Mobile Adhoc Network(MANETS) : Proposed solution to Security Related Issues

Rachika Gupta
Chanderprabhu Jain College of Higher Studies , GGSIP University
Plot no.OCF Sector A-8,Narela,New Delhi-110040,India
guptarachika@yahoo.co.in

Abstract

Most of the research in MANETS has been focused on Routing issues. Security on the other hand has been given low priority. This paper provides an introduction to Mobile Adhoc Networks, Routing related issues and overview of security problems for MANETS, by distinguishing the threats on the basic mechanisms and security mechanisms. It then addresses the possible solution to protect the security mechanism, which involves availability, integrity, authentication and non repudiation. These securities related issues are well addressed if one can provide methods that are pertinent for authentication, key distribution, and intrusion detection and rerouting in case of Byzantine failure in MANETS.
Keywords*: Infrastructure, routing, non-repudiation, Byzantine failure*

1. Introduction

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems.

The next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of **Mobile Ad Hoc Networks.** Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network.

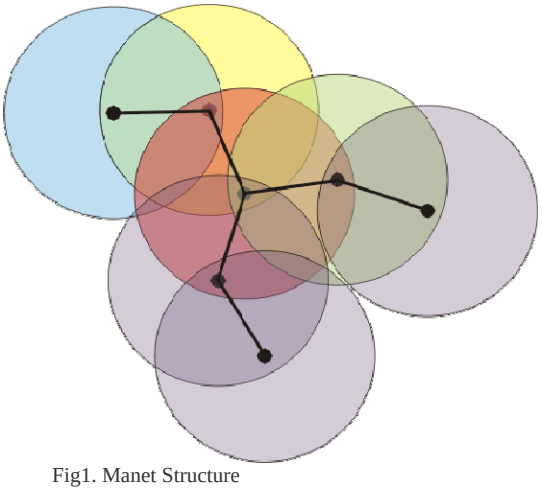

Fig1. Manet Structure

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the nodes themselves must execute the topology and delivering messages, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETS is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETS need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETS. Factors such as variable wireless link quality, propagation path loss, fading, multi-user interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

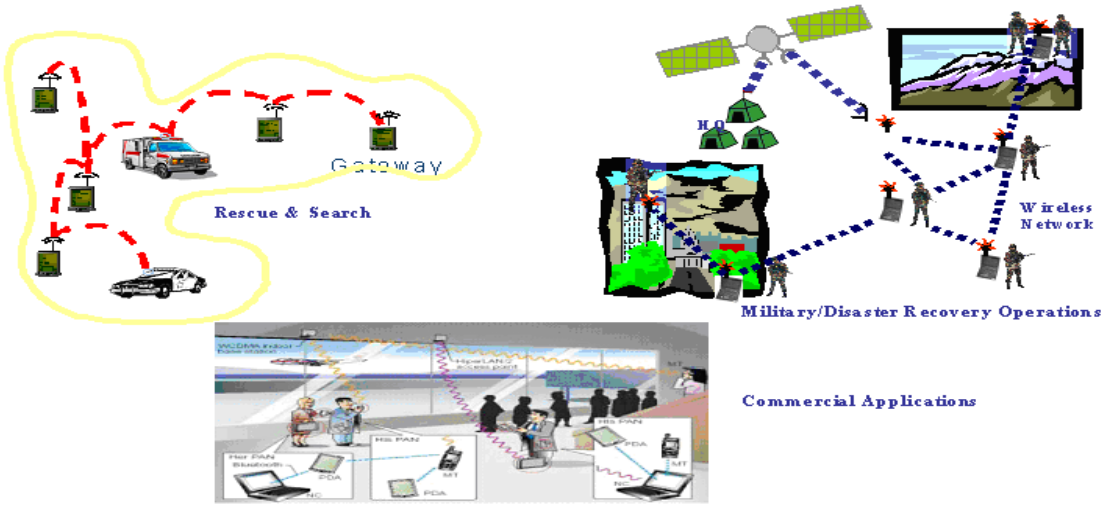

Fig 2. Mobile Ad Hoc Network Applications

Mobile ad-hoc network (MANET) is ideally to be used in emergency situations like natural disasters, military conflicts, emergency medical situations etc as shown in Fig.2

