ABSTRACT

Researcher's Name : **TARAN SINGH BHARATI**

Supervisor's Name : **Dr. RAJENDRA KUMAR**

Department : **COMPUTER SCIENCE**

Faculty : **FACULTY OF NATURAL SCIENCES**

Research Title : **SECURITY ENHANCEMENT OF MOBILE AD-HOC NETWORKS USING INTRUSION DETECTION SYSTEM**

Whether we are business man, corporate employee, researcher, student, scientist, and a common person, most of us people can be seen using mobile gadgets like laptops, PDAs, mobiles etc. They allow us to be connected with the rest of the world for sharing the information. Hence the security of the mobile devices is of the prime concern so that the confidential information should reach to the intended people only. In no case impersonation of the identity and modification of the information should take place.

There are some fixed infrastructure networks like LAN, MAN, and WAN because they use the fixed infrastructure like nodes, server, and software etc. They are good in operations and in performance when they use wired connections. But in wireless networks, nodes are connected together with help of wireless connections like, infrared, microwave, leased lines, ISDN, and satellite. In wireless networks the transmission and reception of the messages is done through the antennas. When data moves in an open environment, there is no control on it. In open environment there are so many contaminations exist like Noise; mixing of unwanted and undesirable messages into the actual message. Interference which leads to the security laps because of interference of the other messages. Distortion- because of lack of bandwidth of the channel and sampling, message signals overlap each other. Magnetic field of earth - it also creates disturbance in the operations.

In the some emergency situations like natural disaster, catastrophic situation, flood, catch fire etc., network of fixed infrastructures get damaged and operations are disrupted. In order to provide the services in such situations, the mobile gadgets form, a small, for time being, infrastructure less network named Mobile Adhoc Network (MANET). In MANETs nodes themselves have to cooperate to each other to perform the network operations. MANETs have some design issues also: lack of Central Controlling Authority, lack of Fixed Infrastructure, Limited Computing Capabilities, Limited Power Backups, Limited Bandwidth, Dynamic Topology, and Security etc.

Since MANETs work in wireless and open environment, hence they are more susceptible to the vulnerabilities and to the attacks. Attack is any activity which compromises the system security. There are two types of attacks; Active Attacks- in which attacker is capable of modifying the messages, Passive Attacks- in which attacker is able to see the contents only.

Attackers are of three types; Masquerade- internal people who misuse their old privileges i.e. ex-employee fired from the job and she knows all the passwords etc. for some time, Misfeasor- these are the outsider people who try to insight you or sometimes harm you, and Clandestine- they may be either insiders or outsiders willing to insight un-authorizely.

Intrusion Detection Systems detect intrusions in the system and send alarming messages so that protective or corrective action can be taken by the system administration. An IDS has the following types on the basis of their place of installation; Host-based IDS- it is installed at every host in the network. It inspects the intrusions into the local host; Network-based IDS- it is installed in the routers or in the gateways. It inspects all the messages which pass through these routers or gateways.

A general IDS has three components; Data Collection Unit- this component is responsible for collecting the intrusion related data from all nodes; Intrusion Detection Engine- an intrusion detection process is applied here to make sure that intrusion has taken place into the network and; Alarming Unit- if something suspicious is noticed, an alarming message is sent to all the nodes so that preventive and corrective actions can be initiated.

Basically all IDSs are classified into the categories namely Anomaly-Based Detection-here irregularities in the operations are watched; Misuse-Based Detections-here a watch is kept at the attempt of the user for monitoring the misuse of the privileges of the user.

This Thesis focuses on the security issues of IDSs despite of having many intrusion detection methods. The security of the MANETs can be enhanced: with the help of Agents- by using the autonomous intelligent agents, by using the Cryptosystem- by using advanced public key cryptosystems, and by improving the Key Management Techniques- by using the best and hybrid key management techniques for all keys i.e. session, public, master key, encryption, and decryption keys etc.

The performance of the Intrusion detection system depends on the functioning of its all components. Hence emphasis is given on the intrusion detection techniques and message communication, and key management process. Each intrusion detection techniques has its own advantages and disadvantages i.e. statistical based, anomaly based, signature based, rule base, machine learning based, fuzzy logic based, game theoretic etc. Anomaly based and signature based detections are the two main basic detection techniques. Misuse based techniques are better because they minimize the false positive and false negative detection. While signature based detection techniques are better for identifying the intrusions whose signatures or patters are already stored into the database.

As a first contribution, the security of MANETs is enhanced by using the cryptosystems and distributed 3-phase commit protocol and communication is made secure. As a second contribution, the mobile agents with no manager are employed to achieve intrusion detection efficiently. The security is enhanced in the respect of mutual exclusion, fault tolerance, consensus, and secure communication. As a third contribution, machine learning techniques and state transition analysis are used to detect the. As a fourth and the last contribution, the security of MANETs is improved by enhancing the key management techniques by using the secret sharing techniques. The proposed work is tested on MATLAB R2010a and NS2.