CHAPTER 1

INTRODUCTION

1.1. Introduction

In the contemporary world, security has got immense and critical significance for any type of networks, whether it is wired or wireless communications. At the latest, the emerging mobile technology and other mobile computing devices like PDA (Personal Digital Assistants), handheld devices, laptops, net books, notebooks, tablets and iPods have prompted a revolutionized conversion in the mobile era. This change has brought the concept of ubiquitous computing and can be chosen as one of the research hot topics in computer networking area [1]. This forms one of the major computing environments, wherein users can utilize the available network individually through different electronic platforms. This enables the users to access the necessary information to be communicated wherever or whenever they may be in [2]. The wireless networks act as interfaces to connect people in this kind of environment for communication. One such wireless network that is used for the purpose of communicating with people wherever and whenever they are is a MANET (Mobile Ad hoc Network). Basically a MANET is used to communicate using wireless links with mobile devices forming a temporary network. This kind of network changes dynamically and contains a self-organized infrastructure-less topology which is depicted in Figure 1.1. Eventually, this helps the people on the move to get connected to remote areas without any pre-existing infrastructure [3]. MANETs uses intermediate nodes to communicate with end nodes if they are not in direct radio transmission range. MANETs have some special features which are depicted below [4]:

1. Unreliability of wireless links exists between the nodes, as there are constraints of energy supply, and mobility. These inconsistent links are not suitable for communication.
2. Consistent changes in the topology makes nodes to go in and out of the available radio transmission range and lead to change in the routing information continuously.

3. Existing wireless protocols are statistically configured and do not suit the changing topology of MANETs. The ad hoc feature of the network needs every node to maintain the adjacent node information so as to prevent vulnerabilities from the intruders in the form of attacks.

![Figure 1.1. MANET Network](image)

The data communication in MANETs depends on the requirements of the people in its security as most of the nodes are mobile in nature. But, this factor by itself cannot sufficiently prove that security is maintained in MANETs. However, the above listed salient features in MANETs pose several issues and challenges in realizing security requirements, such as, data confidentiality, authentication, data integrity and availability. As the network is highly susceptible to routing and other attacks resulting in malicious behaviors from the moving nodes, countermeasures should be developed to eliminate such anomalies.
This is where the attention of researchers is to be turned on for discussing the several security issues in MANETs. The available security solutions and counter measures are to be considered and at the same time the loopholes in those existing systems are to be studied for further developments [5]. These factors will necessarily lead to designing of new innovations and expansions of systems to make MANETs very secure, whether it may be the case of military or the commercial networks. In this direction the current thesis makes way towards the design and implementation of the new defensive mechanism to overcome the vulnerabilities in the form of network layer attacks. The later sections discuss the security related topics in MANETs, attacks, protocols, encryption techniques, security mechanisms used in MANETs, problem statement, objectives and organization of the thesis.

1.2. Security in Mobile Ad Hoc Networks

The MANETs unique features and complexity has made them highly vulnerable to security threats than the wired network counterparts. The inherent features of MANETs make them vulnerable to several routing and other layer attacks and it may be impossible to take any counter action once the attacks have been launched. With the latest advancements in hacking, the intruders can easily be successful in infiltration of the system [6]. Eventually, this is what makes very crucial from the point of MANETs to monitor them consistently or occasionally to know what is happening in the system and identify types of misbehaviors that are present in the system. The review for security solutions opens up the fact that it is very much necessary to judge that on what basis we can find a MANET is secure or not or what is the security criteria to inspect the state of security in MANETs. The following sections will brief up the various security requirements needed to secure MANETs:

1.2.1. Network Security Requirements for MANETs Availability

Availability is defined as a security requirement which means that the network is available for all the services and nodes should also behave accordingly without the consideration of the security status of the network [4].
The security requirement is mainly confronted during the malicious attacks in the network and makes the services unavailable for the nodes in the network [5].

- **Data Integrity**: Integrity assures the identity of the messages when they are communicated. The integrity requirement can be negotiated in either of the two ways: as malicious altering and unintentional altering [7]. A malicious altering is one, where a message is detached, repeated or revised by an adversary with some malicious goal. On the contrary, if a message is lost or its contents are changed due to some reasons like the transmission errors in communication or hardware failures as hard disk errors etc; it can be an unintentional altering.