2. Routing in Ad-Hoc Networks

Mobile Ad-Hoc networks (MANETS) are by definition peer-to-peer, multi-hop networks, without any existing infrastructure. If a network host wishes to communicate with another network host that is outside its radio range, it must use intermediate hosts to route the communications. Therefore routing functionality needs to be incorporated into the mobile hosts.

Note: - Because of the common distinction between *hosts* and *routers* in networking documentation, the term *mobile node* shall be used from here on.

In wired networks routing algorithms are categorized as link state based protocols (e.g. OSPF Open Short Path First) or distance vector based (e.g. RIP Routing Information Protocol). The link state protocols use the Dijkstra algorithm. Link state advertisements are sent to all network routers. The routers accumulate link-state information and the Dijkstra algorithm is used to calculate the shortest path to each node. The distance vector based protocols use the Bellman-Ford algorithm. These call for routers to distribute their routing table, but only to their neighbors. The Bellman-Ford algorithm can be used to maintain and update routing information in a wireless network, where there is not a high degree of mobility. However, when a high degree of mobility is introduced, Bellman-Ford protocols are not able to catch up with the frequent link changes and resulting in poor network convergence and low communication throughput. In the design of routing protocols for mobile ad-hoc networks, the following are desirable factors: -

(1) Distributed operation: - With no central hierarchy of routers, routing must be distributed amongst the participant nodes.

(2) Loop-freedom: - Aim to avoid route discovery or maintenance processes from spinning from node to node indefinitely.

(3) Demand-based operation versus Proactive operation: - Are routes to be determined as a source requires it or should a pre-defined current table of routes be distributed amongst nodes? Both approaches are taken in ad-hoc networks and protocols fall into either of these two categories.

(4) "Sleep" period operation: - To conserve energy, it is desirable that when a node is not actively participating on a network, should be able to enter a ‘sleep’ state. The routing protocol should be able to accommodate such periods without major impact on operation.

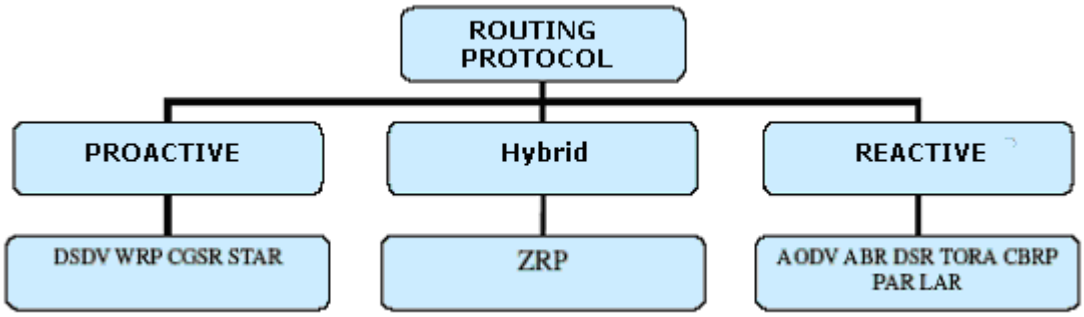

Fig 3 Categorization of adhoc routing protocols

(5) Unidirectional link supports: - Due to variances in wireless radio range between devices, routes may not be bi-directional. This needs to be factored into protocol design so that an alternative route can be used for the return path.As mentioned, ad-hoc network routing protocols fall into two categories: - Demand driven (reactive) protocols or Table-driven (proactive) protocols. Proactive protocols seek to reduce node discovery latency. These protocols require each node to maintain up-to-date routing tables containing routing information from each node to every other node in the network. They respond to changes in network topology by propagating route updates throughout the network to maintain a consistent network view. The areas in which the various protocols differ are the number of necessary routing-related tables and the methods by which changes in the network structure are broadcast. In 2.1 the operation of the proactive protocol, DSDV (Destination Sequenced Distance Vector routing), is outlined. Demand-based (Reactive) protocols seek to reduce control overhead and

