Introduction

Communication technology and services have witnessed major growth in recent years. Mobility has become very important, as people want to communicate anytime, anywhere. In the areas where there is little or no infrastructure available or the existing wireless infrastructure is expensive and inconvenient to use, Mobile Ad hoc Networks (MANET) are the useful means of communication.

1.1 Mobile Ad Hoc Networks

MANETs are becoming the integral part of next generation mobile services. A MANET is a collection of wireless nodes to exchange information without using any pre-existing fixed network infrastructure (Sun, 2001). The term MANET refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time without using any kind of fixed wired infrastructure. MANET is actually self-organizing and adaptive network that can be formed and deformed on-the-fly without the need for any centralized administration (Frodigh et al., 2000). Generally, there are two distinct approaches available for enabling wireless mobile units to communicate with each other. They are the infrastructure and infrastructureless networks.

Infrastructure

Wireless mobile networks have conventionally been based on the cellular concept and rely on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the fixed network infrastructure. Typical examples of this kind of wireless networks are UMTS, GSM, WLL and WLAN.

Infrastructureless

In infrastructureless approach, the mobile wireless network is generally known as a Mobile Ad hoc Network (MANET). A MANET is a collection of wireless nodes to exchange information that can dynamically form a network without using any pre-existing fixed network infrastructure (Carvalho, 2008). It has a lot of important applications, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of a wireless connections on-the-fly. Figure 1.1 shows an example of MANET.

“Mobile ad hoc networks (MANETs) stand for complex distributed systems that include wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ad-hoc network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure” (Pravin and Katkar, 2010).
1.1.1 Military Background Environment

MANETs have received the attention of numerous agencies due to their self-configuration and self-maintenance capabilities. Their many applications include military battlefields, disaster relief efforts, conferences, classrooms, taxicabs, sports stadiums, boats, and small aircraft (Sun, 2001). Figure 1.2 shows how teams of MANETs composed of several military components, to include UAVs, can be organized and deployed.

![Figure 1.2 : A Large-scale Deployment of Autonomous Teams in a MANET](Bellur et al., 2002)

Early MANET research efforts were focused on functionality (Kolodzy and Consulting, 2008). Security has now become a priority since MANETs are being deployed in potentially military environments (Kioumourtzis et al., 2007). Traditional wired security solutions do not apply to MANETs due to their “open” network architecture (nearby nodes will often be capable of sending and receiving MANET protocol packets), shared wireless medium, resource constraints, and dynamic network topology (Corson and Macker, 1998). For a MANET to be secure, required services include authentication, confidentiality, integrity, availability, and non-repudiation. Any security solution that provides these services must be implemented at each level of the communications stack (Carvalho, 2008).

A unique characteristic of MANET security is the lack of a clear line of defense. Traditional fixed networks have dedicated infrastructure such as firewalls, routers, and Intrusion Detection
Systems (IDS) to provide protection from outside threats. However, each MANET node functions as its own router and forwards packets to other peer nodes. The wireless channel used by a MANET is open to legitimate users, eavesdroppers, and malicious attackers. No well-defined place exists in a MANET where traffic can be monitored or access control deployed. Therefore, there is no clear separation between the “inside” and “outside” network. Since there is no clear threat to defend against, typical MANET routing protocols assume a trusted and cooperative environment. This blind trust enables malicious nodes to disrupt network operations by intentionally disobeying protocol specifications. Nodes may also misbehave unintentionally due to hardware failure or restriction of resources, such as limited battery power.

MANET protection techniques can be classified as proactive or reactive. Proactive approaches use various cryptographic techniques to prevent an attacker from launching attacks while reactive techniques attempt to detect security threats after they occur and react appropriately. Any complete security solution for MANETs should include prevention, detection, and reaction (Yang et al., 2004).