- **Data Confidentiality**: Data confidentiality means the communicated information is accessible to only authenticated nodes. The messages transferred may contain some confidential information which needs to be protected from all entities that are not authenticated ones.

- **Authenticity**: Authenticity defines the security requirement as the communication parties are genuine not impersonators [4]. The sender and receiver have to prove the identity using the authenticated technique. Otherwise, the adversaries can easily get access to the confidential information and propagate false updates in order to disturb the normal operation of the network.

- **Authorization**: Authorization is defined as the process in which an entity is issued a permission which includes the privileges and policies to be followed. Different users can be assigned different rights, so that the authorization process makes the functionalities accessible accordingly.

### 1.2.2. Issues and Challenges in Security Provisioning for MANETs

Designing a foolproof security protocol for MANETs is a very challenging task. This is mainly because of certain unique features of MANETs, which are listed below. The difficulty caused by the features like shared broadcast radio channel, insecure operational
environment, lack of central authority, lack of association among nodes, limited availability of resources and physical vulnerabilities in providing security are discussed as below:

- **Shared Broadcast Channel:** The radio channel used for communication in MANETs is broadcast in nature and is shared by all the nodes in the network. The nodes within the direct transmission range can receive the messages instantly. This feature makes malicious nodes to get access of the data transmitted in the network. The problem is overcome by using directional antennas and is not in the coverage of this thesis work.

- **Insecure Operational Environment:** The deployment of MANETs in different network environments may not be always secure. One such example, is military battlefield, search and emergency operations, rescue operations, where there is no question of network connectivity at all and nodes tend to move in and out of the range often becomes more vulnerable to attacks [8].

- **Lack of Security Boundaries in MANET:** MANETs vulnerability is very much self-evident in the sense that there is no clear defined secure boundary as compared to wired networks. This is solely because of the MANETs movable nodes which can join, leave or move inside the network at their will. As in wired networks, the adversaries in MANETs cannot pass through several lines of defense as firewalls or gateways, which make them easily, perform malicious behaviors in the network layers [9]. In MANETs, the adversary need not to have a physical access to the network, but it can directly enter in the radio range and communicate with other nodes in that range and join or leave network instantly. Because of this reason, MANETs lacks the presence of secured boundary line that is needed to protect the network from potential attacks from intruders. This absence of boundary line makes MANETs suffer from many attacks from any nodes in the available radio range. Examples of such attacks are message tampering, message contamination, DoS attacks, eavesdropping of packets, rushing attack, replication attacks, black hole and gray hole attack [4].
➢ Security Threats from Compromised nodes in the Network: In an organization, if every node shares a common goal and be in the same radio range as in military or big corporate offices, it creates a trust environment accessible over the Internet. Since the wireless technology has taken a big leap in today’s era, it appears that more and more, huge and heterogeneous networks are emerging in business and other areas. In such big networks, the neighboring nodes behavior remains unforeseen and leads to lot of insecurities. In these circumstances, if proper security precautions are not taken, any node at any instant can become compromised to violate the data integrity in communications [10].

In case of the routing attacks as discussed above, the nodes present in the route tries to launch malicious behaviors to destruct the routing. Apart from these attacks, there exist some nodes, which compromise situations to control the network services to execute misbehaviors. These types of attacks from compromised nodes are merely from the insiders in the network. Since MANET itself is an autonomous system, the nodes also behave as they will to join or leave the network and it becomes very critical even for some of the genuine nodes in the system to prevent the misbehaviors as many nodes have different kind of behaviors. Since most of the compromised nodes are insiders in the network range they are very well known with the network conditions like mobility and neighboring nodes. Extracting this kind of information, the compromised nodes frequently change their attack strategies and make it very difficult to track their misbehaviors especially in large networks. These types of attacks are far more dangerous than the attacks from outsiders of the network and are tough to detect. Examples of these attacks are byzantine failures, where a set of compromised nodes with a good understanding among themselves launch malicious attacks which are harder to detect [4]. As the compromised nodes behave well inside the network range, they try to utilize some of the inconsistencies and anomalies in the routing protocols to totally disturb the routing information by giving false updates of stale routes, non-existent routes and forwarding fake route information in the network.
Even the threats from compromised nodes are proved to be harder for MANETs and need the attention of researchers through which some kind of trust policies can be expected [5].