link usage by constructing routing information only when the source node requires a route. These savings are gained at a cost of increased route discovery relay. A source node looking for a route to a destination initiates a route discovery within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been discovered and established, some form of route maintenance procedure maintains it until either the destination becomes inaccessible along every path from the source or the route is no longer desired. In 2.2 the operation of the reactive protocol AODV (Ad Hoc On-Demand Distance Vector routing) is outlined.

2.1 DSDV Protocol Outlined

Destination Sequenced Distance Vector routing is a table-driven routing protocol based on the Bellman-Ford algorithm. The modification for ad-hoc networks is that routing loops are avoided. Each network node maintains its own routing table in which all destination nodes in the network and the numbers of routing hops are recorded. Routing information is always available, whether a route is required or not by a source node. Routes are given a sequence number to distinguish stale routes from new ones. Routing table updates are sent periodically throughout the network to maintain consistency. To reduce the amount of network traffic that this produces, table updates are sent as smaller incremental updates during periods of low mobility. During periods of high mobility, full table updates are distributed. As new routes are added to the tables, they include the destination node address and the number of hops. The route with the most recent sequence number (indicating freshness) is always used. If two routes have the same sequence number then the one with the smaller hop count is used.

2.2 AODV Protocol Outlined

The Ad Hoc On-Demand Distance Vector (AODV) builds on the DSDV protocol by minimizing the required number of broadcasts by creating routes on a source initiated, on-demand basis. There is no requirement to maintain a complete list of routes. When a source node wants to communicate with a destination node, it broadcasts (multicasts, if IPv6 is being used) a route request (RREQ) packet to its neighbors. They will forward it on to their neighbors and so on, until it reaches a node with a fresh route to the destination or the destination itself. (Fig. 4)

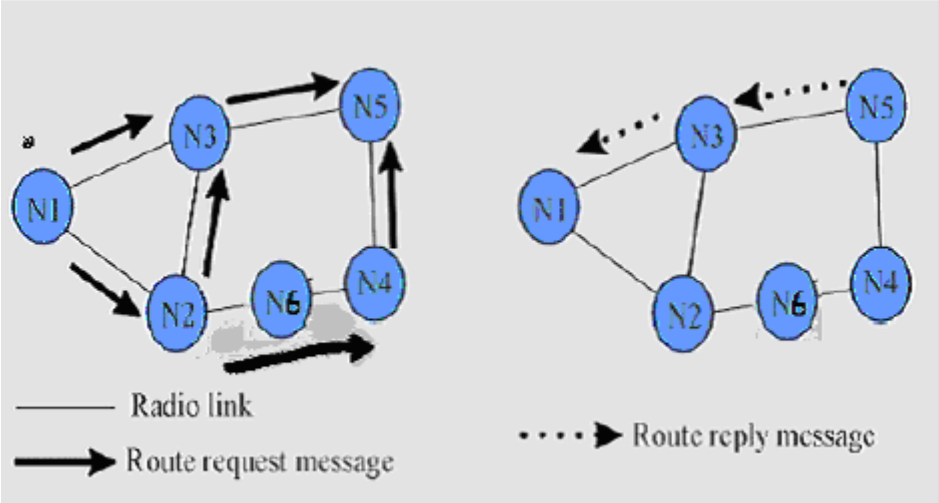

Fig 4 AODV/DSR route discovery, route request message is broadcast, route reply message is unicast

AODV uses sequence numbers to indicate route freshness and to avoid route loops. During the forwarding of RREQ packets the intermediate nodes record in their cached route tables the address of the neighbor from whom they received the RREQ, thereby establishing a reverse path. The destination node or intermediate node with a fresh route to the destination, responds by unicasting a route reply (RREP) package to the source along the reverse path. (Note: Because of this AODV has the limitation of only supporting routes over bi-directional links, routes over uni-directional links will fail). Mobility of nodes may break a previously established route. An upstream node detects this and a link failure notification is sent to each of its active upstream neighbors until the source is reached which may initiate a new route request if required.

