SECURITY ISSUES IN MOBILE AD HOC

V. Madhu Viswanatham, Varun Sharma & Sumit Bhatnagar
School of Computing Sciences,
VIT University,Vellore-632014,TN,INDIA.
vmadhuviswanatham@vit.ac.in

Abstract

Mobile ad hoc networks are autonomous, wireless networks those do not depend on any fixed infrastructure unlike traditional mobile wireless networks. Connectivity management is taken care of by host only, which are interconnected through wireless interfaces. They lack specialized nodes like routers to perform packet forwarding instead every node in the network functions as a router as well as an application node. This paper analyses the characteristics and applications of ad hoc networks in brief and related security issues in detail.

Keywords

Mobile Ad hoc networks, Mobile computing, 802.11, Certification Authority, Mobile Certification Authority

1. Introduction

Ad hoc networks originated in early 1970s. In 1972 DoD sponsored Packet Radio Network which evolved into Survivable Adaptive Radio Networks program in the early 1980s. These programs were focused on providing packet switched networks to mobile battlefield entities like soldiers, aircrafts, tanks, etc. The military tactical and other security-sensitive areas still from the major fields where these networks find their applications of personal devices such as PDAs, cellular phones, laptops etc. is evident, but still many challenges are present in this direction.

- The ad hoc network is a non-infrastructure architecture; in which nodes can access services from one another regardless where they are. In ad hoc all the nodes are responsible for network formation (self-organizing) and management (self-administrating).

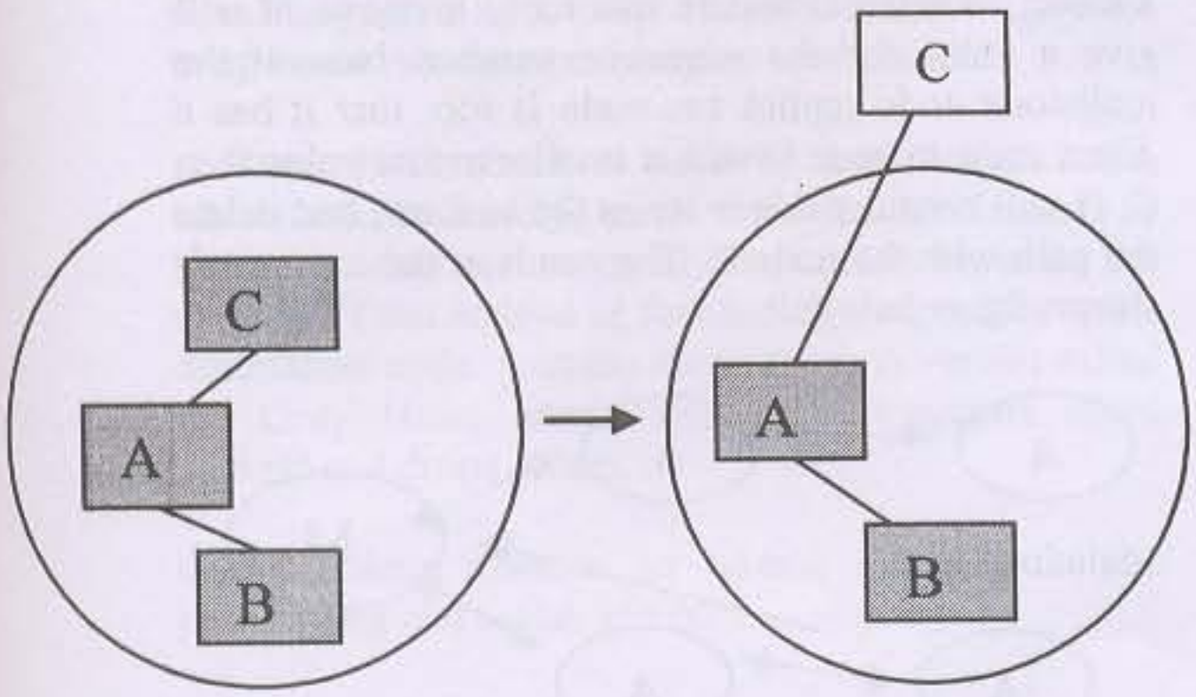

Fig: Topology change in ad hoc networks.

