CHAPTER 1

INTRODUCTION

This chapter starts with an introduction to a new type of networking, mobile ad hoc networks (MANETs). In order to develop suitable security solutions for this new environment, we must first understand how MANETs can be attacked. This chapter provides a comprehensive survey of attacks against a specific type of target, namely the routing protocols used by MANETs. The security issues specific to this environment are introduced in Section 1.2 and a detailed classification of the attacks and attackers against these complex distributed systems is presented in Section 1.3.

1.1 SECURITY IN MOBILE AD HOC NETWORKS

MANETs of various forms have emerged in recent years, supporting the increasing usage of mobile devices such as PDAs, mobile phones, and laptops. Since these devices are getting smaller, cheaper and more powerful, they are becoming increasingly popular. Moreover, the flexibility of MANETs makes them attractive for many applications such as military applications, where the network topology may change rapidly to reflect a force’s operational movements, and disaster recovery operations, where the existing/fixed infrastructure may be non-operational. The ad hoc self-organization also makes them suitable for virtual conferences, where setting up a traditional network infrastructure is a time consuming, high-cost task. The main applications of MANETs are military applications in which
aircrafts, tanks and moving personnel and the like can communicate at peace or in war time.

1.1.1 Mobile Ad Hoc Networks

A mobile ad hoc network (MANET) is a self-configuring network of mobile nodes connected by wireless links. MANETs do not have any fixed and pre-established infrastructure such as centralized management or base stations in wireless networks. The union of nodes forms an arbitrary network topology. However the network topology changes frequently because the nodes can move, leave, and join the network randomly due to mobility.

Conventional networks use dedicated nodes to carry out basic functions like packet forwarding, routing, and network management. In ad hoc networks these are carried out collaboratively by all available nodes. Nodes on MANETs use multi-hop communication: nodes that are within each other’s radio range can communicate directly via wireless links, while those that are far apart must rely on intermediate nodes to act as routers to relay messages. So every node acts both as router and host in MANETs.

Mobile nodes can move, leave, and join the network and routes need to be updated frequently due to the dynamic network topology. For example, node S can communicate with node D by using the shortest path S-A-B-D as shown in Figure 1.1 (the dashed lines show the direct links between the nodes). If node A moves out of node S’s range, he has to find an alternative route to node D (S-C-E-B-D). A routing protocol in such a network is responsible for finding routes and providing communication between end points through cooperating intermediate nodes.
A variety of new protocols have been developed for finding/updating routes and generally providing communication between end points, but no proposed protocol has been accepted as standard yet. There are two kinds of routing protocols on MANETs: proactive and reactive protocols. Proactive routing protocols such as OLSR use periodic exchange of control messages between nodes to build up a routing table. In contrast, reactive routing protocols such as AODV and DSR discover routes when they are needed. There are also hybrid approaches which combine both proactive and reactive approaches. For example, ZRP uses a proactive approach for communication with neighbouring nodes, while it uses a reactive approach for communication with other nodes. These new routing protocols, based on cooperation between nodes, are vulnerable to new forms of attacks. Unfortunately, many proposed routing protocols for MANETs do not consider security, but there are some secure routing protocols proposed in the literature. They take into account active attacks that aim at intentionally tampering with the execution of routing protocols, but do not address passive attacks and selfishness.

Figure 1.1 Communication between Nodes on MANETs
1.2 ATTACKS

We can classify attacks as passive or active at the top level.

**Passive attacks:** In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

Eavesdropping Attacks, also known as disclosure attacks, are passive attacks by external or internal nodes. The attacker can analyze broadcast messages to reveal some useful information about the network. Solutions protecting the radio interface from attacks such as eavesdropping (and jamming) attacks have been proposed in the literature, e.g. spread spectrum communication and frequency hopping.

Traffic Analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols, or seek to provoke communication between nodes. Attackers may employ techniques such as RF direction finding, traffic rate analysis, and time- correlation monitoring. For example, by timing analysis it can be revealed that two packets in and out of an explicit forwarding node at time \( t \) and \( t+c \) are likely to be from the same packet flow. Traffic analysis in ad hoc networks may reveal:

- the existence and location of nodes;
- the communications network topology;
- the roles played by nodes;
- the current sources and destination of communications; and the current location of specific individuals or functions (e.g. if the commander issues a
daily briefing at 10am, traffic analysis may reveal a source geographic location).

**Active Attacks:** These attacks cause unauthorized state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with authorization to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group. Dropping Attacks: Malicious or selfish nodes deliberately drop all packets that are not destined for them. While malicious nodes aim to disrupt the network connection, selfish nodes aim to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted, new routes to the destination to be discovered, and the like.