- **Lack of Central Authority:** The absence of centralized authority in MANETs makes it more vulnerable to attacks. As there is a lack centralized authorities like name servers, base stations, it is very difficult to monitor the traffic and detect attacks in a highly dense mobile environment [7]. The frequent occurrence of failures in MANETs such as, packet dropping, path breakages, communication impairments etc; makes it critical to detect misbehaviors as the adversaries keep changing their attack patterns and targets randomly. The vulnerabilities caused by the adversaries cannot be identified as to whether it is a benign or malicious failure, as large amount of malicious activity exists. That is the reason why lack of central authority is going to cause severe problems when vulnerability persists. This feature will also impede the trust policies for the nodes in MANETs [4].

The co-operation among nodes plays a major role as there will be no central security association present in the network. There are some algorithms in MANETs that depend on the co-operative participation of all nodes and the network topology. As MANET is decentralized network an adversary can take advantage of this feature and launch attacks that can break these algorithms [11]. The lack of centralized authority will lead to severe vulnerabilities in the normal operation of the ad hoc network. There is a crucial need to develop a solution to mitigate this problem, which will be discussed in the later chapters.

- **Power Supply Constraints:** The node mobility is another issue in MANET which causes power constraints for the devices as there are no power supply outlets, which in turn lead to several problems. This leads to attacks where an adversary targets the battery restricted destination or neighboring node. There may be a possibility of nodes spending time in routing additional packets or in some time consuming computations. This makes the destination nodes battery to get exhausted and makes them deprived of service to all genuine service requests from the network.
This further leads to selfishness in the nodes for not supporting the network functionalities. These selfish behaviors are not malicious behaviors which need to be identified as, whether it is due to power constraint or decisively not to co-operate in operation.

- **Scalability Issues:** The design of MANET cannot be pre-defined like wired networks as there will be mobility of nodes within the range and this keeps on adding as new node enters the range. This causes the scalability problem in MANETs, as the protocols and services for routing and key exchanges should also become compatible with the changes in the environment. This results in scaling up of standards like protocols and services whenever the network grows and needs to be scaled down when network shrinks with less number of nodes.

### 1.3. Security Attacks in MANETs

The complexity and unique features of MANETs make them more susceptible to security threats than the wired networks. Attacks on ad hoc wireless networks are classified broadly in to two types: Passive and Active attacks as shown in the Figure 1.2. This categorization depends on whether the normal operation of the network is disrupted or not.

- **Passive Attacks:** These attacks do not disrupt the normal operation of the network where an attacker snoops the data exchanged in the network without altering it. Passive attack identification is difficult in wireless networks as the network operation will appear to be normal. A very good solution for this problem is to employ a powerful encryption technique. This makes it impossible for the attacker to get the valuable information from the data overheard.

- **Active Attacks:** These attacks attempt to modify or destroy the data being communicated in the network thereby disrupting the normal functioning of the network. There are two types of active attacks viz Internal and External attacks:

  In an external attack, the adversary aims to cause congestion, fake the route information or deprive the nodes from providing services. In case of internal attacks the adversary
gains normal access to the network and tries to disturb the operation of the network through malicious impersonation or compromise with a current node in the network to accomplish its malicious behavior.

The external attacks can be prevented as the adversaries will be within the proximity but cannot be trusted and it becomes easier to detect these attacks using the conventional security approaches. Since the ad hoc networks are more a open media and pervasive in nature, the internal attack identification is difficult and are proved to be dangerous to the network. The network mainly consists of genuine nodes which normally participate in all the activities of the network have access to authenticated information and can gain protection from security mechanisms. The adversaries in the same network can also pretend to be co-operating with these nodes and easily gain access to private network information, to be capable of launching internal attacks. This consequence needs more attention and we need to consider ways to tackle these internal attacks, especially when the security issues in MANETs are discussed.