3. Securities in Mobile Ad-Hoc Networks

When discussing network security in general, two aspects need to be considered; the services required and the potential attacks. The security services aspect includes the functionality that is required to provide a secure networking environment while the security attacks cover the methods that could be employed to break these security services.

3.1 Network Security Goals

In providing a secure networking environment some or all of the following services may be required:

- ***Confidentiality:*** Ensures that the intended receivers can only access transmitted data. This is generally provided by encryption. Two types of encryption are commonly used (a detailed description of these is outside the scope of this report).*Symmetric Encryption*, where 2 nodes share a key (e.g. - DES, AES). Any data transmitted between the nodes is encrypted using this key. This key must be provided to the nodes over a secure channel. Symmetric encryption generally requires less computational resources than public key encryption. *Public Key Encryption*, where all nodes participating generate a public\private key pair *pubKn/privKn*. The node makes its public key *pubKn* available to all nodes. If other nodes wish to send data to node *n*, they encrypt their data using *pubKn*, safe In the knowledge that it can only be decrypted by *n*'s private key *privKn*, which only node n knows.

- ***Integrity*:** Ensures that the data has not been altered during transmission. The integrity service can be provided using cryptographic hash functions along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

- ***Authentication*:** Both sender and receiver of data need to be sure of each other's identity. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures and certificates. Details of the construction and operation of digital signatures can be found in RFC2560.

- ***Non-repudiation*:** Ensures 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. Non-repudiation requires the use of public key cryptography to provide digital signatures. A trusted third party is required to provide a digital signature.

- ***Availability*:** Ensures that the intended network security services listed above are available to the intended parties when required. The availability is typically ensured by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocols.

This is a vague metric and is provided in varying degrees by all security protocols. There are various types of threats or attacks networks can be vulnerable to, some of which are listed below:

3.1.1 Attacks

- ***Eavesdropping***: This attack is used to gain knowledge of the transmitted data. This is a passive attack, which is easily performed, in many networking environments. However using an encryption scheme to protect the transmitted data can prevent this attack.

- ***Impersonation*:** Here the attacker uses the identity of another node to gain unauthorized access to a resource or data. This attack is often used as a prerequisite to eavesdropping. By impersonating a legitimate node the attacker can try to gain access to the encryption key used to protect the transmitted data. Once the attacker knows this key, she can successfully perform the eavesdropping attack.

- ***Modification*:** This attack modifies data during the transmission between the communicating nodes, implying that the communicating nodes do not share the same view of the transmitted data. An

example could be when the transmitted data represents a financial transaction where the attacker has modified the transactions value.

- ***Replay*:** The attacker retransmits data previously transmitted by a legitimate node.

- ***Denial of Service (DoS)*:** This active attack aims at obstructing or limiting access to a certain resource. This resource could be a specific node or service or the whole network. This will affect the availability security service mentioned above. The nature of ad-hoc networks where several routes exist between nodes and routes are very dynamic gives ad-hoc a built-in resistance to DoS attacks, compared to fixed networks. Security mechanisms for wireless ad-hoc networks should aim to provide all the security services listed above and prevent any of the attacks mentioned. However, due to the lack of infrastructure in an ad-hoc wireless network, typical wired-network implementations of the methods mentioned above may not be possible. Along with the general issues listed above, there are also other specific key issues and challenges for providing security in ad-hoc.

