Intrusion detection systems in security

Abstract

Modern world provide the latest system of internet which is disputing for the security of information systems. The defense of information is becoming the part and parcel for internet day by day. Current Intrusion Detection systems cannot make sure to detect attacks in real time environment as it has insufficient ability to do that. To cope with latest invasions attack, database should be rationalized time to time. Systems fall squat to recognize fresh attacks due to lack of domain familiarity. If there is any lack of domain familiarity, Intrusion Detection system can fall squat to recognize new attack.

In Wireless and AD HOC networks, Information security revolves into imperative role. Possibility of vulnerability to attacks rises as for their flexible nature. A few intrusion detection schemes suggested for where wired networks are not sufficient for Wireless and AD HOC networks. In AD HOC networks, it is significant for such slant that is proficient to intellect any variety of eccentric actions.

In fact, it is out of ability of technology to encumber each single contravention. In this thesis I am going to model a IDS using time series techniques for wireless AD HOC network by which it can detect intruders. Time series is a technique by which we can detect intrusion. To form the rapid change of time series data, the technique applies the Auto-Regressive (AR) method, and achieves in order hypothesis test to detect the intrusion. By means of time and location correlation, the systems and modes verify the existence of anomalous commotion, as well as its occurring time and location. It is proved and demonstrates that the experimental outcomes perform better with the recommended method in detecting the intrusion.

Acknowledgements

Introduction

Security is the major issue for the wireless and Mobile AD HOC network because it is using “ AIR” as media . Research project address this part as Intrusion Detection. Mounting world cannot imagine even for a single day without computer and computer is basis on internet. Nowadays secure information of internet is becoming very high priority. Modern world emphases in a way by which it can be protect the data and information from any illicit and unauthorized access.

Intrusion Detection Systems (IDS) can be differs in various techniques and advance with the objective to detect suspicious traffic in dissimilar ways. There are two significant categories of intrusion detection systems. One is called network-based intrusion detection system (NIDS) and the other one is host-based intrusion system (HIDS). The existing system that detects attacks based on looking for specific signature of identified threats. It reveals particularly that we may have two sets of data; one is of usual and common data and other one apprehensive and suspicious data. So intrusion detection systems match the data with the set of normal and suspicious data and if the deference between the two set is above a threshold value then intrusion is detected.

Currently, if Internet infrastructure assault such as man in the middle attack, denial of service attacks and worms infection, have become one of the most serious threats to the network security [1]. It is very likely feasible to detect the attacks and abnormal behaviors if there is sufficient and efficient method and technique exists for monitor and examine, and it can not only make sure proceed warning of potential attacks, but also help out to recognize the reasons, source and locations of the anomalies. By this way, it may assist to restrain the attacks, sooner than they have enough time to broadcast across the network. This document represents the method, in support of detecting network anomalies by analyzing the unexpected change of time series data . With the comparison of other anomaly detection methods. We have focal point on the vibrant behavior of the network rather than using the static models. Our process and method concerns the Auto-Regressive (AR) process to model the rapid and unexpected change of time series data, and performs sequential hypothesis test in contrast with two adjoining non-overlapping windows of the time series to detect the anomalies

Aim and Objectives

Aim:

The aim of this thesis is to design and implement a IDS for wireless network to detect and monitoring malicious activities by using time series analysis techniques.

Objectives:

- Review current intrusion detection system
- Analyze the data with suspicious activities
- Design appropriate system architecture for IDS
- Implement the system using time series analysis
- Testing and evaluate the system.
- Future work

Academic Background

Intrusion detection system

In general, an Intrusion Detection System is not an antivirus program to detect virus or not a network logging system for detecting complete vulnerability or not a vulnerability tools which can check bus, flaws and network services.

Intrusion Detection System (IDS) is a software or hardware by which we can detect hackers, male ware and bots. There are few types of Intrusion detection system like Network Intrusion Detection System, Protocol-based Intrusion Detection System, Application protocol-based Intrusion Detection System and Host-based Intrusion Detection System etc.

Now a day, wireless network is increasing dramatically. We are trying to make everything which can connect to internet without wire. Compare to wired network, it is easy to capture the channel of wireless network for an intruders.

Why We Need Intrusion Detection System

Why we need IDS

An overview of current intrusion detection system

Wireless networks are extremely vulnerable to man in the middle attack, DOS and other attacks because they depend on a shared communication medium as well as depend on limited resources. Wireless ad hoc networks do not have a central control as wireless LANs and they also provide a dynamic topology. This increases the complexity of the intrusion detection schemes in ad hoc networks.

Network Anomaly Detection Using Time Series Analysis

According to Qingtao Wu and Zhiqing Shao’s research paper,

This research paper explain to detect network intrusion using time series analysis.

Anomaly and sequential detection with time series data

Intrusion Detection Alert Flow Processing Using Time Series Analysis Methods

Processing intrusion detection alert aggregates with time series modeling

Compare Wired and Wireless Intrusion Detection System (Dragan Pleskonjic)

In wired network,

Intruder should be attached physically. Intruder needs a direct connectivity into the network.

It is possible to trace the intruder

In wireless network,

Intruder does not require any physical connection. So Intruder can stay everywhere.

There are no difference between internal and external network so it is difficult to specify the attack whether it is insider or outsider.

The border of Defense of wireless networks is weak compare to wired network.