The network protocol stack pertains to both passive and active attacks for all the layers. This section however, focuses on network layer attacks (routing attacks) as the thesis

![Figure 1.2. Attacks Taxonomy](image_url)

The network protocol stack pertains to both passive and active attacks for all the layers. This section however, focuses on network layer attacks (routing attacks) as the thesis
primarily concentrates on the network layer attacks, which are termed to be the internal attacks for MANETs. The following section, discusses the different network layer attacks in detail. The routing attacks can be classified into five categories depending upon various attacking behavior as wormhole attack, blackhole attack, greyhole attack, byzantine attack, information disclosure attack, resource consumption attack and routing attacks. Amongst these, disclosure is a passive attack and others belong to active attack category. These are discussed in the next section.

1.3.1. Network Layer Attacks in MANETs

Routing mechanism is one of the main problems in MANETs as it consists of only communication terminals that are mobile in nature. As a result, network layer which covers the routing mechanism in the network protocol stack suffers major attacks. There are mainly three stages in routing mechanism such as route discovery, route selection and forwarding and route maintenance. If the contents of discovered routes are changed, route reply messages are modified, stale route entries in route cache and refusing to participate in route discovery process may cause attacks on route discovery process. In route selection and forwarding, if the contents of data packets or route are modified via the path travelled or pretending to be normal node and later involving in packet dropping cause severe throughput degradation and other attacks [6]. In this regard, the following attacks for network layer in MANETs are discussed:

- **Wormhole attack**: This attack involves tunneling of packets from one location to another in the network. The adversary can even create a tunnel for the packets which are not addressed to it. Though the wormholes do not create much harm, if proper security measures are not employed to defend the network, the routing protocols used may end up in finding invalid routes.

- **Blackhole attack**: In this attack, a malicious node falsely advertises the optimal paths for destinations during route discovery process.

The chances of packet dropping activity may be more in case of black hole attacks and intercept the packets being sent to destined nodes.
- **Byzantine attack:** This attack mainly aims in creating routing loops, to route packets on non-optimal paths and also goes for selective packet dropping (Gray hole attack) [7]. Since the network seems to be operating smoothly in the presence of these attacks, the byzantine failures are hard to detect.

- **Resource Consumption Attack:** In this attack, a malicious node tries to consume away the resources on other nodes in the network. The resources may include battery power, bandwidth and computational power which are very much limited in MANETs.

- **Routing Attacks:** These attacks aim on routing protocols used for route discovery process and usually disturb the normal operation of the network.

Some of the routing protocol attacks pertaining to network layer in MANETs are discussed below:

- **Routing Table Overflow:** An adversary tries to advertise routes to non-existent nodes. As a result, this causes routing table overflow and avoids new entries in the table by authenticated nodes. Proactive protocols are highly susceptible to these attacks than reactive protocols.

- **Routing Table Poisoning:** The modification and fictitious updates to genuine route updates are done by adversaries. This result in sub-optimal routing, congestion in parts of the network and even some parts are inaccessible in network.

- **Packet Replication:** The attack aims in replicating the stale packets, as a result the bandwidth and battery power are consumed more. The attack also creates some kind of unnecessary confusion in the route discovery process.

- **Route Cache Poisoning:** This pertains mainly to on-demand routing protocols like AODV (Ad Hoc on Demand Distance Vector), where each node maintains route cache information on latest routes found. Here, also the same objectives such as route table poisoning can be achieved in creating stale routes, loops and sub-optimal entries, congestion etc.
➢ **Rushing Attack:** The on demand protocols are more vulnerable to these attacks. The attacker node which receives a route request packet from source node floods the packet quickly throughout the network before other nodes which also receive the same route request packet can react. Nodes that receive the legitimate route request packet assume the packet to be the duplicates of the packet already received through attacker and discard the genuine ones. Hence, the route discovered may contain the attacker node as one of the intermediate nodes in the optimal path chosen [12].

- **Message Tampering Attack:** In this type of attack, the adversary may tamper the data being communicated via the optimal route. The tampering may in the form of adding some more bytes of data to the original one or by deleting some bytes of information from the original data. This attack mainly causes violation of data confidentiality security requirement.