1.1.2 Challenges of Mobile adhoc Networks

The features of MANET include several challenges that must be studied carefully before a wide commercial deployment can be expected (Taneja and Patel, 2007). These include:

i. Routing
ii. Security and Reliability
iii. Quality of Service
iv. Internetworking
v. Power Consumption
vi. Scalability
vii. Link Level Security
viii. Secure Routing
ix. Key Management,

Dynamic mobility
x. Lack of infrastructure
xi. Connectivity
xii. No prior relationships
xiii. No prior relationships
xiv. Physical vulnerability
xv. Limited Resources and
xvi. Adversaries

i. Routing

Since the topology of the network constantly changes, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which are more complex than the single hop communication.

ii. Security and Reliability

An adhoc network has its particular security problems e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics also introduce reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem) data transmission errors and mobility-induced packet losses.
iii. Quality of Service (QoS)

To provide different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic nature of communication quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.

iv. Internetworking

In addition to the communication within an adhoc network, internetworking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

v. Conservation of power

For the majority of the light-weight mobile terminals, the communication-related functions should be optimized for power consumption. Power-aware routing and conservation of power must be taken into consideration.

vi. Scalability

The traditional wired network in which its scale is generally predefined when it is designed and does not change much during the use; the scale of the ad hoc network keeps changing all the time. One can hardly predict the number of nodes in the network in the future. As a result, the services and protocols that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds, or even thousands of nodes. In other words, these protocols and services need to scale up and down efficiently.

vii. Link level security

Nodes in an ad hoc network communicate via wireless links, which are much prone to various active and passive attacks. Eavesdropping is a common type of attack as messages transmit through air. This must be due to absence of security mechanisms like firewall, access control etc. Attacks like spoofing, impersonating a node, traffic re-direction, denial of service etc, make it hard to achieve the prime security goals.

viii. Secure routing

Most of the researches in the area of ad hoc networking lead to obtain a secured routing protocol for mobile ad hoc networks, which is tough to achieve. In most of the routing protocols of mobile ad hoc networks, intermediate nodes act as relays. So, if a node is compromised, then it can generate false routing information, replay previous routing information, insert vague information with existing information, in which the whole network gets eventually collapse. Sometimes nodes can act selfishly to save their own battery power. A compromised node can also send malicious information to other nodes, which in turn attacks other nodes in the network (Papadimitratos.P et al, 2002).

xi. Key management
Managing cryptographic keys is one of the prime requirements in any secure network. Most of the key management protocols in the present literature require the presence of a central authority to securely distribute keys among the nodes. However an ad hoc network has no fixed infrastructure, no central authority and when connectivity is not always guaranteed and the key management becomes a key issue for securing ad hoc networks. Distributive Schemes address this problem to a certain extent.

x. Dynamic mobility

One of the major characteristics of an ad hoc network is that the nodes are dynamic in nature. Nodes can join or leave the ad hoc network at any time and thus there is no guaranteed connectivity between nodes. So, static security mechanisms are not always suitable for mobile ad hoc networks. This inherent property of mobile ad hoc network makes it difficult for the researchers to come up with secure key management and routing protocols.

xi. Lack of infrastructure

An ad hoc network is a spontaneous, self created network which cannot rely on a fixed network infrastructure and by definition does not. This lack of infrastructure can enhance a network’s survivability; allowing new communication opportunities which may have been limited by previous restrictive network infrastructure. A fixed entity structure such as a base station or central administration is vital for security mechanisms. The trusted third party member which is expected in traditional networks often defines security services, and manages and distributes secret keying information which allows secure communication of data through encryption and decryption techniques. Therefore, the absence of such a control entity introduces new opportunities for security attacks on the network. The network instead of relying on a central administrator for network and security service, it relies on the nodes to realize these duties in a self-organized manner.

xii. Connectivity

Connectivity is a problem in ad hoc networks as networks are created spontaneously and nodes are mobile. Therefore, connectivity between the nodes is sporadic. This is due to the shared, error-prone wireless medium and frequent route failures caused by the unpredictable mobility of nodes. There are existing routing protocols for mobile ad hoc networks which can administer the dynamic nature of mobile ad hoc networks, but fail to effectively incorporate mechanisms to prevent, tolerate or defend against malicious network security attacks.