Most of past research protocols, leaving the security aspects unexplored. New applications for ad hoc networking like ubiquitous computing wire free sensor networks, personal per-to-peer networks has introduced a need for robust privacy protection and security mechanisms.

Security goals of ad hoc networks are identical to those of any other communications system and require the following criteria to be met.

- Availability: Survivability despite Denial of service (DOS) attacks.
- Confidentiality: Non disclosure of certain information to unauthorized entities.
- Integrity: Ensuring that message being transmitted is never corrupt.
- Authentication: Ability of node to ensure the identity of the peer node it is communicating with.
- Non-repudiation: Ensuring that the origin of a message cannot deny having sent the message.

MANET are exposed to various kinds of attacks due to following vulnerabilities.

- Vulnerabilities of channels: Ad hoc networks on account of being wireless are easier to eavesdrop; information can be distroied by injecting fake packets into the network, without having a physical access to network components at all.
- Lack of infrastructure: This makes the classical security mechanisms based on certification authorities and online servers non prolific.

Use of intangible wireless links renders an Ad hoc network more susceptible to link attacks that range from passive eavesdropping (violating confidentiality) , to active attacks like impersonation of a node, message replay, message deletion, and message distortion.

In general to ensure survivability Ad hoc networks require a distributed decentralized architecture. Trust relationships between nodes should be changed from time to time and security mechanism needs to be dynamic and scalable. In this paper our concern is about routing_system attacks, attacks from compromised nodes and appropriate counter measures. Data confidentiality ensuring mechanisms like authentication and key management and intrusion detection.

2. Routing

Routing protocols are required to establish routes between nodes communicating within a MANET conventional routing protocols based on distance vector or link state methods are not adequate here.

This is because of various factors like (i) Limited transmission range; multiple network hops enable data communication between two nodes in the network. (ii) Lack of infrastructure; nodes act host as well as routers. (iii) Frequent topological changes etc. Thus routing protocols for MANETs are designed to be bandwidth efficient and less consideration is given to security aspects.

The existing routing protocols can be classified as:

- PROACTIVE
- DSDV: DynamicDestination-Sequenced Distance-Vector routing algorithm.

Based on Bellman-Ford routing algorithm. Every mobile station maintains and uses for routing packets, a routing table, listing all available destinations, the number of hops to reach the destination and the sequence number assigned by destination and the sequence number distinguished old routes from new ones. Stations periodically and on significant changes transmit their routing tables to their neighbors.

GSR: Global State Routing

Based on link state routing but avoids flooding of routing messages. Each node maintains Neighbor list, a Topology table, a Next hop table and a Distance table. The routing messages are generated on a link change and the node updates its topology table if the sequence number of the message is newer than the number stored in the table.

FSR : Fisheye State Routing

In FSR each update message contains information about closest nodes frequently and farther nodes as required i.e. details and accuracy of information decreases as the distance from node increases.

OLSR: Optimized Link State Routing

In OLSR each node selects a set of its neighbor nodes as "multipoint relays". These nodes announce to the nodes that have selected them as MPR. This technique reduces the size of control messages as well as minimizes flooding of control traffic.

- REACTIVE [Lazy approach]

AODL: Ad hoc On Demand Distance Vector Routing.

This algorithm enables dynamic, self-starting multi hop routing between nodes. This method does not require nodes to maintain routes to destinations that are out of active communication.

TORA: Temporary-Ordered Routing Algorithm

It is an adaptive routing protocol for multihop networks and has following features.

- Distributed execution,
- Loop free and multipath routing,
- Reactive or proactive root establishment,
- Localization of algorithmic reactions to topological changes.

ZRP: Zone Routing Protocol

It combines the advantages of the proactive (for nodes within zone) and reactive (for nodes outside) approaches.

