

# Data Mining IN IDS

Dr. Jala Atoum, Mr. Ayham Nazir Alolabi

New York Institute of Technology [NYIT]

## ABSTRACT

This paper provide an improvement of the intrusion detection system using data mining in a way to reduce the analysis time and the false alarms, also briefly review of the intrusion detection with its several techniques, and the data mining basics with useful algorithm to know, related work is mentioned in purpose to declare the difference between my contribution and those works

**Keywords:** Instruction Data Mining, Intrusion Detection System.

## 1 INTRODUCTION

Intrusions are everywhere; the problem is detecting these intrusions earlier to have the better circumstances to prevent later, the earlier you detect an intruder the less damage you will have. This is always the problem which what we all want to solve for our systems, so far Intrusion Detection Systems “IDSs” are designed to do the job, but like anything it has to be improved in order to detect intruders earlier and faster with efficient results which is the problem we face these days, it is called the false alarms.

Intrusion detection is the process of monitoring and analyzing the events occurring in a computer system in order to detect signs of security problems (Bace, 2000). Intrusion Detection Systems has the additional job of triggering alarms toward this security problems and some of it automated in the role of triggering or doing an action in behave of the network administrator, here it comes the problem declaring itself, the false alarms.

However, intrusion detection is not yet a perfect technology (Lippmann et al., 2000; Allen et al., 2000).

That definitely gave the role of data mining (Section 3) the opportunity to introduce some contributions to the intrusion detection technology.

But the problem remain in extracting the data as fast as possible and with the least consuming resources we can, and in parallel with using this new data input to our intrusion detection systems, in the purpose of solving this problem, this paper will introduce an idea (Section 5) of reducing the time of the data mining and specially reducing the false alarms (Section 2).

Simply, when you are facing too many choices in your life you start by eliminating them

one by one to finally determine the right solution, this will be applied in a new methodology using an algorithm I designed on use of data mining in intrusion detection using a certain order of data mining algorithms (Section 3) on a data set, by comparing, grouping and validating the attack patterns then forming a completely reduced data set to produce the input to the IDS within the right format and the least information and pattern to look and dig in.

In order to get finally understand the idea, I assumed that the reader already have a little bit knowledge of the intrusion detection and data mining but in order to make this paper as self-contained as possible, but because given the abundance and the interdisciplinary nature of the topic, it was not possible to write a complete details on both intrusion detection and data mining, so you will be introduced to intrusion detection in section 2. Section 3 is about data mining basics. Section 4 surveys related research project and an article that almost have the same approach of thoughts, the contributions is in section 5...

To receive full document contact  
UbiCC Information Desk:  
[info@ubicc.org](mailto:info@ubicc.org)