xiii. No prior relationships

In ad hoc networks, nodes may have no prior relationships with other nodes within the network. Prior acquaintance between nodes can be seen as pre-trust relationships between nodes. It cannot be assumed that pairwise secrets exist between nodes.

xiv. Physical vulnerability

Another challenge in ad hoc networks is the physical vulnerability of nodes. Compromised nodes are of higher probability in ad hoc networks than in traditional wired networks with stationary
hosts. The attacker could then analyze the node to gain secret keying information or use the node to compromise other nodes. The same threats exist in wired formal networks but they may rely on a secure host to detect and recover compromised nodes. Sensitive security information may also be stored on that host, minimizing information stored in the nodes. Examples of this can be seen in hybrid ad hoc networks which combine fixed and volatile distributive architecture to enhance security within the network.

xv. Limited resources

Since there is no central administrator to perform network and security tasks, and rather relies upon other nodes to accomplish such services, it creates a heavy burden upon nodes to perform their own tasks as well as network tasks. The ad hoc networks are primarily mobile networks; therefore nodes have limited resources compared to fixed wired nodes. To ensure mobility and maximize size, cost and battery life of mobile nodes, the CPU and memory size of the nodes must be optimized. Nodes will also have restricted bandwidth and transmission ranges. Even with Moore's Law predicting the exponential growth of IC technology, network and security schemes must be optimized to accommodate mobile ad hoc networks limitations.

xvi. Adversaries

Threats or attacks upon the network come from entities known as adversaries. These may include insider and outsider nodes that maliciously attack or threaten the network or the secrecy of the network's content. More specifically for ad hoc networks, adversaries focus upon the routing protocol as a point of attack (Raju.G.V.S et al, 2004)

1.1.3 Applications of Mobile adhoc Networks

MANETs are typically used when there is little to no communication infrastructure. They can also be used where the existing infrastructure is too expensive or inconvenient to use. (www.ietf.org/html.charters/manet-charter.html).

Applications that use MANETs varies between large-scale, mobile, highly dynamic networks and small, static networks constrained by power sources (Sun J.Z, 2001). Additionally, MANETs have varied missions, implementations, and operational requirements. A few examples are summarized in the following subsections.

i. Military Battlefield

Information technology is increasingly prevalent in the modern battlefield. MANETs allow the military to use mobile network technology to maintain connectivity between soldiers, vehicles, and information headquarters (Oh and Gerla, 2009). The Defense Advanced Research Projects Agency's (DARPA's) Network Centric Radio System (NCRS) is a first-generation MANET designed to enable ground and airborne-vehicle-based on-the-move and on-the-halt network-centric connectivity (Kolodzy and Consulting, 2008). NCRS offers interoperability among various current, future, coalition,
and first responder communication radios via the network. One of the most challenging aspects of a military MANET is the use of mixed node types.

As shown in Figure 1.3, these networks operate and interface between unattended ground sensors, pedestrians, ground vehicles, low altitude aircrafts, ships, high altitude aircrafts, and satellite platforms. Each has different characteristics in mobility, available power, line-of-sight, and latency tolerance. They also have different networking requirements, placing challenges on the interfaces between them.

![Figure 1.3: DARPA’s First-Generation MANET Network Architecture](image)

(Kolodzy and Consulting, 2008)

**ii. Commercial Sector**

Emergency rescue operations for disaster relief efforts such as fire, flood, and earthquakes are appropriate applications for MANETs (Super and Smith, 2010). Often, these operations take place where non-existing or damaged communication infrastructure exists and rapid deployment of a communication network is needed. Information is relayed from one rescue unit to another via a handheld device or node (Sun, 2001).

