AN EFFICIENT APPROACH OF DATA AGGREGATION ALONG WITH OUTLIER DETECTION BASED LAYERED APPROACH FOR INTRUSION DETECTION TECHNIQUES

Sana Sheikh, Prof. Angad Singh

Department of Computer Sc. &Engg., NRI Institute of Science and Technology, RGPV, Bhopal

ABSTRACT

With the grow of time, data size also gets bigger and bigger. This big data size creates a performance issue with the intrusion detection system. Intrusion detection systems are huge in numbers but with the increasing of their data size these intrusion system gets stuck with their performances. Here this article talks about the Intrusion Detection system performance along with its key issue which is size of web log data. This work is implemented in MATLAB and work on two aspects Data Aggregation and Intrusion Detection System.

Keywords: Intrusion Detection, Data Aggregation, Accuracy.

1. INTRODUCTION

An Intrusion detection system (IDS) is designed to detect unwanted attempts at accessing, disabling of computer are associate with the network, like as the Internet. Intrusion detection plays a key role in the area of network security, so an attempt to apply the idea in WSNs makes a lot of sense. Intrusion, i.e. unauthorized access or login (to the system, or the network or other resources); intrusion is a set of actions from internal or external of the network, which violate security aspects (including integrity, confidentiality, availability and authenticity) of a network’s resource. There are two approaches: misuse detection and anomaly detection. Misuse detection identifies an unauthorized use from signatures while anomaly detection identifies from analysis of an event. When both techniques detect violation; they raise an alarm signal to warn the system. Wang divides intrusion detection techniques into single-sensing detection and multi-sensing detection. In single-sensing detection, the intruder can be successfully detected by one sensor. While in multisensing detection, multiple collaborating sensors are used to detect the intrusion.

The ultimate aim of the intrusions detection is to find out the unauthorized use, abuse and misuse of the system (PC). the intrusion detection is taken as the automatic system for the purpose of the detection of the computer system, the IDS secure the computer system from the both of the side external intruders and the insider intruders. There are some other computer security system like as firewall and cryptography along with the IDS for preventing the system from the misuse. Now there is a rapid growth in the work process of IDS and also shown in [1], [2]. Some other scientist also discover some general computer immune model for the virus detection and the intrusion[3], [4], [5], [6]. The positive results from these models have boost up the computer scientist to become familiar with the concept of the human immune system.

This paper determines the important features of human immune system, which become suitable to work with the novel network intrusion detection model. Various unknown qualities of the human immune system, which works on searching the intruding pathogens, are seriously analysis and the benefits of dealing with such kind of functions for the network intrusion detection are implemented

2. INTRUSION DETECTION TECHNIQUES

In this section we explain the intrusion detection techniques. Basically, there are two techniques in IDS: Anomaly based and Signature/Misuse based intrusion detection. We also explain the Target Monitoring and Stealth Probe techniques later in this section.

A. Anomaly based intrusion detection
Anomaly detection method is designed to reveal the footprint of behavior that are far from normal and anything which deviates in a greater amount is taken as a possible intrusion. Anomaly detection can be categorized into static and dynamic [7]. In static anomaly detector it is assumed that a portion of the monitored system remains constant or static. The static portion comes with two parts of a system: Static portions which taken as a binary bit string or a set of such strings (such as files). The system code where data remains unchanged. If there is some change in the portion from the actual one, it is due to the fault arises or any intruder which change the static portion of that system, the Static Anomaly detectors works on checking the data integrity

In dynamic anomaly detector the definition of behavior is included. System behavior is refers a series of distinct events (or partially ordered sequence). Like as, audit records obtained from the operating system are being utilized by IDS to express the events of interest. Here the behavior is being analyzed when audit records are formed by OS. Events perhaps take place in a tough sequence. Like as with distributed systems, partial ordering of events is more appropriate.

Anomaly based intrusion detection is useful for detecting attacks like:
1) Misuse of Protocol and Service Ports
2) DoS Based on Crafted Payloads
3) DoS Based on Volume (DDoS)
4) Buffer Overflow
5) Other Natural Network Failures

B. Misuse/Signature Based Intrusion Detection

The second major category of IDS is known as misuse detection also express as signature-based detection due to which alarms are generated depended on specific attack signatures. These attack signatures form specific traffic or activities which depended on familiar intrusive activity.

