Security Concepts Underlying MANET

Dr. Deepak Chahal, Dr. Latika Kharb
Associate Professor (IT), JIMS, New Delhi, India.

Abstract – Ad-hoc networking is a concept in computer communications, which means that users wanting to communicate with each other form a temporary network, without any form of centralized administration. Each node participating in the network acts both as host and a router and must therefore is willing to forward packets for other nodes. For this purpose, a routing protocol is needed. An ad-hoc network has certain characteristics, which imposes new demands on the routing protocol. In this paper, we have discussed about ad hoc networks and their types along with routing and forwarding mechanism in ad hoc network. Recent advancement of wireless technologies like Bluetooth, IEEE 802.11 introduced a new type of wireless system known as Mobile ad-hoc network (MANETs), which operate in the absence of central access point. It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time.

Index Terms – MANET, Security, Attacks, Protocol.

1. INTRODUCTION

In MANETs each node operates in a distributed peer to-peer modes, serves as an independent router to forward message sent by other nodes. MANETs has shows distinct characteristics, such as weaker in security, device size limitation, battery life, dynamic topology, bandwidth and slower data transfer rate. Apart from these limitation MANETs has many extensive application like: Military application, Natural disaster, Medical service. In ad hoc network there can be node that will try to disrupt the proper functioning network. These nodes can be malicious or selfish. They try to disrupt network function by modifying packets, injecting packets or creating routing loops. So, security is an important task, because MANETs has characteristics such as; dynamic topology, infrastructure less. There are large numbers of secure routing protocols proposed by many researchers they fulfill different security requirements and prevent specific attacks. They are divided into three categories: Reactive routing protocol, Proactive routing protocol and hybrid routing protocol. In reactive routing protocol the route is discovered when it required, in proactive each node maintain network information regarding to network connectivity and route information to all others node within the network and proactive is one which is neither reactive nor proactive. Now, the most of the solution uses cryptography mechanism to detect selfish, malicious behavior of nodes and securing information from other types of attacks. The mechanisms which are used by different secure routing protocol to detect malicious and selfish node have address separately in different protocol. No secure mechanism has been proposed till date that can address to detecting malicious and selfish node collectively. We proposed a mechanism, Extended Public key Cryptography (EPKCH) that able to detect the malicious nodes and selfish nodes collectively in order to achieving security goals such as; Authentication, Integrity, Confidentiality and Non-Repudiation. Also, we proposed a routing protocol named Authenticate and Secure Routing protocol for mobile Ad hoc Network (ASRP). We implemented EPKCH mechanism in monitor mode of ASRP to securing MANETs. To design of this protocol follows the table-driven approach, in which each node maintain the information, regarding to network structure and route from a particular source to its all possible destination in its node info table. ASRP is a proactive secure routing protocol.

The specific features of MANETs present a challenge for security solutions. Many existing security solutions for conventional networks are ineffective and inefficient for many envisaged MANET deployment environments. Consequently, researchers have been working for the last decade on developing new security solutions or changing current ones to be applicable to MANETs. Since many routing protocols do not consider security, some research focuses on developing secure routing protocols or introducing security extensions to the existing routing protocols. Routing protocols have been proposed to counter selfish activities by forcing the selfish nodes to cooperate. Existing key management mechanisms are usually based on central points where services such as certification authorities or key servers can be placed. Since MANETs do not have such points, new key management mechanisms have had to be developed to fulfil requirements. Finally, since prevention techniques are invariably limited in effectiveness, intrusion detection systems are generally used to complement other security mechanisms. This applies to MANETs too and researchers have proposed new IDSs to detect malicious activities on these networks. If we are to develop more general solutions we must first have a comprehensive understanding of possible vulnerabilities and security risks against MANETs. They share the vulnerabilities of wired networks, such as eavesdropping, denial of service, spoofing and the like, which are accentuated by the ad hoc context [109]. They also have further vulnerabilities such as those that take advantage of the cooperative nature of routing Algorithms.