### 1.4. MANET Protocols

The major issue in MANETs is its dynamic changing topology which may lead to inconsistency in the routing process. To stabilize the routing process in network many protocols have been used. The routing protocol employed should be tolerant to dynamic topology, wireless links, bandwidth restrictions and energy-related problems. Based on these considerations, the desirable qualitative properties of a routing protocol for MANETs are: they should obligated to mobility, ensure small convergence time, robust in nature, supporting unidirectional communications, support scalability and satisfies a huge number of design and functional requirements as high throughput, heterogeneous traffic, priority traffic, low overheads and delays. Finally, the target is to design such a routing strategy which suits most of these needs for MANETs and considered as a part of the current thesis work and will be explained in the later chapters of the thesis. With the constraints in routing protocols, the table-driven approaches will definitely perform badly in dynamic environments.

Based on the routing information we need to update the mechanism and address the challenges of MANETs, like, mobility, shared broadcast channel, hidden and exposed
terminal problems etc. The classifications of ad hoc protocols are described in the following section:

1.4.1. Proactive and Reactive Protocols

The Proactive protocols are also called table driven protocols, where every node maintains a routing table for network topology information for periodic exchange of data. Routing information is generally flooded in to the network and all the time the path finding process is active whether it is needed or not. This results in consuming much of the network bandwidth and overhead and subsequently degrades the network performance.

The reactive protocols are on-demand protocols wherein every node maintains routing information whenever it is required. There will be no periodic exchange of routing information and it saves the network bandwidth and power to the maximum. This is one of the reasons why the developed work uses on-demand approach for path finding process.

1.4.2. Secure Routing in MANETs

The primary issue in wireless networks like MANETs is to find out whether a conventional routing protocol like link state protocol or an on-demand protocol could be applied to network. To answer back, the measure of vitality in route discovery and selection process depends on the factors in MANETs such as: the type and frequency of changes in network and session state; restrictions on response delay forced in accumulating, propagating and acting upon this state information; the amount of network resources available for these functions etc.;. The routing strategy used must be able to rapidly notice and respond to state changes in order to decrease service degradations of existing traffic sessions and also at the same time should use minimum of network resources to maximize the network performance.

The efficacy of a routing protocol increases as network topology information becomes more detailed and up-to-date. As MANETs are having highly dynamic topology, they need frequent exchanges of control information (routes, route updates and routing tables)
among the nodes within the range of the network. If a table-driven protocol is suggested in this case, it triggers flooding, resulting in a flooding rate equal to topological change rate. This kind of blind route update mechanism wastes network resources, as network density may be larger in MANETs, the number of source and destination pairs will also be more and requires high volume of control information to be shared between nodes. This may result in high amount of update traffic and propagation of which eventually saturates the network [13].

Thus, the fundamental requirements of a secure routing protocol for MANETs should include detection of malicious nodes, guarantee of correct route discovery, confidentiality of network topology and stability against attacks. The proposed and developed routing mechanism in the thesis will cover maximum of these requirements stated for a routing process and is independent of protocol in nature.

1.5. Cryptography Methods

The necessity of cryptography techniques in MANETs sound very important as the data transmitted between end parties need to be secured. The communication should cover all the security requirements as data confidentiality, data integrity, availability and authentication. A brief description of all these is given in sub section 1.1.1. As usual, the process of cryptography involves encryption and decryption of data governed by keys, which are small amount of data information in the form of numbers, text or any kind of data used by a particular cryptographic algorithm. The different categories of cryptographic algorithms are discussed in the sub-sections below.

1.5.1. Symmetric Key Algorithms

The symmetric key technique uses a single key for both encryption and decryption. These will be faster to execute and require a secret key to be shared between sender and receiver. Whenever groups are involved, every sender and receiver pair should share a key, which makes the system non-scalable in nature and moreover, if the same key is used by more than one pair the whole system gets corrupted.
The secret key sharing alone cannot maintain the security of a system. MANET involves, mobile adversaries who can easily move from one location to other, attacks them and gets hold of secret keys, totally breaching the security of the network.