3. Security Attacks [Routing Based]

Routing scheme based attacks on Ad hoc networks are based on one of the following methods.

Modification: In the attacks using modification the malicious node announces false routes as better routers than the other nodes in order to either redirect data to itself or to any other particular node. This is done by changing the route sequence number, modified hop count and denial of service attacks. DOS (Denial Or Service Attack) is implemented by changing the packet headers in such a way that they don't reach the destination.

1. Redirection by changing the route sequence number

Router sequence number is a metric based on which the nodes determine the shortest path. Algorithms discussed above are used to ascertain this number. Smaller this value is, better is the route. That's why a simple way to attack a network is to change this value with a smaller number than the last "better" value. Consider fig below.

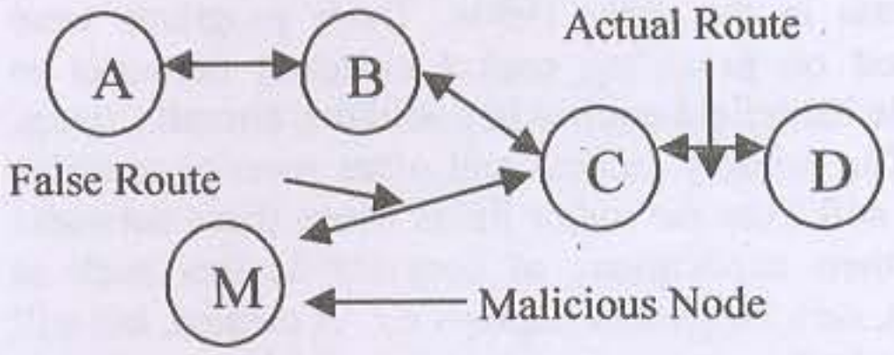

Fig Attack based on Modification of route

In this case a malicious node tries to insert itself into the network in order to disturb its operation. When node A wants to communicate with node D, it broadcasts a message asking all the nodes around the better path to reach the node D. B will received the message and forward it. Node C will replay that it has a direct route to D and in this reply message; it will give a value for the sequence number. Now if the malicious node replies to node B too, that it has a direct route to node D with a smaller metric value than C, B will consider this route as the best one and delete the path with the node C. The result in the example is shown figure below.

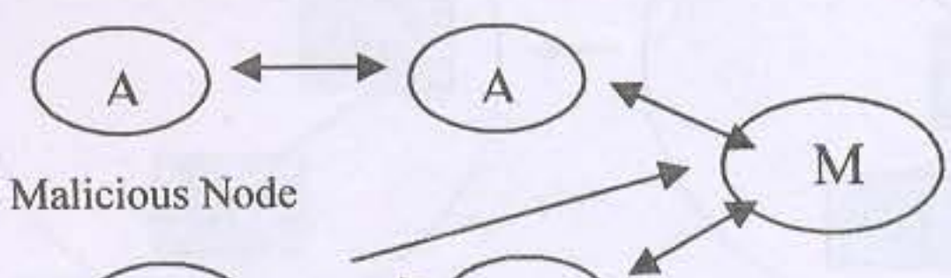

Fig : Result of Modification of rote based attack

Redirection with modified hop count.
When a node cannot decide what the best route is regarding to different route sequence numbers , it can use the number of hops to decide which path is the best route to reach a specific node. This is the case in the AODV protocol. , which uses the hop count value to determine the best route. Malicious nodes can disturb the network by announcing the smallest hop count value to reach the node. In general , hackers use the value zero to be sure to have the smallest hop count value.

Denial Of Services (DOS) attacks .
The DOS attack is well-known in computer security and can be efficient in ad-hoc networks without secure routing protocols. The operation of DOS attacks is evident figure here; a malicious node is located in the network. If node A wants to communicate with node E, it sends data packets according to its route cache to the node E including the malicious node. Further when the malicious node receives the data packets, it changes the header of these packets in order to abort the transmission of the data.