- ***Link Level Security:*** In wireless environment the links are susceptible to attacks where eavesdropper can intercept data packets. Physical barriers such as walls\rooms\&c. provide no barrier to wireless radio packets.

- ***Routing\Network layer Security:*** The routing within ad hoc networks is more vulnerable to attack as each device itself acts as a router. An attacker can pose as a member node and incorrectly route packets to achieve an attack. Denials of service attacks are particularly easy doing this. Thus implementation of secure routing protocol is one of the challenges within ad hoc network. The use of IPSec to provide authentication, confidentiality and integrity is discussed in this report. By securing all IP traffic (or whatever network layer protocol is used), you are also securing outing.

- ***Key Management:*** General network security implementation of keys involves a trusted authority. Given the lack of infrastructure in ad-hoc, it is generally not possible to have a fixed trusted authority. An alternative to this is required. Security mechanisms will now be outlined for the 802.11 protocols and the Bluetooth protocol.

3.2 802.11 Based Security

3.2.1 WEP

Included with the release of 802.11b (WiFi) is an encryption protocol, Wireless Encryption Protocol (WEP). WEP protects packets at the data link layer using symmetric key encryption. It is described in detail in the 802.11 standard .WEP aims to provide the following security services:

- ***Confidentiality:*** The fundamental goal of WEP is to prevent eavesdropping attacks.

- ***Integrity:*** A related goal is to prevent tampering with transmitted messages; the checksum provides this.

WEP does not aim to provide authentication or non-repudiation. (It cannot as it uses a symmetric key shared amongst all parties). WEP relies on a secret symmetric key *k* shared between the communicating nodes to protect the data. It also requires an initialization vector-IV (sometimes called a Network Number or SSID), which needs to be configured identically on each node. To improve security the IV should be updated at regular intervals. This can be done manually or programmatically and is left up to the implementer. Also left up to the implementer is the method for distributing the symmetric shared key *k*, between the nodes. This may not be an issue for ad hoc networks formed where all nodes were pre-configured with this key. But it would render WEP unsuitable for ad-hoc networks where nodes were fully independent of each other before joining the network, as the key would have to be distributed in plain text over the radio link, leaving it wide open for an attacker to intercept. A suggested method for distribution of this key to nodes joining an ad-hoc network could be taken from the paper, where the key is transmitted over a secure side-channel independent of the main data communication channel. IrDA, audio or physical means are possible candidates for this side-channel. The basis of the confidentiality and integrity security of WEP is in the “inabilities to brute force attack the RC4 hashing algorithm. There are variations on the bit size of the key used in WEP from a basic 40-bit encryption, (which is still common in many devices) to 128-bit encryption. The ability to computationally crack 40 bit encryption

keys has been possible for several years (as detailed in the publication of the Netscape 40-bit SSL crack). Any 40-bit implementations of WEP are therefore very insecure. Adding to this insecurity is the usage of the IV the encryption initialization vector). In many devices it is configured to reset on device power reset and to increment non-randomly at periodic intervals. This design increases attacker's chances of success. It has also been shown that the 128-bit version of WEP is also open to attack. This report exposes weakness to attack regardless of key size used. If this key is not updated regularly, (as is the case with some basic WEP implementations), then nodes leaving the network could be compromised and the shared key discovered. It has been shown that WEP has serious flaws and even without these flaws may not be suitable for ad-hoc networks due to the requirement that nodes must be pre-configured with the symmetric encryption key. However, if it is possible to provide this WEP symmetric key to nodes participating in and ad-hoc network, WEP would be infinitely better than no security at all.

3.2.2 WPA & 802.11i Security

As a result of the problems discovered with WEP for wireless data encryption, an IEEE group proposed and is working on protocol 802.11i. Preceding the release of 802.11i, WiFi Protected Access (WPA) was designed to shore up the insecurities of WEP. WPA was created and promoted by the WiFi Alliance, which includes Microsoft, Intel, Cisco, and Apple. They effectively used the 802.11i draft proposals to create WPA, which provides some of the proposed functionality of 802.11i.WPA is backward compatible with 802.11a & b.