The three main ways to build symmetric key cryptographic techniques are key agreement, key pre-distribution and key distribution using trusted third parties (TTP). The TTP-based schemes like Kerberos highly rely on trusted servers for key agreement between nodes. Moreover, these techniques are proved to be impractical for larger network densities, as the deployment of TTP servers is either restricted due to the environmental constraints or uneconomical because of the scalability issue.

On the contrary, key pre-distribution schemes (KPD), have gained more researchers’ attention now a days due to their efficiency and simplicity. KPD uses a trusted authority to generate and distribute secret information, so that, only privileged users can recover the private key, which enables the privileged user to compute the secret key individually. This type of scheme is suitable to moderate density networks, as it utilizes maximum memory when network grows larger. If the network density is average, then the KPD algorithms can scale well to network. Lot of research work is done in KPD protocols in papers like [14, 15]. In the current thesis, as a counterpart to the preventive techniques, a symmetric key approach is used based on key pre-distribution technique which uses the genetic algorithm concept to generate keys of size 32 bits for moderate density networks.

1.5.2. Asymmetric Key Algorithms

The asymmetric key algorithms are also called public key cryptography techniques as they make one key public and the other key in secret (private). As it involves two keys sometimes the key management may become an issue. All the key agreement schemes are based on this rule itself. These protocols will establish a secure context where a session can be run and many parties can communicate on an insecure channel. These types of algorithms make use of mathematical computations which increases computational complexity for the nodes in the network.
The Symmetric key algorithms have proved to be more secure for data transmitted over wireless networks than the asymmetric algorithms. Hence, the developed work considered and compared both preventive and IDS approaches using key and keyless approaches. The symmetric key distribution scheme is based on genetic concept and AES encryption standard built in to the network and IDS keyless scheme is based on a simple substitution method, which are applied for different routing strategies implemented in the work.

*For our convention the detective technique is represented as IDS in the coming chapters.*

### 1.6. Security Solutions in MANETs

The previous sections reveal the different vulnerabilities in MANETs as issues in security provisioning, security attacks, problems from protocol approaches and finally the limitations of the cryptography techniques. To mitigate these kinds of problems a profound security solution to deal with all these odds need to be framed. Security solutions based on cryptographic methods can keep the data confidential, authenticate the identity of hosts and validate data integrity. But cryptography, it is not sufficient protection for mobile hosts; it prevents attacks or prevents hosts from capture. This really opens up some opportunities to MANET researchers’ to build new solutions and they are called Intrusion Detection Systems (IDS). They are the part of typical defense in depth strategies where various security components from layers of protection against attacks are considered. But, goal is not yet met to achieve perfect protection, but pushes adversaries to put more effort.

As a part of the work, popular security schemes existing and the proposed security solution to deal especially with the network layer security attacks in MANETs are discussed in the following sub-sections. The IDS so far proposed in MANETs against attacks are either single layer detection techniques or multi-layer using the preventive or IDS approaches. The IDS presented in the current thesis is different in the sense that it combines multi-layer technique with routing strategies independent of protocol used to evaluate both preventive and IDS approaches.
1.6.1. Intrusion Detection Techniques

By analogy, the intrusion detection technique continually monitors activities like packet traffic or host behavior and automatically recognizes the suspicious, malicious or inappropriate activities. IDS can be host-based or network-based. Usually host-based IDS monitor host activities and is the most reliable detection but does not scale well. Whereas, network-based IDS monitor packet traffic which is scalable, but, detection accuracy is problematic. IDS are classified as misuse detection and anomaly detection methods. Since MANETs changing dynamic topology makes centralized analysis and correlation difficult, nodes must depend on own analysis. The cryptographic methods are used to authenticate source identity of routing information, but the more serious debacle is false routing information from internal nodes. That is why a combination of approaches which includes both cryptography and routing security in identifying attacks is needed and the same has been presented in the current thesis.

One of the earliest intrusion detection schemes presents an architecture where every node is equipped with an IDS (Intrusion Detection system) agent. Here, all the IDS can operate independently to detect intrusions in larger range and is based on co-operative intrusion technique [16]. The other constraints for MANETs like, battery power, selfish behavior of nodes, possible overhead due to multi-layer integration detection and response mechanism are not discussed. The current thesis work concentrates on these issues by comparing the performances obtained applying such detection techniques as applied to MANETs.

