CHAPTER 1

INTRODUCTION

In this chapter we discuss the project overview, problem statement, aim of project, motivation for the project, proposed system, implementation and organization of our report.

1.1 SECURITY ATTACKS

Network Security Attacks can be classified into two broad categories namely passive and active attacks. A passive attack does not disrupt the operation of the network; the adversary snoops the data exchanged in the network without altering it. The requirement of confidentiality can be violated if an adversary is able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of overcoming such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overhead.

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. Active attacks can be classified further into two categories, namely, external and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewall.

Internal attacks are from compromised nodes that are actually part of the network. Since the adversaries are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.

The security attacks can be on any layer namely MAC layer, Network layer, Transport layer, Application layer, and some other attacks. The classification of security attacks is depicted in the Figure 1.1.