2. SECURITY IN MANET

With the proliferation of cheaper, smaller, and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the fastest growing areas of research. This new type of self-organizing network combines wireless communication with a high degree node mobility. Unlike conventional wired networks they have no fixed infrastructure (base stations, centralized management points and the like). The union of nodes forms an arbitrary topology. This flexibility makes them attractive for many applications such as military applications, where the network topology may change rapidly to reflect a force's operational movements, and disaster recovery operations, where the existing/fixed infrastructure may be non-operational. The ad hoc self-organisation also makes them suitable for virtual conferences, where setting up a traditional network infrastructure is a time consuming high-cost task. Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. They are an attractive technology for many applications, such as rescue and tactical operations, due to the flexibility provided by their dynamic infrastructure. However, this flexibility comes at a price and introduces new security threats. Furthermore, many conventional security solutions used for wired networks are ineffective and inefficient for the highly dynamic and resource-constrained environments where MANET use might be expected. Conventional networks use dedicated nodes to carry out basic functions like packet forwarding, routing, and network management. In ad hoc networks these are carried out collaboratively by all available nodes. Nodes on MANETs use multi-hop communication: nodes that are within each other's radio range can communicate directly via wireless links, while those that are far apart must rely on intermediate nodes to act as routers to relay messages. Mobile nodes can move, leave and join the network and routes need to be updated frequently due to the dynamic network topology. For example, node S can communicate with node D by using the shortest path S-A-B-D as shown in Figure (the dashed lines show the direct links between the nodes). If node A moves out of node S' range, he has to find an alternative route to node D (S-C-E-B-D). A variety of new protocols have been developed for finding/updating routes and generally providing communication between end points (but no proposed protocol has been accepted as standard yet). However these new routing protocols, based on cooperation between nodes, are vulnerable to new forms of attacks. Unfortunately, many proposed routing protocols for MANETs do not consider security. Moreover their specific features -the lack of central points, the dynamic topology, the existence of highly-constrained nodes, presents a particular challenge for security.

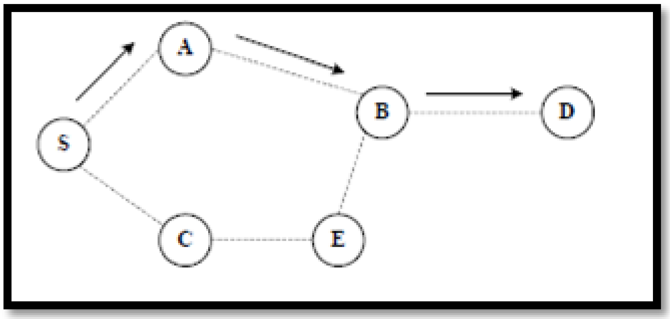


Fig. 1 : Security in MANET

At the highest level, the security goals of MANETs are not that different from other networks. Most typically authentication, confidentiality, integrity, availability, and non-repudiation. In providing a secure networking environment some or all of the following service may be required [1,2].

- **Authentication** is the verification of claims about the identity of a source of information. Authenticity is essentially assurance that participants in communication are genuine and not impersonators [3]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations. This service verifies the identity of node or a user, and to be able to prevent impersonation.

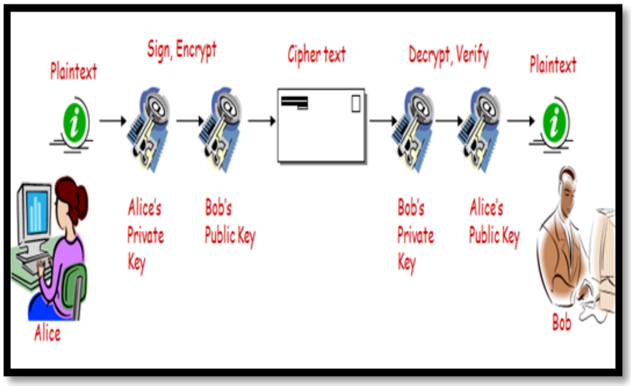


Fig 2. Key Level Authentication

In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANET, and it is much more difficult to authenticate an entity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes [4].

- **Confidentiality** means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information. For example, yesterday's troop location will typically be less sensitive than today's. MANET uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data, and another technique is to use directional antennas. It also ensures that the transmitted data can only be accessed by the intended receivers.