1.6.2. Cluster Based Intrusion Detection Techniques for MANETs

As MANETs are constrained with limited power supply, the cooperative intrusion technique may cause huge power consumption for all the participating nodes in the network. In such a case, nodes behave selfishly and violate the original intention of the co-operative intrusion detection techniques. To solve such problems, cluster-based technique is presented for MANETs intrusion detection [17]. A cluster is formed with a number of nodes within the range and in one-hop vicinity.
Through experimentation results, it was found that the cluster-based techniques increase the CPU speed and network overhead will be lower than per node IDS methods. But the detection rate in this case, will be slightly lower than other IDS, as there will be only one cluster head that is monitoring the traffic of the network resulting in inaccurate judgements because of limited processing power [5].

1.6.3. Cross Layer Analysis for Misbehavior Detection in MANETs

The multi-layer intrusion detection technique identifies the vulnerabilities in multiple layers and always stays below the detection threshold so as to escape from capture by the single layer misbehavior detector. The multi-layer technique needs input from all the layers of network stack to be combined and analyzed by the cross layer detector in a comprehensive way. The acknowledgement feature from the MAC layer can be combined with network layer detection of dropped packets and for malicious activity. The current thesis uses this concept and works on network layer packet forwarding technique combined with acknowledgement method from data link layer to know the security violation. Therefore, it becomes necessary to figure out the possible solution for combining features of different layers. It becomes important to know how much of the network resource and network overhead will be increased by applying such a method for intrusion detection. As MANET nodes suffer from power constraints, it is better to adopt a method like cross layer analysis to save energy and measure the performance gain in the network.

1.6.4. Preventive and IDS Security Mechanisms of the Developed Work

The other way to overcome security attacks in MANETs is Preventive and IDS approaches. Preventive approaches are typically based on message encryption methods i.e. key-based cryptography whereas, IDS approaches use the application of digital signatures and cryptographic hash functions. The most popular preventive schemes suggested for external attacks are Key and Trust management and for internal attacks are secure routing protocols. Key distribution is at the center of preventive mechanisms, as there will be no central authority in MANETs, key management has to be distributed over the nodes in the network. The encryption technique used in preventive approaches
ensures only confidentiality of the data communicated. On the other hand, the IDS are detective approaches, has to depend on the audit trace which will be limited to communication activities taking place in the range (localized information) and the techniques like digital signature in IDS schemes ensure the other security goals like message integrity and authentication [18].

1.7. Problem Definition

With the rapid growth in communication infrastructure, access to wireless telecommunications and networks has become affordable and easy to use. Based on the growing demands of military and industrial projects for evolvable systems [19, 20], the state-of-the-art MANETs SSA (Security Solution Architecture) is an excellent solution to those demands. It was found that providing cross layer or multi-layer security architecture is a proper solution and this solution stands as IDS covering many aspects of security as independent of protocol mechanism for routing, encryption techniques and an acknowledgement approach. As per literature review and industrial experience the following problems were investigated:

- **Routing issues in MANETs**: To mitigate the problems in existing protocols there is a paramount need to design a routing scheme independent of protocol used. The proposed and developed routing strategy is able to quickly detect and respond to state changes and minimize the service degradations of existing traffic sessions and at the same time, uses minimum of network resources to maximize the network performance. This helps in defining the mitigation of problems in tolerating extreme topological changes by adopting high scalability, demand-based operation, multiple routes information and finally security, which covers the maximum security requirements.

- **Security Attacks**: Most of the earlier work relies on node failures due to DoS attacks, black hole attacks, jelly fish attacks or wormhole attacks, using existing or new routing protocols. The current research work is defined to enhance the problem to identify link failures caused by many other attacks such as message tampering, gray hole and replication attacks independent of routing protocol.
• **Performance Measure:** This problem defines that the existing approaches have used standard routing protocols with either preventive or IDS approaches, which is enhanced in the work by using both security schemes and evaluated for text, image and graphics data. A detailed study on performance measure in both simulation and experimental approaches combining the functionalities from network layer as packet forwarding and MAC layer as ACK transmissions are done. This cross layer behavior has been observed in two situations of network as ideal and correction cases.