The Rescue Information System for Earthquake Disasters (RISED) is designed to support a more efficient rescue and relief operation for catastrophic earthquakes (Jang *et al.*, 2009). The
objective of RISED is to provide the most up-to-date and accurate rescue-related information possible, such as disaster locations, possible damages to lives and constructions, available rescue and relief resources, and the shortest way to the disaster spots. Two-tier architecture supports a command post with the first tier and local deployments with the second tier. If external network connectivity is lost, local deployments can independently operate to help rescue and relief operations. Figure 1.4 illustrates a MANET-based peer-to-peer network used to support RISED.

![Figure 1.4: Peer-to-Peer MANET Architecture (Jang et al., 2009)](image)

### iii. Tactical UAVs

Tactical UAVs are aircrafts with greater endurance and payload capacity than smaller “micro” UAVs (Allen and Walsh, 2008). These two features often determine when a tactical UAV can be utilized. Tactical UAVs are lower in cost than larger platforms like “Global Hawk” and “Predator” (Reidt and Wolthusen, 2008). Examples of tactical UAVs include the “MQ-5B Hunter” and the “RQ-7B Shadow”. Both are designed to gather battlefield reconnaissance, surveillance, target acquisition, and battle damage information in real time using a multi-mission optical payload, then relaying it via video link to commanders and soldiers on the ground. Improvements to the “Shadow” have allowed it to accommodate a communications relay package, which allows the aircraft to act as a relay station and participate in tactical MANETs. Though it is traditionally resource constrained, research is currently underway to incorporate tactical UAVs into the battlefield.

### 1.1.4 Communication in MANETs

As these Mobile Ad hoc Networks are increasingly being considered for more and more complex applications, the various Quality of Service (QoS) attributes, for these applications must also be satisfied as a set of pre-determined service requirements. In addition, due to the increasing use of the Ad hoc networks for military/police use, and commercial applications, it is being envisioned to be
Routing is one of the primary functions for communicating between two nodes that are not in direct range with each other. The routing protocol (Arunkumar et al, 2008), plays a vital role to make some critical decisions such as the optimal route from the source to the destination, because the mobile nodes operate on battery power. In fact, Ad hoc networks have the capability of making communications even between two nodes that are not in direct range with each other. It is even possible to exchange the packets between these nodes and forwarded by intermediate nodes.

The development of efficient routing protocols is a nontrivial and a challenging task because of the specific characteristics of a MANET environment:

- Due to node movements, the network topology may change randomly and rapidly at unpredicted times.
- The available bandwidth is limited and can vary due to fading, noise, interference, etc.
- Most mobile devices are battery powered; therefore energy consumption plays an important role.
- It is necessary to transfer the data with the minimal delay so as to consume less power.
- Quality of Service support is also needed reducing the packet drop ratio and increasing the key.

Unfortunately, most of the routing protocols suffer from a number of shortcomings: like

- Security problems in communication.
- Scalability problems with growing network size.
- Their performance is only optimal under certain network conditions such as mobility.
- Unreliability in drop of packets.

With the increasing number of applications to harness the advantages of Mobile Ad hoc Networks, more concerns arise for security issues in MANETs. Natures of Mobile Ad hoc networks make them vulnerable to security attacks based on the following reasons. Open medium: Eavesdropping is easier than in wired network.

- Dynamically changing network topology: Mobile nodes come in and go out of network, thereby allowing any malicious node to join the network without being detected.
- Attacks from compromised entities or stolen devices.
- Cooperative Algorithms: The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of network security.
- Lack of Centralized Monitoring: Absence of centralized infrastructure prohibits monitoring agent in the system.

1.1.5 Security issues in MANETs
While early research efforts assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wireline networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design (Djenouri et al., 2005). These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. The characteristics of Mobile Ad hoc Networks, pose numerous challenges in achieving conventional security goals.

**Security goals**

Security is very important in communication networks, but perhaps more so in MANETs because they are so easily eavesdropped and there are no infrastructure devices such as firewalls in place to protect the nodes.

MANET nodes depend on each other to provide security for the network. In addition to the functional challenges of operating a MANET, many security risks must be addressed. To be secure, a network must provide confidentiality, authentication, integrity, non-repudiation, and availability as well as physical security (Biswas and Ali, 2001).