**Modification Attacks:** Insider attackers modify packets to disrupt the network. For example, in the sinkhole attack the attacker tries to attract nearly all traffic from a particular area through a compromised node by making the compromised node attractive to other nodes. It is especially effective in routing protocols that use advertised information such as remaining energy and nearest node to the destination in the route discovery process. A sinkhole attack can be used as a basis for further attacks like dropping and selective forwarding attacks. A black hole attack is like a sinkhole attack that attracts traffic through itself and uses it as the basis for further attacks. The goal is to prevent packets being forwarded to the destination. If the black hole is a virtual node or a node outside the network, it is hard to detect.

**Fabrication Attacks:** Here the attacker forges network packets. In, fabrication attacks are classified into “active forge” in which attackers send faked messages without receiving any related message and “forge reply” in
which the attacker sends fake route reply messages in response to related legitimate route request messages.

In the forge reply attack, the attacker forges a Route Reply (RREP) message after receiving a Route Request message. It causes route disruption by causing messages to be sent to a non-existent node or putting the attacker itself into the route between two end points of a communication channel if the insider attacker has genuinely a route to the destination. Figure 1.2 shows an example of a forge reply attack. The best route (with minimum hops) from node S to node D is S-I1-I2-D. Malicious node M forges a Route Reply message to the source node S through node I1. The faked message results in the updating of the route entry to the destination node in the routing tables of node S and I1. Node I1 forwards data packets to the malicious node instead of node I2 since node M seems to have a fresh route to node D, so the new route becomes S-I1-M-I2-D (it is not the optimal route).

![Figure 1.2 Forge Reply Attack](image-url)

Attackers can initiate frequent packets to cause denial of service (DoS). Example DoS attacks that exploit MANETs’ features are sleep deprivation torture attacks, routing table overflow attacks, ad hoc flooding
attacks, rushing attacks, and the like. The sleep deprivation torture attack consumes a node’s battery power and so disables the node. It does so by persistently making service requests of one form or another. Another interesting fabrication attack on MANETs is the routing cache poisoning attack. The attacker can make use of this property to poison the routes to a victim node by sending spoofed routing information packets, causing neighbouring nodes to update their tables erroneously.

**Timing Attacks:** An attacker attracts other nodes by causing itself to appear closer to those nodes than it really is. DoS attacks, rushing attacks, and hello flood attacks use this technique. In all existing on-demand protocols, a node needing a route broadcasts Route Request messages and each node forwards only the first arriving Route Request in order to limit the overhead of message flooding. So, if the Route Request forwarded by the attacker arrives first at the destination, routes including the attacker will be discovered instead of valid routes. Rushing attacks can be carried out in many ways: by ignoring delays at MAC or routing layers, by wormhole attacks, by keeping other nodes’ transmission queues full, or by transmitting packets at a higher wireless transmission power.

A further significant attack on MANETs is the collaborative wormhole attack. Here an attacker receives packets at one point in the network, tunnels them to an attacker at another point in the network, and then replays them into the network from this final point. Packets sent by tunneling forestall packets forwarded by multi-hop routes as shown in Figure 1.3 and it gives the attacker nodes an advantage for future attacks. Since the packets sent over tunneling are the same as the packets sent by normal nodes, it is generally difficult to detect wormhole attackers by software-only approaches such as IDS.
Figure 1.3 Wormhole Attack

The very nature of MANETs renders them open to many attacks. The benefits of significant flexibility come at a price. Many of the attacks described above could be avoided by including authentication techniques in the routing protocol. The main idea here is to guarantee that all nodes wishing to participate in the routing process are authenticated nodes; i.e., trusted network elements that will behave according to the protocol rules. Authentication should be enforced during all routing phases, thus preventing unauthorised nodes (including attackers) from participating in the routing and so from launching routing attacks. Authentication can be provided based either on public-key or symmetric cryptography.

1.3 INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

There are three main components of an IDS: data collection, detection, and response. The data collection component is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage, and sending data to the detection module.
1.3.1 Intrusion Detection Systems (IDS)

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. Most existing systems have security flaws that render them susceptible to intrusions, and finding and fixing all these deficiencies are not feasible. Prevention techniques cannot be sufficient. It is almost impossible to have an absolutely secure system. Even the most secure systems are vulnerable to insider attacks. New intrusions continually emerge and new techniques are needed to defend against them.

Since there are always new intrusions that cannot be prevented, IDS is introduced to detect possible violations of a security policy by monitoring system activities and response. IDSs are aptly called the second line of defense, since IDS comes into the picture after an intrusion has occurred. If we detect the attack once it comes into the network, a response can be initiated to prevent or minimize the damage to the system. It also helps prevention techniques improve by providing information about intrusion techniques.