1.7.1. **Motivation**

The aim and scope of wireless technology has to meet the need for fast, reliable and secure information exchange, communication networks in the future. In the last few years, there has been considerable interest in MANETs, as they have significant potential in military communications [21], disaster recovery situations, rescue missions, in commercial environments like electronic payments, business applications to get access to customer files on the fly over the internet within the radio range [22] and providing database for all mobile agents, vehicular services like transmission of news, road condition, weather etc, smart homes and academic institutions such as class/conference room applications.

Consequently, the main challenge facing MANETs is security, as disconnected operations are very common. Providing security solution architecture is considered to be the most crucial need to the MANET security problem, which includes independent of protocol approach, providing efficient key management, and routing and security administration as prevention and detection techniques [23].
1.7.2. Objectives and Scope of the Research Work

The main objectives covered in the developed research work are:

1. Study of issues and challenges in MANETs and the security solutions.

2. Development of the analytical modelling for analysis of node behaviors, showing the impact and isolation of misbehaviors on MANETs using probability analysis.

3. Development of the proposed novel design, Security Solution Architecture (SSA) with four levels incorporated in to it.

4. Development of the proposed new routing strategies independent of protocol used, covering most of the security requirements, namely, Time on Demand Distance Vector Routing (TODV), DH routing scheme and Dijkstra’s algorithm using weight as time concept routing scheme.

5. Implementation and evaluation of SSA in each of its levels and using it as the base model in simulation approach for IDS and preventive approaches, and experimental approach. The SSA is applied as the base architecture for all the developed approaches.

6. Comparison and analysis of the results obtained for all the three developed approaches to draw the inferences.

The Scope of the proposed and developed work is as follows:

- The current research work is applicable to any type of ad hoc mobile communications which involves mobile devices, laptops, PDA (Personal Digital Assistance) etc;
- The Research work limits to the moderate mobility as it is highly difficult to test for different data like text or image.
- The work can be applied to any of the enterprise or military or emergency networks to check the performance and to detect security threats.
• An efficient implementation of simulation environment exactly suits the research work and may need some modifications if extended.

1.7.3. Organization of Thesis

The thesis is organized into six chapters and the description of each chapter is as given below:

Chapter 1: Covers introduction to MANETs, its security issues and challenges, network security attacks, protocols, encryption techniques, security mechanisms and finally the motivation, objectives, problem formulation for the current thesis.

Chapter 2: Includes literature survey towards the present investigation in the area of MANET intrusion detection and prevention, thereby summarized as a research gap to show the relevance of the proposed and developed work.

Chapter 3: Presents a semi-Markov process to show the node behavior model and analysis of probability distributions in isolating malicious nodes from the selected path for communication.

Chapter 4: Presents the design and implementation details of SSA using experimental and simulation approaches and their outcomes.

Chapter 5: Covers the result analysis of analytical modelling, simulation based IDS and preventive approaches undertaken. The discussions include comparison of the performance measures in all the implemented preventive and IDS approaches.

Chapter 6: This chapter contains the conclusions and suggestions for future directions in the area of enhancement of the routing strategy and other related issues.

The Chapter 6 will be followed by References and Appendices.
Chapter Summary:

This chapter inspects the security challenges, attacks, protocols and security solutions in MANETs. It also emphasizes how the current research work addresses the problems of vulnerabilities in MANETs and proposes a new solution to protect network from different kinds of security risks. The main security requirements are first clearly identified to ensure security in MANETs and extracts useful facts to devise an ultimate security solution which is robust and defensive. Secondly, the strong need to define a clear line of defense for MANETs is identified. A discussion on network security attacks classification in MANETs is also made from which, it is clear that the internal attacks are more vulnerable to MANETs than external ones. The need for an on-demand protocol is also suggested which can overcome to some extent the problems with conventional protocols. The symmetric key protocols discussed are better suitable for MANETs to adapt to dynamic topology and mobility factors. To counteract network layer attacks in MANETs, the possible security solutions, both existing and proposed are also discussed.