Confidentiality has been defined by the International Organization for Standardization (ISO) as “ensuring that information is available only to those authorized to have access” and is one of the cornerstones of information security. Confidentiality is one of the design goals for a lot of cryptosystems, made possible in practice by the techniques of modern cryptography. MANETs can suffer from multiple points of attack as eavesdroppers may obtain the data transferred without being in the path of traffic (Johansson E and Johnson, 2005).

Authentication is the act of establishing or confirming that claims made by or about something or someone are true. This might involve confirming the identity of a person, the origins of an object, or assuring that a computer program is trusted. A lack of authentication in a MANET can allow an adversary to masquerade as a node, gain access to unauthorized information, and interfere with the operation of the network (Garg and Mahapatra, 2009).

Integrity comprises perceived consistency of values, actions, methods, measures, and principles. Applied to MANETs, integrity ensures a transferred message is not corrupted while in transit between the sender and the receiver nodes (Yang et al., 2004).
Non-repudiation is the concept of ensuring that a party cannot disprove taking part in a transaction. Although this concept can be applied to any transmission of data, the most common application is in the verification and trust of signatures. Non-repudiation is important to a behavior grading mechanism in MANETs so appropriate grading actions can be accurately assessed and to isolate attackers or compromised nodes.

Availability is the degree to which a system, subsystem, or service is operable and ready for use when it is required. Simply put, availability is the proportion of time a system is in a functioning condition. MANETs are vulnerable to DoS attacks, such as electronic jamming, attacks on the routing protocols, and attacks on key management systems, all of which can disrupt trust relationships and disconnect the entire network.

Since MANET nodes are mobile, they are not likely to have physical protection in hostile environments. If a MANET node provides a central service and that node is compromised, the entire network may be deprived of that service. Every node in a MANET is a potential victim of compromise. Therefore, the MANET must be able to discern if a particular node has been compromised and effectively mitigate it.

1.1.6 Layer wise MANET Security for Hostile Environment

From the literature survey (Biswas and Ali, 2001) security issues are analyzed from individual layers namely application layer, transport layer, network layer, link layer and physical layer. The ultimate goals of the security solutions for MANETs are to be providing security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, anonymity and availability to mobile users. In order to achieve the goals, the security solution should provide complete protection spanning the entire protocol stack. Layerwise Security has now become a priority since MANETs are being deployed in potentially hostile environments.

Functions of MANET protocol stack

The functionalities of layer of MANET protocol stack are explained.

i. Physical Layer

The Physical Layer defines the electrical and physical specifications of communicating devices. In particular, it defines the relationship between a device and a transmission medium, such as a copper or optical cable.

ii. Data Link Layer

The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.

iii. Network Layer

The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors.
iv. Transport Layer

The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.

v. Application Layer

The Application Layer is the closest to the end user, which means that both the application layer and the user interact directly with the software application.

Security threats in MANET layers

The layer wise security threats (Biswa and Ali, 2001) are summarized here. They are

   i. Security Threats in Physical Layer
   ii. Security Threats in Link Layer
   iii. Security Threats in Network Layer
   iv. Security Threats in Transport Layer
   v. Security Threats in Application Layer

i. Security Threats in Physical Layer

Physical layer security is important for securing MANET as many attacks can take place in this layer. The physical layer must adapt to rapid changes due to link characteristics. The most common physical layer attacks in MANET are eavesdropping, interference, denial-of-service and jamming. The common radio signal in MANET is easy to jam or intercept. Moreover, an attacker can overhear or disrupt the service of wireless network physically. An attacker with sufficient transmission power and knowledge of the physical and medium access control layer mechanisms can gain access to the wireless medium.

ii. Security Threats in Link Layer

The MANET is an open multipoint peer-to-peer network architecture in which the link layer protocols maintain one-hop connectivity among the neighbors. Many attacks can be launched in link layer by disrupting the cooperation of the protocols of this layer. Wireless medium access control (MAC) protocols have to coordinate the transmission of the nodes on the common communication or transmission medium.

