [doi>10, 1145/581291.581312]

[27] Papadiminitratos and Zygmunt J.Hass,"Secure data Communication in Mobile ad hoc Networks"IEEE JSAC, vol.24, No.2, February 2006.

[28] Papadimiatos and Zygmunt J.Haas and Samar."The Secure Routing Protocol (SRP) for ad hoc Networks.draft-papadimitratos-secure-routing-protocol"00.txt, Dec.2002