www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 19063-19064

Review on Intrusion Detection and Prevention System

Sayalee Shinde [1], *S.V.Athawale* [2]

[1]Student, Department of Computer Engineering, AISSMS COE Pune, Maharashtra, India
sayaleeshinde1993@*gmail.com*

[2] Assistant Professor, Department of Computer Engineering, AISSMS COE Pune, Maharashtra, India
svathawale@gmail.com

Abstract: ***Nowadays internet and network technology have been spread rapidly, cyber-attack increasing accordingly. In this paper we propose a network based Intrusion Detection and Prevention System (IDPS) which can detect many attack types that can prevent network systems from network attack. Our system is simple that can be used with several machine learning algorithms. We test the IDPS using machine learning algorithm in online network environment. The result of the test shows that our IDPS can distinguish normal attack activities from main attack types. We apply C4.5 machine learning technique in our approach to consider unknown or new attack types.***

Keywords: IDS (Intrusion Detection System; IPS (Intrusion Prevention System); real time detection; network security system; data mining.

1. INTRODUCTION

These days internet plays important role for communication. By using world wide data and lot of information on internet people can communicate with each other around the world. When we use internet services we do not know who are attacking on the computer network. These network attacks can slow down the network services for long period of time. The active denial of service attack (DoS) and the port scan attacks are the main attack types in the network. So, it is necessary for users and network administrator to detect these attacks before they slow down services in the system. In this paper we proposed an Intrusion Detection and Prevention System (IDPS) which effectively protect the network services from the attackers in the internet.

2. LITERATURE SURVEY

In the literature review [1], Maheshkumar Sabhani and Gursel Serpen used pattern recognition and machine learning algorithms on four attacks found in the KDD dataset. [2], K.Labib and R.Vemuri used self-organizing map which classify normal data and DOS attack evaluated by different characteristics of visualization.
In [3], Morteza Amini used unsupervised neural network for the detection of known and new attacks in the network traffic. It evaluates the approach using 27 types of attacks and observed 97% precision using ART nets 95% precision using SOMNETS. In [4], P. Sangkatsanee, N. Wattanapongsakorn an d C. Charnsripinyo used Real-time Intrusion Detection System (RT-IDS) using decision tree technique to classify an online network data. It can also classify normal network activities and main attack types consisting of probe and denial of service (DoS).

3. METHODOLOGY

3.1 Machine Learning techniques

There are various machine learning techniques are available for data classification. Here we consider the several well-known techniques which are decision tree, ripple rule, random forest and Bayesian network. These are supervised learning technique so that it has to be trained with known input dataset for classifying and detecting unknown data.

3.2 Intrusion Detection and Prevention System Model

The Intrusion Detection and Prevention system (IDPS) consist of processing part, classification part and protection part. In the beginning system detect the packet from Ethernet and transfer packet data to preprocessing part for capturing important features to form a data record within a certain period of time. Then the preprocessing data is sent to the next part which is classification part to determine type of attack after identifying the attack the result is sent to protection part. The protection part block network data packets by using IP table if network attacks are detected.

3.2.1 Preprocessing part

The preprocessing part use the Jcap library of java language to get the packet information between source destination IP pair which includes IP header, TCP header, UDP header and ICMP header from the Ethernet interface card.

3.2.2 Classification part

In classification part, it takes each preprocessed data in order to classify whether it is normal data or attacked data. The classification is done by machine learning algorithm written in Java. The result of the classification will be saved into log file and also sent to the protection part.

3.2.3 Protection part

If the network attacks are detected the network data packets will be blocked by using IPtable. The result from previous classification part used for making decision on which operation to be used. If the classification result is normal system does nothing.

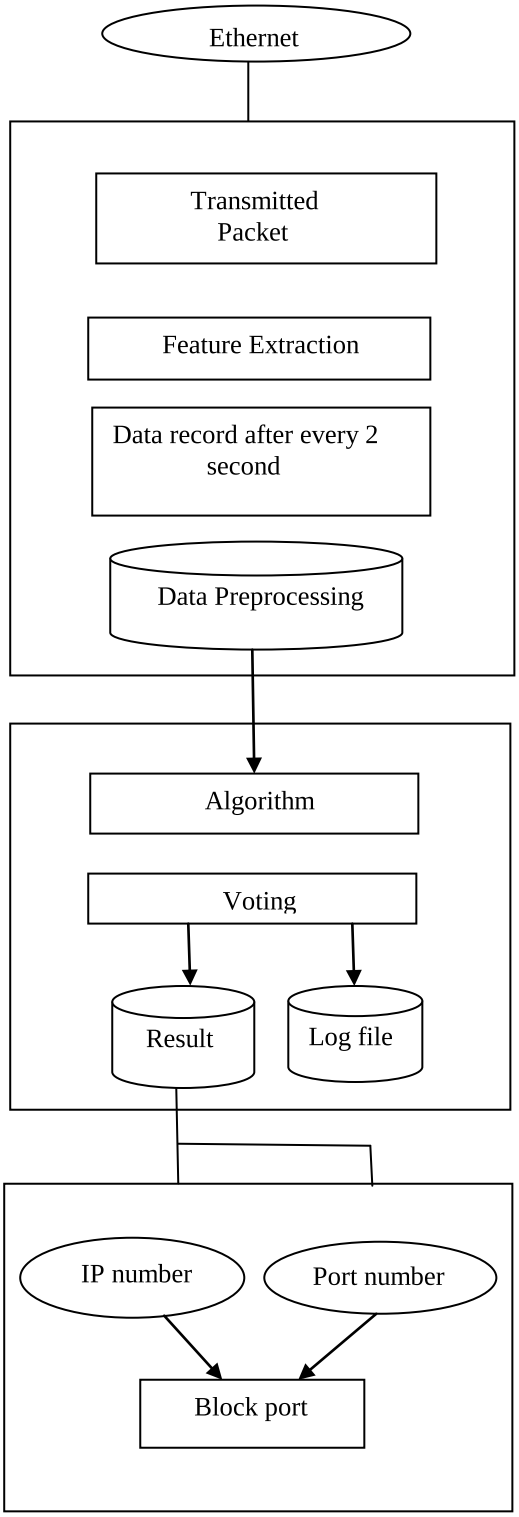

FIGURE 1. INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) PROCESS

4. CONCLUSION

This paper proposed a network based Intrusion Detection and Prevention system (IDPS) using machine learning algorithms to identify and classify network attacks. Decision tree, Ripple rule, Random forest and Bayesian network these well-known machine learning algorithm and only 12 features of network traffic are used to detect and classify 17 attack types of probing and denial of services. The result shows that the Intrusion Detection and Prevention system (IDPS) offers high detection rate.

In future work, the unsupervised learning algorithm with the help of new techniques work as hybrid IDPS approach which helps to improve the performance of anomaly intrusion detection.

References

[1] M. Sabhnani and G. Serpen, “Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context”, Inter Conference: Machine Learning, Models, Technologies and Applications (MLMTA), 2003, pp. 209-215.

[2] K. Labib and R. Vemuri, “NSOM: A Real-Time Network-Based Intrusion Detection System Using Self-Organizing Maps”,Networks and Security, 2002.

[3] M. Amini,, A. Jalili and H. Reza Shahriari,, “RT-UNNID: A Practical Solution to Real-Time Network-Based Intrusion Detection Using Unsupervised Neural Networks”, Computer & Security 25, 2005, pp. 459-468.

[4] P.Sangkatsanee,N. Wattanapongsakorn an d C. Charnsripinyo, “Practical real-time intrusion detection using machine learning approaches”, Computer Communications (34), 2011, pp. 2227-2235.