- **WPA**

WPA provides authentication by requiring an implementation of the 802.1X standard. The 802.1X standard was developed to secure wired networks and is commonly referred to as RADIUS. The 802.1X framework provides the link layer with extensible authentication, normally seen in higher layers. 802.1X requires three entities:

- ***The supplicant*** - Resides on the wireless LAN client
- ***The authenticator*** - Resides on the access point
- ***The authentication server*** - Resides on the RADIUS server.

The authentication of the supplicant by the authenticator\authentication server takes place using EAP\TLS public key authentication. The authenticator only allows access to itself via a single port; the supplicant has no access to the rest of the network. The authenticator challenges the supplicant for credentials, which could be a digital certificate or a username and password, and passes this information to an authentication server. If access is approved, the authenticator hands over a unique per-supplicant master key from which the supplicant's network adapter derives the TKIP key (Temporal Key Integrity Protocol), the packet integrity key, and other cryptographic necessities. After a user has been authenticated, EAP is used to frequently refresh the master key, reducing the window of opportunity for intercepting packets for cracking. Note that while EAP itself is not encrypted, and EAP-TLS is difficult to implement in wireless networks, there have been works to tunnel EAP within a tunnel. (See 'PEAP' in Microsoft TechNet for Microsoft's solution). WPA was designed for communication between wireless devices and a central access point. The limitations of this system for ad-hoc networks are immediately obvious. It would be possible to implement this 802.1X-based authentication for ad-hoc networks where there exists a permanent, always-available device with enough resources to operate as an authentication server. This is not the case for a stereotypical ad-hoc network, without any pre-existing infrastructure. The article in does list an alternative for networks without an RADIUS server, where WPA supports the use of a pre-shared key. This alternative is, similar to the WEP symmetric key, subject to the same limitations as in distribution of this key to the nodes in the ad-hoc network prior to their joining the network. WPA provides confidentiality by discarding WEP's encryption and using AES. It also uses TKIP to update the security key for each frame sent. TKIP is operational for both the RADIUS based and pre-shared key based implementations of WPA.WPA provides data integrity by use of an 8 bit MIC (message integrity code) that is added to the 32-bit ICV (integrity check value) from WEP, which was found to be susceptible to attack in.

- **802.11i**

WPA addresses a subset of what 802.11i will be. 802.11i is expected to be ratified in mid-2004. 802.11i shall increase the confidentiality provided by WPA by use of RSN (Robust Security Network), which uses the AES encryption algorithm. It also will remove the option of using a pre-shared key that WPA offers, to allow only the

more secure RADIUS\TKIP based key distribution. For the same reasons detailed for WPA this will make 802.11i unsuitable for typical ad-hoc network implementations where no fixed authentication server exists.

3.3 Bluetooth Security

In the previous sections we saw how WEP was introduced to provide security for 802.11, how WPA and ultimately 802.11i were designed to shore up problems with 802.11i. Now we will take a look at how link layer security is implemented in Bluetooth. (LMP and L2CAP layers in Bluetooth terminology). This security is for intra–piconet communication. For scatternet communication, like routing, security is left up to the implementer. In every Bluetooth device, there are four entities used for maintaining the security at the link level.

- **The Bluetooth device address (BD_ADDR)**, which is a 48-bit address that is unique for each Bluetooth device.
- **Private authentication key**, which is a 128-bit random number used for authentication purposes.
- **Private encryption key**, 8-128 bits in length that is used for encryption.
- **A Random number** (RAND), which is a frequently changing 128-bit random or pseudo-random number that is made by the Bluetooth device itself.