iii. Security Threats in Network Layer

In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network.

iv. Security Threats in Transport Layer
The security issues related to transport layer are authentication, secure end-to-end communications through data encryption, handling delays, packet loss and so on. The transport layer protocols in MANET provide end-to-end connection, reliable packet delivery, flow control, congestion control and clearing of end-to-end connections. Like TCP protocol in the Internet model, the nodes in MANET are also vulnerable to the Wormhole and black hole attacks.

v. Security Threats in Application Layer

Applications need to be designed to handle frequent disconnections and reconnections with peer applications as well as widely varying delay and packet loss characteristics. Like other layers, application layer is also vulnerable and attractive layer for the attackers to attack. This layer contains user data that supports many protocols such as SMTP, HTTP, TELNET and FTP which have much vulnerability and access points for attackers. The main attacks in application layer are malicious code attacks and repudiation attacks.

Countermeasures on MANET layers

The countermeasures followed to defend against layer wise attacks are listed and explained below (Biswa and Ali, 2001).

i. Countermeasures on Physical Layer Attacks

ii. Countermeasures on Link Layer Attacks

iii. Countermeasures on Network Layer Attacks

iv. Countermeasures on Transport Layer Attacks

v. Countermeasures on Application Layer Attacks

i. Countermeasures on Physical Layer Attacks

The physical layer of MANET is immune to signal jamming, DoS attack and also some passive attacks. Spread spectrum technology changes frequency in an arbitrary fashion or spreads it to a wider spectrum which makes the capture of signal difficult. DSSS (Direct Sequence Spread Spectrum) represents each data bit in the original signal by multiple bits in the transmitted signal through 11-bit Barker code. To capture and release the content of transmitted signal, the attacker must know frequency band, spreading code and modulation techniques. Still, there is a problem. These mechanisms are secure only when the hopping pattern or spreading code is unknown to the eavesdropper.

ii. Countermeasures on Link Layer Attacks

The security issues that are strongly related to link layer are protecting the wireless MAC protocol and providing link-layer security support. One of the vulnerabilities in link layer is its binary exponential backoff scheme. The original 802.11 backoff scheme is slightly modified in that the backoff timer at the sender is provided by the receiver instead of setting an arbitrary timer value on its own. The common known security fault in link layer is the weakness of WEP.

iii. Countermeasures on Network Layer Attacks
Network layer is more susceptible to attacks than all other layers in MANET. A variety of security threats are imposed in this layer. The active attack like modification of routing messages can be prevented through source authentication and message integrity mechanism. By an unalterable and independent physical metric such as time delay or geographical location can be used to detect wormhole attack. For example, IPSec is most commonly used on the network layer in Internet that could be used in MANET to provide certain level of confidentiality.

iv. Countermeasures on Transport Layer Attacks

One way to provide message confidentiality in transport layer is point-to-point or end-to-end communication through data encryption. Though TCP is the main connection oriented reliable protocol in Internet, it does not fit well in MANET. TCP feedback (TCP-F), TCP explicit failure notification (TCP-ELFN), ad-hoc transmission control protocol (ATCP), and ad hoc transport protocol (ATP) have been developed but none of them cover security issues involved in MANET. Secure Socket Layer (SSL), Wireless Transport Layer Security (WTLS) protocols are designed on the basis of public key cryptography to provide secure communication.

v. Countermeasures on Application Layer Attacks

Viruses, worms, spy wares, Trojan horse are the common and challenging application layer attacks in any network. Firewall provides protection against some of these attacks. For example, it can provide access control, user authentication, incoming and outgoing packet filtering, network filtering, accounting service etc. Anti-spy ware software can detect spy ware and malicious programs running on the system. Still firewall is not enough because in certain situations, the attacker even can penetrate firewall and make an attack. The application layer also detects a DoS attack more quickly than the lower layers.