Impression: In the attacks using impersonation the malicious node emulates the identity of another node by spooling its MAC address. These attacks come in the category of spooling, since the malicious node hides its real IP address or MAC address and uses another one. As current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. For example, a hacker can create loops in the network to isolate a node from the remainder of the network. To do this, the hacker just has to take IP address of other node in the network and then use that to announce new route (with smallest metric) to the other nodes. By doing this, he can easily modify the network topology as he wants.

Fabrication: In attacks based on fabrication the malicious node generates traffic to disturb the proper operation of the ad-hoc network. Disruptions like falsifying route error messages, corrupting route state, route table overflow attack, black hole attack and replay attack are common. Non optimal paths called Routing Loops are used by attackers to make data travel through a node more than once; this may result in unwanted resource exhaustion by the node.

A Black Hole attack is used by a malicious node, which makes all traffic travel through it by claiming to be on the shortest routes of all possible roots on the network. Then instead of forwarding the packets to the destination node it simply drops them. A variant called the Gray Hole; attack selectively transmits some packets and drops others.

Other attacks towards an ad-hoc network include partitioning and replay attack.

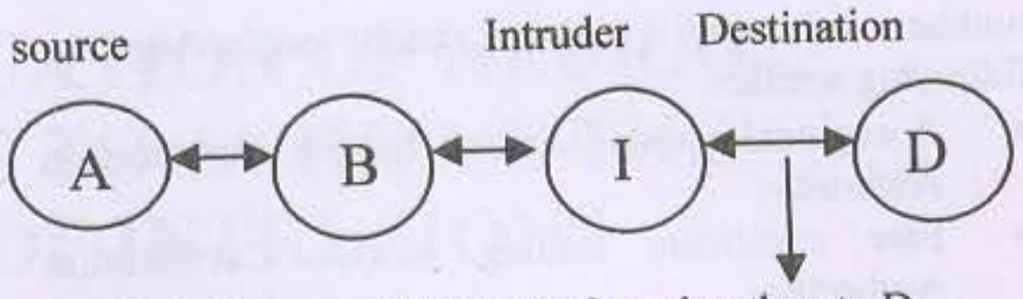

Fig: Operation of black hole attack

The network traffic is analyzed by the attacker to single out any node connecting independent parts of the network. Further network is split into two halves two create useless islands of nodes.

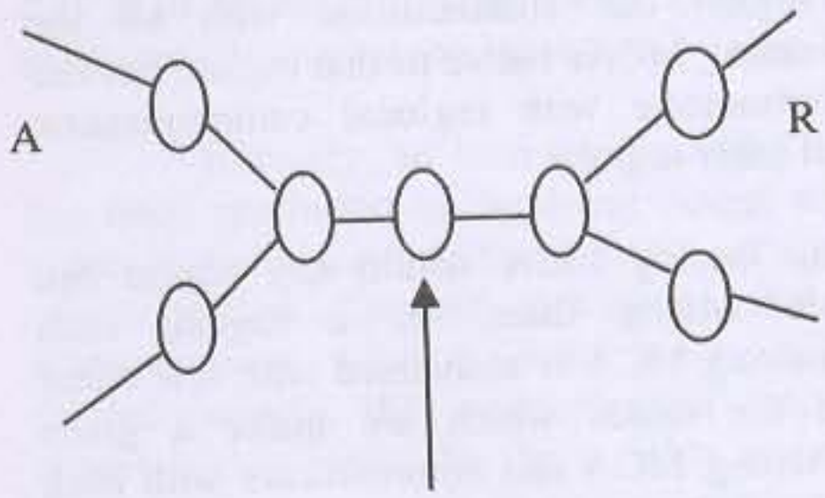

Fig: Attacker node splits the network into two disconnected zones A and B

Key Management:

Cryptographic schemes like digital signatures, encryption algorithms, digital digests etc are used to protect data as well as the routing information. Public key algorithms being robust and safe are widely used. In public key infrastructure each node has a public key public/private key pair. Public keys are known to everyone, while private keys are kept to nodes themselves confidentially. Further to ensure greater security trusted third parties called Certification Authority Fig do key management. CA has a public/private key pair, with its public key known to every node and signs certificates binding public keys to nodes. The CA has to stay online to reflect the current bindings, since they can change with time. Public key should be revoked if the owner node is no longer trusted or is out of network

Centralized, single key management service does not suffice for an ad-hoc network and even becomes a weak link in the overall security of whole system. If the CA goes down nodes cannot get current public keys of other nodes to establish secure connections. This defeats the whole purpose of the CA. one simple and robust solution is to decentralize the CA system and distribute the trust to a set of nodes by letting these nodes share the key management responsibility. 'Hierarchical Mobile Certification Authority' is one such system discussed.

4. Hierarhical Mobile Certification Authority

In Hierarchical Mobile Certification Authority (MCA) based networks, a big network is divided into a

number of small regions, each onehaving the following entities.

- A regional communication Mobile Certification Authority.
- Few certificate issuing mobile Certification Authorities.
- A number of client nodes.

Physically most secure and computationally most powerful nods are chosen as MCAs. Effort is made not to disturb the heterogeneity of network and it appears seam less.

In this model regional communication MCA of a particular region can communicate with all the certificate issuing MCAs native to that region. Further it can communicate with regional communication MCAs of all other regions.

A certificate issuing MCA within any region can communicate among them. In a region, each certificate issuing MCA is associated with few client nodes, and the nodes which are under a given certificate issuing MCA can communicate with each other. A certificate issuing MCA contains all the information about the client nodes that are under its control.

A new node on requiring a certificate sends request to the entire certificate issuing MCAs that it is in direct communication with. Using threshold Cryptography, a certificate is issued and a node is added to the region if the number of MCAs that agree to issue a certificate equals or exceeds the threshold k. of that region. When certificate renewal is required by the client node it sends the requests for renewing the certificate to all the certificate issuing MCAs in immediate communication, here also Threshold value is checked before renewing the certificate.

When a client node becomes malicious certificate needs revocation. Certificate issuing MCAs scan for malicious nodes every few seconds and on finding some revoke their certificate and send the information to all certificate issuing MCAs and client nodes, which reacting delete the culprit node from the database.

Frequent movements of nodes of an ad hoc network create a lot of complications and HMCA needs to incorporate many features to accommodate these. For instance when a client ode moves to another region, therefore the certificate issuing MCA communicated to the regional communication MCA, which further this information to all regional communication MCAs. Thus the network reconfigures itself.

On death of a node in its own region all the MCAs delete it from their tables but if MCA of one region moves to another region or dies, then before moving it has to transfer all its information to the node which is selected as a new MCA according to a voting procedure. Similar is the case with RMCAs.

Voting involves all MCAs/RMCAs broadcasting their features like; computational strength, memory capacity, proximity to client nodes, security parameters etc. Naturally best one is selected.

Conclusions

In this paper we visualized security in Ad Hoc networks from various perspectives .i.e. attacks on routing system, authentication schemes and information safeguarding using seceret keys and various other encryption algorithms. Identification of alternative approaches to remove inherent weakness from current algorithms is key work of this paper. If considered at an professional level, and refined by professional researches these may be converted in to profile products.

References

1. Ram Ramanathan & Jason Redi(May 2002),"*A brief overview of ad hoc networks challenges & directions.*" IEEE communication magnizine ,pp 20-22.

2. Richard Dawkins, *The selfish Gene.* Oxford University press,1980 edition.

3.V Rajaraman (April/June 2005),"Building blocks of e-commerce."Sadhna Vol 30, Parts 2&3 ,pp.89-117

4. Tracy Camp, J.Boleng,Vanessa Davies(Sep 2002)," *A survey of mobility models for ad hoc network research.*"WCMC: Special issue on mobile Ad Hoc Networking. Research trends and applications vol2,pp 483-502,2002.

5.. Maarit Hietalahti."*Key Establishment in Ad Hoc Networks.*"Helsinki University of Technology.