- **Integrity** means that the information is not modified or corrupted by unauthorized users or by the environment. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [5]:
    - *Malicious altering*
    - *Accidental altering*

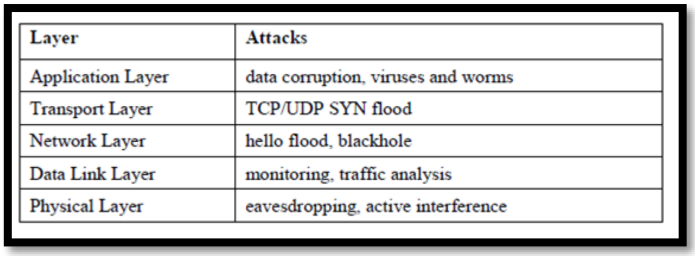
A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering. The integrity service can be provided using cryptography hash function along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

- **Availability** refers to the ability of the network to provide services as required. The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it [3]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [6]. Ensure that the intended network security services listed above are available to the intended parties when required. The availability is typically endure by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocol. Denials of Service (DoS) attacks have become one of the most worrying problems for network managers. In a military environment, a successful DoS attack is extremely dangerous, and the engineering of such attacks is a valid modern war-goal. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service [4].

- **Non-repudiation** ensures that committed actions cannot be denied. In MANETs security goals of a system can change in different modes (e.g. peace time, transition to war, and war time of a military network). The characteristics of MANETMANETs make them susceptible to many new attacks. At the top level attacks can be classified according to network protocol stacks. *Table 1* gives a few examples of attacks at each layer. Some attacks could occur in any layer of the network protocol stack, e.g. jamming at physical layer, hello flood at network layer, and SYN flood at transport layer are all DoS attacks. Non-repudiation ensure that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message.

- **Access Control/ Authorization:** Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions. To prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

- **Anonymity:** Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.



Layer	Attacks
Application Layer	data corruption, viruses and worms
Transport Layer	TCP/UDP SYN flood
Network Layer	hello flood, blackhole
Data Link Layer	monitoring, traffic analysis
Physical Layer	eavesdropping, active interference

Table 1: Layer wise Attack

- **Scalability:** Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network [4]. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system. It is very easy to make an island-hopping attack through one rough point in a distributed network.

3. MANET SPECIFIC ATTACKS

The unique characteristics of MANET routing algorithms result in new sets of wireless computing attacks. The majority of these attacks are directed at the algorithmic capabilities; the means of communicating routing information and the transporting of data. A partial listing of MANET specific attacks follows:

- ***Altering Radio Route Tables*** – Hack the radio and modifying routing tables and the propagation of these alterations[7].
- ***Black Listing*** – Trick a network/system into believing a good node is behaving maliciously [8].
- ***Black Hole*** – Complete refusal to participate in a network, can be sudden.
- ***Gray Hole*** – Selectively dropping packet causing network disruption - can be difficult to detect.
- ***Jamming*** – Selectively jamming routing messages that define the network. Jamming a central node can break down a network. Timed jamming at intervals can cause the appearance of messages being lost, route loss.
- ***JellyFish*** – Active insertion of jitter/delay into packet routing harms QoS and can deny timely packet delivery[9].
- ***Man in the Middle*** – A class of attacks where an intermediary node maliciously manipulates routing messages creating loops, wormholes, and biasing the network to route packets thought malicious nodes [9].
- ***Masquerading Data*** – Message injection without response: Loop forming, spoofing ***Masquerading Peer*** – Presenting self with multiple identities or presenting self as neighbors taking on neighbor functions and roles. MAC spoofing, also know as Sybil attack.
- ***Replay*** – A node in a network may rebroadcast the energy from a neighboring node, extending its range. Thus node B, hearing the replayed message of A by C, will believe that the shortest route is through A. Nodes A and B have no knowledge that packets are being replayed. This is a type of Man in the Middle attack, classified as an unauthenticated node having inserted itself into the network function[10].
- ***Rushing*** – An attack where a node “rushes” a corrupt packet identified to match the real packet. The receiving node first accepts the corrupt packet, dropping it and then, on receipt of the good packet matches the packet identity to that of the prior, and drops it [11].
- ***Selfish Node*** – Nodes that refuse to fully participate in routing.
- ***Sink Hole*** – Taking on more routing than needed, forcing data thought it self; becoming an overly critical network node [12].