The following are the two techniques in misuse detection:
a. Expression matching

The simplest form of misuse detection is expression matching, which searches an event stream (log entries, network traffic, or the like) for occurrences of specific patterns/signatures. A simple example would be “*/etc/passwd” - this checks for something that looks like an HTTP request for the Unix password file. Signatures can be very simple to construct, however especially when combined with protocol-aware field decomposition.

b. State transition analysis

State transition analysis models attacks like a network with transitions (matching events) and states. Every single analyzed event deals with the measured state machine instances (each representing an attack scenario), possibly causing transitions. This approach permits complicated intrusion scenarios to be displayed in a simplified manner, and able to find out the distributed attacks or slow, but it’s hard to express elaborate scenarios.

c. Target Monitoring

Any change or modification in the target objects are reported by the Target Monitoring Systems. This is usually done through cryptographic algorithm that computes a Crypto checksum for each target file [7,1-8]. Changes such as file adjustment or program logon which results in changes in the crypto checksum are reported by the IDS. This type of System is the easiest to implement, due to less need of constant monitoring from administrator. Integrity checksum can be calculated at our desirable interval, and sometimes all files or just the mission/system critical files.

d. Stealth Probes

Stealth probes collects and related the data for the detection for a long time duration mostly known as “low and slow” attacks [8]. Attackers, for example, will check for a system vulnerabilities & open ports for 2 months duration, and wait for the coming next 2 months for the purpose of launching the attacks. They take a wide-area sampling and attempt to discover any correlating attacks.

3. LITERATURE REVIEW

Numerous research works are going on these days in IDS for better improvement in the performance of host system as well as networks and its components. The already accomplished research work in the contrast of Mobile Agent depended Intrusion Detection Systems (MA-IDSs) have central conceptualization oriented over its feature constraints like design architecture, technique used to develop, strength and weakness also. All these aspects are going to be explored in this paper. Intrusion is an undesirable act which leads to losses of different magnitude in different forms.
Intrusion detection (ID) is a part and parcel tool to detect the unauthorized and suspicious activities of intruders that can compromise the security aspects (i.e. Confidentiality, Availability, Integrity, and Authentication) of data or information as well. In [9] IDS with the integration of Mobile Agents is presented to look after the anomalies found and respond back by taking appropriate measures using agents.

Previously, a lot of works has been done to detect the network intrusion such as anomaly based or misuse detection. In this section we are describing the several approaches developed or implemented by different author and researcher that are explained below:

M. Chandra sekhar, K. Raghuveer et al. proposed a technique which is divided into four steps: initial step, k-means clustering is used to generate different training subset then based on the obtained subset, various neuro-fuzzy data model are trained. Consequently, a vector for SVM classification is obtained and in last, classification using radial SVM is applied to detect the intrusion occurred or not. To demonstrate the applicability and ability of the new method, the result of KDD dataset is confirmed in which it shows that the proposed methods produce better result than the BP, multiclass SVM and other approach such as decision tree etc [10].

4. PROPOSED WORK

In this session, it provides the details and description of proposed method mention in this article. This illustrates the use of this Proposed Work and how it works for the considered datasets. To maintain the Intruder Detection Through clustering and classification result. The methodology for evaluating the above objective of the proposed technique is also discussed in this session. The proposed method of Data Aggregation and Intrusion Detection is discuss in algorithm mentioned bellow (fig 1).

![Proposed algorithm for Intrusion Detection and Data Aggregation](image)

5. RESULTS AND ANALYSIS

The system used for execution of the proposed method for intrusion detection by clustering is as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Core 2 Duo</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>32 Bit Operating System</td>
<td>Windows 7</td>
</tr>
</tbody>
</table>

KDD 99 dataset is chosen and taken for our experiments. In this , a software to detect network intrusions protects a computer network from unauthorized users, including perhaps insiders. The intrusion detector learning task is to build a predictive model capable of distinguishing between “bad” connection.

Parameters which are used for evaluation of this work are:
A. Achieved Aggregation Ratio
B. Accuracy
C. Detection Rate
6. CONCLUSION

There are two aspect of the work which is proposed in this article. These parameters are mainly of two categories. First is related with data aggregation and another is related with Intrusion detection. From the table II and II along with the fig 2 and 3, it is very conveniently shown that the proposed algorithm of data aggregation works better than existing work. Whereas there was no intrusion detection system in existing work so proposed work accuracy works.

REFERENCE