1.3.2 Taxonomy of Intrusion Detection Systems

IDS can use different data sources which are the inputs to the system: system logs, network packets, etc. If an IDS monitors activities on a host and detects violations on the host, it is called host-based IDS (HIDS). An IDS that monitors network packets and detects network attacks is called network-based IDS (NIDS). NIDSs generally listen in promiscuous mode to the packets in a segment of the network, allowing them to detect distributed attacks. There are also intrusion detection systems that use both host-based IDS and network-based IDS. For example, a system can use NIDS and also
HIDS for important hosts in the networks such as servers, databases, and the like. Since NIDS cannot monitor encrypted packets, a hybrid approach, network node IDS (NNIDS) is introduced where each host in the network has NNIDS to monitor network packets directed to the host.

The first technique is anomaly-based intrusion detection which profiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU usage for programs, and the like. It detects intrusions as anomalies, i.e. deviations from the normal behaviours. Various techniques have been applied for anomaly detection such as classification based (e.g. neural networks, support vector machines), nearest neighbour based, clustering based and statistical techniques. Defining normal behaviour is a major challenge. Normal behavior can change over time and intrusion detection systems must be kept up to date. False positives – the normal activities which are detected as anomalies by IDS – can be high in anomaly-based detection. On the other hand, it is capable of detecting previously unknown attacks. This is very important in an environment where new attacks and new vulnerabilities of systems are announced constantly.

1.3.3 Research on IDS

A great deal of research has emerged in the field of IDS. Major research areas are given below:

- Foundations: research on intrusions, intruders and vulnerabilities
- Data Collection: selecting data sources and features, how to collect data, logging, data format.
• Detection Methods: finding the best detection technique(s), improving efficiency and effectiveness of the detection techniques

• Reporting and Response: how to respond to detected intrusions, representation of detected intrusions to the proper authority.

• IDS environment and architecture: how to distribute IDS agents and facilitate interoperability between IDS agents, IDS issues on different systems, encrypted networks, etc.

• IDS security: protection of IDS and IDS traffic

• Testing and evaluation: how to test and evaluate IDSs

• Operational aspects: maintenance, portability, upgradeability, etc.

• Social aspects: privacy issues

Most of the research areas above are immature. The majority of research has been carried out on detection techniques. There are also researches on developing standards for IDS like the Intrusion Detection Exchange Format (IDEF). The aim of IDEF is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to the management systems which may need to interact with them.

1.4 INTRUSION DETECTION ISSUES IN MANETS

Even though there are many proposed IDSs for wired networks, MANET’s specific features make conventional IDSs ineffective and inefficient for this new environment. Consequently, researchers have been
working recently on developing new IDSs for MANETs or changing the current IDSs to be applicable to MANETs. There are new issues which should be taken into account when a new IDS is being designed for MANETs.

Lack of Central Points MANETs do not have any entry points such as routers, gateways, etc. These are typically present in wired networks and can be used to monitor all network traffic that passes through them. A node of a MANET can see only a portion of a network: the packets it sends or receives together with other packets within its radio range. Since wireless ad hoc networks are distributed and cooperative, the intrusion detection and response systems in MANETs may also need to be distributed and cooperative. This introduces some difficulties. For example, distribution and cooperativeness of IDS agents are difficult in an environment where resources such as bandwidth, processor speed and power are limited. Furthermore, storing attack signatures in a central database and distributing them to IDS agents for misuse-based intrusion detection systems is not suited to this environment.

Mobility MANET nodes can leave and join the network and move independently, so the network topology can change frequently. The highly dynamic operation of a MANET can cause traditional techniques of IDS to be unreliable. For example, it is hard for anomaly-based approaches to distinguish whether a node emitting out-of-date information has been compromised or whether that node has yet to receive update information. Another mobility effect on IDS is that IDS architecture may change with changes to the network topology.

Wireless Links Wireless networks have more constrained bandwidth than wired networks and link breakages are common. IDS agents
need to communicate with other IDS agents to obtain data or alerts and need to be aware of wireless links. Because heavy IDS traffic could cause congestion and so limit normal traffic, IDS agents need to minimize their data transfers. Bandwidth limitations may cause ineffective IDS operation. An IDS must be capable of tolerating lost messages whilst maintaining reasonable detection accuracy.