4. ATTACKERS OF MANET

Attackers against a network can be classified into two groups: insider and outsider attackers. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs. Routing algorithms are typically distributed and cooperative in nature and affect the whole system. While an insider MANET node can disrupt the network communications intentionally, there might be other reasons for its apparent misbehaviors. A node can be *failed*, unable to perform its function for some reason, such as running out of battery, or collusions in the network. The threat of failed nodes is particularly serious if they are needed as part of an emergency/secure route [1]. Their failure can even result in partitioning of the network, preventing some nodes from communicating with other nodes in the network. A *selfish* node can also misbehave to preserve its resources. Selfish nodes avail themselves of the services of the other nodes, but do not reciprocate. In routing attacks attackers do not follow the specifications of routing protocols and aim to disrupt the network communication in the following ways:

- *Route Disruption:* modifying existing routes, creating routing loops, and causing the packets to be forwarded along a route that is not optimal, non-existent, or otherwise erroneous.
- *Node Isolation:* isolating a node or some nodes(s) from communicating with other nodes in the network, partitioning the network, etc.
- *Resource Consumption:* decreasing network performance, consuming network bandwidth or node resources, etc.

Ning et al. consider each of these goals in their research which analyses insider attacks against AODV [13].

5. CONCLUSION

Mobile Ad hoc Networks (MANETs) have certain characteristics and properties that separate them from traditional computer networks. Most importantly they have no requirements to pre-existing or fixed infrastructure and they need no centralized administration maintaining the network. Here it is the participating nodes' responsibility to sustain routing paths between nodes and make sure that traffic is routed efficiently and reliably from a source to a destination.

In the recent time there has been a lot of interest in the field of wireless networks. The fast moving world demands seamless communication facilities, so former types of connectivity like wired networks, radio waves are fast becoming obsolete. One of the recent developments in the world of wireless technology is the use of mobile ad hoc networks which was initially developed for military applications but now has expanded to include many commercial applications. The rapid use of MANET has resulted in the identification of several problems. Earlier MANET protocols did not focus on the quality of service but the recent applications like multimedia has impressed the importance of quality of service in MANET and this has become the area of potential interest. To compare and analyze mobile ad hoc network routing protocols, appropriate classification methods are important. Classification methods help researchers and designers to understand distinct characteristics of a routing protocol and find its relationship with others. Therefore, the presentation of protocol characteristics which are used to group and compare different approaches are related to the information, which is exploited for routing, when this information is acquired, and the roles, which nodes may take in the routing process helps in the implementation of AD-HOC Networks. In our work, we have made an analysis of all the above mentioned protocols in order to find the positive and negative aspects of each protocol. This type of analysis could be of much importance to make any new development in MANET protocols.

REFERENCES

[1] M. G. Zapata and N. Asokan, " Secure Ad hoc Routing Protocols," in Proceeding of the ACM Workshop on Wireless Security, Atlanta, GA September, 2002

[2] Y. C. Hu, A. Perrig, and D. B. Johnson, " Ariadne: A Secure On Demand Routing Protocol for Ad hoc Network," in Proceeding of 8th ACM Int'l, Conf. on Mobile Comp, Georgia, September 2003.

[3] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[4] L. Gong. Increasing availability and security of an authentication service. IEEE Journal on Selected Areas in Communications, 11(5):657–662, June 1993.

[5] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.

[6] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[7] K. Sanzgiri, B. Dahill, B.N. Levine, E. Royer, and C. Shields. "A Secure Routing Protocol for Ad Hoc Networks" Technical Report 01-37, Department of Computer Science, University of Massachusetts, August 2001

[8] Y.C. Hu, A. Perrig, and D. Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" Technical Report TR01384, Department of Computer Science, Rice University, June 2002

[9] I. Aad, J. Hubaux, and E. Knightly. "Denial of Service Resilience in Ad Hoc Networks," ACM MobiCom, September 2004

[10] M. Brumster, and T. Le. "Optimistic Tracing in MANET," Florida State University, Department of Computer Science, March 2006

[11] Y.C. Hu, and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Proceedings, pp.28-30, May/June 2004

[12] A. Burg. "Ad hoc Network Specific Attacks," Ad hoc networking: Concepts, Applications and Security Seminar, Technische Universität München, 2003

[13] Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003