1.2 Proposed Methodology

This approach also aims in improving the performance in terms of QoS characteristics as metrics. The methodology is proposed in order to assure Layerwise security for Mobile Ad hoc Networks. The specific contributions are structured in six phases.

- Phase I : Integration of SNAuth with SPMAODV.
- Phase II : SNAuth-SPMAODV with SIP for Application and Network layer Security.
- Phase V : SNAuth-SPMAODV with IPSec for Network Layer Security.
- Phase V : SNAuth-SPMAODV with CCMP-AES for Link and Network Layer Security.
- Phase VI: SNAuth-SPMAODV with DSSS for Physical and Network Layer Security.

Integration of SNAuth with SPMAODV
SPMAODV provides multiple paths between sender and receiver nodes that can be used to offset the dynamic and unpredictable configuration of ad-hoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth. The proper selection of routes using a strict-priority multipath protocol can increase further the network throughput. The main idea of this phase to integrate strict priority multipath AODV with secure neighbor authentication that facilitate neighboring nodes exchange messages to discover and authenticate each other. Thus this phase provides security mechanisms like message integrity, mutual authentication, and non-repudiation; defend against Denial of Service attacks and increase network throughput.

**SNAuth-SPMAODV with SIP for Application and Network layer Security**

Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing with Session Initiation Protocol (SIP) provides application layer and network layer security and it is robust against Denial of Service attack. It reduces dependency on single nodes and routes; it discovers multiple paths between sender and receiver nodes and it has the advantages of a multipath protocol without introducing extra packets into the network offering robustness in a secured MANET. It can be used to offset the dynamic and unpredictable configuration of adhoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth in hostile environment.

**SNAuth-SPMAODV with WTLS for Transport and Network Layer Security**

The primary focus of this phase is to provide transport layer security for authentication, securing end-to-end communications through data encryption and to provide security services for both routing information and data message at network layer. It also handles delay and packet loss. The proposed model combines SNAuth-SPMAODV Routing with Wireless Transport Layer Security (WTLS) to defend against Denial of Service (DoS) attack and it also provides authentication, privacy and integrity of packets in routing, end-to-end communications through data encryption, packet loss and transport and network layers of MANET. SNAuth-SPMAODV with WTLS is found to be a good security solution even with its known security problems.

**SNAuth-SPMAODV with IPSec for Network Layer Security**

Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing with IPSec is robust against Denial of Service attack and it also provides security services for both routing information and data message at network layer in MANET. The proposed method uses a hybrid version of the IPSec protocol, which includes both AH and ESP modes. IPSec is a protocol suit for securing IP based communication focusing on authentication, integrity, confidentiality and support perfect security forward. The significant importance of the aforementioned protocol is that it offers flexibility, which cannot be achieved at higher or lower layer abstractions in addition to the symmetric cryptographic schemes. These are 1000 times faster than asymmetric cryptographic schemes, a fact that makes IPSec appropriate to be used in handheld resources constrained devices such as PDAs.
SNAuth-SPMAODV with CCMP-AES for Link and Network Layer Security

SNAuth-SPMAODV combines with CCMP-AES model to defend against Denial of Service attack and it provides confidentiality and authentication of packets in both network and data link layers of MANETs. The primary focus of this phase is to provide security mechanisms applied in transmitting data frames in a node-to-node manner through the security protocol CCMP-AES working in data link layer. It keeps data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination.

SNAuth-SPMAODV with DSSS for Physical and Network Layer Security

SNAuth-SPMAODV combines with DSSS to defend against Denial of Service attack. The physical layer protocol in MANETs is reliable for bit-level transmission between network nodes and network layer is responsible to provide security services for both routing information and data message. The proposed model combines SNAuth-SPMAODV routing protocol and spread spectrum technology Direct Sequence Spread Spectrum (DSSS) to defend against signal jamming denial-of-service attacks in physical layer and network layer for MANET.