Limited Resources Mobile nodes generally use battery power and have different capacities. MANET devices are varied, e.g. laptops, hand held devices like PDAs (personal digital assistants), and mobile phones. The computational and storage capacities vary too. The variety of nodes, generally with scarce resources, affects effectiveness and efficiency of the IDS agents they support. For example, nodes may drop packets to conserve resources (causing difficulties in distinguishing failed or selfish nodes from attacker or compromised nodes) and memory constraints may prevent one IDS agent processing a significant number of alerts coming from others. The detection algorithm must take into account limited resources.

1.5 HEURISTICS USED IN THIS RESEARCH

The term heuristic is used for algorithms to find solutions between all possible, but do not guarantee that the best is, therefore they can be considered and not about specific algorithms. These algorithms, usually find a solution close to the best one and they find it fastly and easily. Sometimes these algorithms can be accurate, because they actually find the best solution, but the algorithm is still called heuristic until this best solution is proven to be the best. The method used a heuristic algorithm is one of the known methods such as greed, but even ignoring algorithm eliminating some of the problems required for the ease and durability.
This Research uses the following three heuristic algorithms:

- Particle swarm optimization
- Differential evolution algorithm
- Simulated Annealing

1.5.1 Differential Evolution Algorithm – An Overview

The Differential Evolution (DE) algorithm, may be visualized as a simple real-coded PSO originally proposed by Storn& price. In DE procedure, the trial solutions generated from the solution parameters are usually compared as parameter vectors or genomes. In this respect, it owes a lot to its two ancestors namely – the Nelder-Mead algorithm, and the Controlled Random Search (CRS) algorithm, which also relied heavily on the difference vectors to perturb the current trial solutions.

DE is a simple evolutionary algorithm. It works through a simple cycle of stage. In the following Sections, we discuss each of these steps very briefly. Initialization (Initialize population with Random Numbers), which will be done based on the number of variables in the problem, Mutation (Calculate Difference Vector), this will be done usually following the scheme DE/rand/1. Crossover / Recombination (Multi-point Crossover), is the feature in DE unlike GA, where single-point Crossover is preferred. Selection (Elitist Replacement) is the choice of new candidate based on competition.

1.5.2 Particle Swarm Optimization – An Overview

PSO can be easily implemented and is computationally inexpensive, since its memory and CPU speed requirements are low. PSO has been proved to be an efficient approach for many optimization problems with
its fast convergence and simple steps to solve a problem. In spite of these merits, a known fact that PSO has a severe drawback in the update of its global best (G\text{best}) particle, which has a crucial role of guiding the rest of the particles, this leads to overcoming better solutions in the course of search. Each particle tries to modify its position using the following information:

- The distance between current and its best position so far,
- The distance between current and best position of group.

1.5.3 Simulated Annealing – An Overview

Annealing of metals are cooled slowly at very low revs metallurgical process. A similar method simulated annealing optimization. Chance is a local minima in the region tend to find to jump up and down for a heuristic value; Greedy will lead to the promotion of local minima. High temperatures, low temperatures are most likely to deterioration of steps. Simulated annealing maintains the current tasks of variable values. At each step, it is then randomly chooses a random variable choice. Change that set the value of a development or increase the number of conflicts, not to accept the mission, and a new algorithm has a current task. Otherwise, it is very dependent on temperature and how bad the current assignment, accepts some of the probable assignment. If you do accept the change, do not change the current task.

1.5.4 Organization of the thesis

Chapter 1: Introduces about the present motivations of this research work carried out on Intrusion detection system on Mobile ad hoc networks.
Chapter 2: Reviews the thorough literature of heuristic algorithms for Intrusion detection system on Mobile ad hoc networks.

Chapter 3: In this chapter, the Intrusion detection system on Mobile ad hoc networks is proposed. Clustering in MANET gives energy efficient solution. In this chapter we proposed a secure clustering algorithm using a particle swarm based optimization technique. The method solves three objective functions based on nodes QoS parameters: life time, trust value and bandwidth. The proposed PSO method is coded with MATLAB and simulated for standard situation. The performance of the proposed approach is demonstrated by varying number of nodes and transmission range of nodes.

Chapter 4: In this chapter we proposed a secure clustering algorithm using a differential evolution algorithm based technique. The proposed DE method is coded with MATLAB and simulated for standard situation. The performance of the proposed approach is demonstrated by varying number of nodes and transmission range of nodes and the test results are compared with that of the results in chapter 3.

Chapter 5: In this chapter we proposed a secure clustering algorithm using a simulated annealing algorithm based technique. The proposed SA method is also developed with MATLAB and simulated for standard situation. The performance of the proposed approach is demonstrated by varying number of nodes and transmission range of nodes and the test results are compared with that of the results in chapter 3&4.

Chapter 6: Presents conclusion and possibilities for future expansion of this research on the Intrusion detection system on Mobile ad hoc networks is presented.