Performance Evaluation of Intrusion Detection System by Applying Routing Protocol on Mobile Ad-hoc Networks

Syed Muhammad Hassan Zaidi and Dr. Manzoor Hashmani

***Abstract*— A Mobile AdHoc Network (MANET) is a network of nodes that communicating with each other without help from a fixed network infrastructure. Securing MANETS is an important part of deploying and utilizing them, since they are often used in critical applications like Commercial, Military, and Private sector where data and communications integrity in important. To obtain an acceptable level of security, conventional security solutions are supposed to be attached with an intrusion detection mechanism. In this thesis, we analyze few wireless Adhoc security attacks and vulnerabilities relative to topology control schemes and evaluate their performance under hostile environments. We propose a Distributed Intrusion Detection System (DIDS) that incorporates rule- based cluster topology relevant to Mobile Adhoc networks (MANETs) to determine their security/performance in application specific environments. DIDS draws inferences of intrusion by comparing anomalous patterns from packet traces of transmit and receive signal powers, ratio of packet arrival rates and anomaly in radio receiver packet power thresholds using buffer window count. We evaluate intrusion detection mechanism on a jammer attack and observe the effect on the network throughput. Our approach is simulated using the OPNET simulator. Simulation results show that the detection capabilities of scheme under a denial of service (DoS) (jammer) attack, increases the bit error rates, increase in transmit delay responses and considerable decrease in both the signal to noise powers and the average network throughput due to the presence of jammer attack which forms the baseline for analysis required to maintain energy efficiency and improve security in Adhoc network.**

I. INTRODUCTION

A wireless Adhoc Networks has grow to be an significant technology in recent era because of the continuously increase of wireless devices, e.g., Mobile Adhoc networks (MANETs) and Wireless sensor networks (WSNs) are extremely susceptible to attacks due to their open medium, dynamically changing network topologies, lack of centralized monitoring points, and lack of a clear line of defense[2]. A Mobile Adhoc Network (MANET) is a network having set of wireless mobile nodes. Nodes communicate with each other without having centralized base stations.

hassandit@gmail.com,mhashmani@iqra.edu.pk
Iqra University, Main Campus, Shaheed Millat Road, Karachi.

In this network, each node acts both as a router and as a host. Multiple hops are desired to exchange data between nodes due to the limited transmission range of wireless network interfaces. In this research work, we investigate and report the progress in developing Intrusion Detection System (IDS) capabilities used for wireless adhoc networks. We analyze how to improve the anomaly detection technique to provide more details on attack types and sources for a number of well-known attacks. We study the attack type, certain vulnerabilities and their effect on the network. These rules are helpful to identify the attacker when an anomaly is reported in some cases. We demonstrate the effect of anomalous patterns detection on a jammer attack model using the proposed DIDS scheme and evaluate the jammer response on the network throughput. OPNET Simulator is the leading simulator especially for network research and development. OPNET gives a great flexibility to design and study networks communication, devices, protocols, and applications [1]. It has a graphical interface to build models for different networks entities from physical layer modulator to application processes. MANET module is included to the basic OPNET modeler to simulate Adhoc routing protocols of AODV (Adhoc on-Demand Distance Vector Routing), DSR (Dynamic Source Routing) and TORA (Temporally Ordered Routing Algorithm). We conduct simulation analysis in order to evaluate the detection capabilities of DIDS in the presence of the jammer attack.

II. MOTIVATIONS AND DIRECTIONS

The vulnerability of adhoc networks to different forms of internal or external attacks such as jamming attack, due to resource constraints, energy depletion, lack of data diversity and the propagation medium [8] of the wireless network remains a great challenge in security deployment. Due to scalability nature and lack of energy efficient implementation of adhoc and sensor networks, the architectures for the purpose of security designed for large size adhoc networks becomes infeasible for deployment. However, any architecture without proper application or design considerations developed with intrusion detection-awareness creates room for unprecedented malicious attacks. Bringing to focus a potential adversary such as the Denial of Service (DOS) attack that has a wide range of attack primitives at its disposition in order to manipulate network subsystems and maliciously take control; the aftermath resulting in data corruption, disruption, repudiation, jamming and other forms