Specific advantages of proposed methodology:

Some of the specific advantages of proposed framework over the existing framework are as follows:

- Defend against Denial of Service attack
- Authentication will be provided by SNAuth, CCMP-AES.
- Confidentiality will be provided by IPSec, CCMP-AES.
- Integrity will be provided by IPSec transport mode.
- Availability will be provided by strict priority multipath routing.
- Non-repudiation will be provided by IPSec transport mode.
- Increased packet delivery ratio
- Increased throughput
- Reduced End to End Delay
- Reduced Jitter
- Reduced Routing Overhead

1.3 Objectives of the Research Work

Layer wise Security (LaySec) is a framework created through this research for integrating multipath routing with secure neighbor authentication and layerwise security techniques in a MANET to defend Denial of Service attack in a hostile environment. Previous researches in this area focused on extending ad-hoc network protocols to address either security or application concerns. There has been little research performed that integrates multipath routing protocols with secure neighbor
authentication due to the limited resources of MANET nodes, limited bandwidth of wireless channels, security attacks and general hostile transmission characteristics of wireless mediums. This framework demonstrates how to deploy a MANET with 1) Secure neighbor authentication that facilitate neighboring nodes to exchange messages for discovering and authenticating each other. 2) Strict priority multipath routing algorithm that provides necessary network resources for hostile environment. 3) Layerwise security technologies to secure MANET layers to defend Denial of Service attacks.

1.4 Organization of the Thesis

Organization of the thesis is structured as follows. Chapter 2 presents the related work of the existing approaches. The summary of famous Layerwise Security Approaches for MANET is presented briefly. Some of the well known routing protocols are discussed indicating the differences, advantages and disadvantages based on the desired routing properties of MANET. The previous enhancement of Secure AODV is also discussed. The need for scheduling algorithms for MANET is presented.

Chapter 3 explains the proposed methodology in six different phases. It introduces overall framework for Layerwise security for MANET. The next coming chapters illustrate the significance of each phase of the proposed approach for Layerwise MANET security.

Chapter 4 presents the integration of existing AODV with Multipath, scheduling algorithm and secure neighbor authentication for neighbor authentication to guarantee the integrity and non-repudiation so that the protocol and nodes can be prevented against Denial of Service attacks. A strict priority multipath routing algorithm that provides necessary network resources for military applications.

Chapter 5 describes the SNAuth-SPMAODV with SIP for MANET Application and Network layer Security and is robust against denial of service attack. It reduces dependency on single nodes and routes; it discovers multiple paths between sender and receiver nodes. It has the advantages of a multipath protocol without introducing extra packets into the network and authenticates the neighbor offering robustness in a secured MANET.

Chapter 6 explains the SNAuth-SPMAODV with WTLS to defend against Denial of Service (DoS) attack and it also provides authentication, privacy and integrity of packets in both routing and transport layers of MANET.

Chapter 7 presents the SNAuth-SPMAODV with IPSec for MANET for network layer security. It uses a hybrid version of the IPSec protocol, which includes both AH and ESP modes. IPSec is a protocol suite for securing IP-based communications focusing on authentication, integrity confidentiality and supports perfect security forward.
Chapter 8 describes the SNAuth-SPMAODV with CCMP-AES to defend against Denial of Service (DoS) attack and it provides confidentiality and authentication of packets in both routing and link layers of MANET.

Chapter 9 presents the SNAuth-SPMAODV with physical layer protocol DSSS to defend against Denial of Service attacks in physical layers of MANET.

1.5 Conclusion

In this chapter, Military background environment and applications of Mobile Ad hoc Network Networks were described. Moreover, this chapter discussed all the general information of ad hoc networks and tackles security issues and challenges. The applications of ad hoc wireless networks include Military Battlefield, Commercial Sector and Tactical UAVs are discussed in detail. This chapter basically provided the necessary details regarding proposed methodology and objectives of the research work. The next chapter discusses the review of literature to understand the current scenario. The famous layerwise security approaches for MANET routing protocols and scheduling algorithms are discussed.