Bluetooth security is divided into three modes:

-Security Mode 1: non-secure
-Security Mode 2: service level enforced security
-Security Mode 3: link level enforced security

The difference between Security Mode 2 and Security Mode 3 is that in Security Mode 3 the Bluetooth device initiates security procedures before the channel is established. In Mode 2, the channel is set up and security is performed higher up the protocol stack. Security keys are created in Bluetooth using a combination of the device address, a RAND and a PIN, entered by the user.

4. Manets security problem and proposed solution

As we are aware of that MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets or impersonate a node. This violets the network's goal of availability, integrity, authentication and nonrepudiation. Compromised nodes can also launch attacks from within a network. Most proposed routing algorithms today do not specify schemes to protect against such attacks. We give below methods that are pertinent for authentication, key distribution, intrusion detection and rerouting in case of Byzantine failures in MANETs.

4.1Cryptography

Often, the sender/receiver is an organization. The goal of cryptography is to split a cryptographic operation among multiple users so that some predetermined number of users so that some predetermined number of users can perform desired operation. In organizations, many security-related actions are taken by a group of people instead of an individual so there is a need for guaranteeing the authenticity of messages sent by a group of individuals to another group without expansion of keys and / or messages. To avoid a key management problem and to allow distribution of power, an organization should have one public key. The power to sign should then be shared, to avoid abuse and to guarantee reliability.

4.2 Decentralized authentication of new modes

Two nodes authenticate each other using signed unforgeable certificates issued by virtual trusted CA. Multiple nodes will function collectively as a CA. Authority and functionality of an authentication server is distributed across *k* nodes that collaboratively serve and provide authentication services.

4.3 Per-packet and per-hop authentication

A new node has to be initially authenticated by each of its neighbors to join the network. Once that has been accomplished, each packet sent by the node to its one-hop neighbor is authenticated by the neighbor using a packet authentication tag. The one-hop neighbor then replaces the tag with its own authentication tag and forwards the packet to its neighbor. This next neighbor verifies the new authentication tag as coming from its immediate neighbor and the process is repeated iteratively until the packet reaches its destination. Therefore, each packet is authenticated at every hop.this scheme has the advantage that is resistant to denial of service (DoS) attacks and sessions hijacking attacks such as man-in-the-middle attack.

4.4 Intrusion detection in manets

An effective IDS is a key component in securing MANETs. Two different methodologies of intrusion detection are commonly used: anomaly intrusion detection and misuse intrusion detection. Anomaly-detection systems are usually slow and inefficient and are prone to miss insider attacks. Misused detection systems can not detect new types of attack. Hybrid systems using both techniques are often deployed in order to minimize these shortcomings.

5. Conclusion

MANETs consists of mobile nodes interconnected by multi hop communications paths or radio links. A MANETs consists of mobile platforms known as nodes, which are free to move at any speed in any direction and organize themselves randomly. The nodes in the network function as routers, clients and servers. These nodes are constrained in power consumption, bandwidth and computational power. Because of this unique characteristics and constraints traditional approaches to security are inadequate in MANETs. Traditional authentication, key distribution and intrusion detection methods are often too inefficient to be used in resource-constrained devices in MANETs. In this paper we propose to combine efficient cryptographic techniques and a distributed intrusion-detection system. We also propose to use distributed Certifying Authority (CA) along with per-packet and per-hop authentication for addressing the related security issues.

References

[1] G.V.S. Raju and Rehan Akbani " Some security Issues in Mobile Ad- hoc Networks" in proceedings of the cutting Edge Wireless and IT Technologies Conference, Nov. 2004.

[2] D. Remondo " Tutorial on Wireless Ad-hoc Networks" HET-NETs '04: Second International Working Conference in Performance Modelling and Evaluation of Heterogeneous Networks.

[3] David Blount, "A study of Mobile Ad-Hoc Network Architectures and Technologies" National University of Ireland, Cork, April 2004

[4] H Yang, H.Y.Luo and F.Ye, "Security in Mobile ad hoc Networks: challenges and Solutions" University of California, 2004. IEEE Wireless communications.11 (1), pp 38-47.