ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

INTRUSION DETECTION FOR MANETS

Insha Majeed*, Insha Altaf
*Dept. of Inforation Technology National Institute of Technology Srinagar, J&K, India
Dept. of Information Technology National Institute of Technology Srinagar, J&K, India

DOI: 10.5281/zenodo.557136

ABSTRACT

Mobile Ad hoc networks are playing very important role in the present world. They are applied to several popular wireless technologies including cellular phone services, disaster relief, emergency services, battlefield scenarios, and other applications. MANETs are decentralized networks, and the network topology is unpredictably dynamic because of node mobility. As a result, mobile nodes in MANETs act as both hosts and routers since MANETs are decentralized; all mobile nodes need to discover the dynamic topology and deliver messages by themselves. MANETs rely on the cooperation of all mobile nodes in the network to ensure reliable routing services in the presence of dynamic topology caused by their mobility. The dynamic and cooperative nature of MANETs presents substantial challenges for network security. Therefore, sufficient protection should be provided to secure MANETs to guarantee the integrity of routing messages and availability of routing services. In other words, the goal of this dissertation is to examine how to secure the routing services of MANETs in order to provide reliable communication among nodes.

KEYWORDS: Access control, routing services adhoc networks, multi authority, secure data retrieval.

INTRODUCTION

A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. The network is an autonomous transitory association of mobile nodes that communicate with each other over wireless links. Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's send range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. The devices or nodes are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes. These mobile nodes establish the routing tables by exchanging routing messages with each other and then delivering data packets for others. Generally, MANETs rely on the cooperation of all mobile nodes in the network to ensure reliable routing services in the presence of dynamic topology caused by their mobility. The dynamic and cooperative nature of MANETs presents substantial challenges for network security.

SPECIAL SECURITY ISSUES FOR MOBILE AD HOC NETWORKS

In addition to authentication, integrity, confidentiality, availability, access control and non-repudiation, which have to be addressed differently in a mobile, wireless, battery-powered and distributed environment, mobile ad hoc networks raise the following security issues:

Cooperation and fairness: There is a trade-off between good citizenship, i.e. cooperation [2], and resource consumption, so nodes have to economize on their resources.

At the same time, however, if they do not forward messages, others might not forward either, thereby denying them service. Total non-cooperation with other nodes and only exploiting their readiness to cooperate is one of several boycotting behavior patterns.

Therefore, there has to be an incentive for a node to forward [illegible] stined to itself.