



Intrusion Detection System Using Neural Network

¹P. Sathish Kumar, ²P.C. Kishore Kumar, ³C. Arul Stephen, ⁴Arun Raaza and
⁵J. Antony Veera Puthira Raja

^{1,2,3,4,5}Department of Electronics and Communication Engineering,

Vels Institute of Science Technology and Advanced Studies (VISTAS),
Chennai, India.

Abstract

Almost of them doing job through internet like, online business, shopping, transfer money, voice call, online application filling data in hospital, booking bus ticket, train, apply jobs etc., such way may attack intruder easily if not secure. Example mobile apps getting updated daily, intrusion also being upgraded rapidly. Intruder can monitor or detection with the help of IDS. Two type of IDS are software or hardware and it helpful in safe guard the entire network or local network, the activities of the system and also helpful in finding the harmful operations. As the hacking techniques getting stronger daily so for improve the IDS but still not having strong intrusion detection system. In this paper we present IDS's various types of attacks and it's features to detect the intrusions on a network and possible ways to secure those intrusions.

1. Introduction

In the past few years computer networks have used very peak or booming and even much risks and chances of malicious intrusions is increasing. Example few real time incidents are in the month of February 2000, DOS attacks are against global largest commercial web sites famous companies are yahoo.com and amazon.com. Next incident on July 2001, Code Red virus sweeps across many countries affected approximately 1,50,000 computers within 14 hours. Cyber space is rapidly used by head of the malicious teams task is credit/debit cards, financial bank account, Customer data and other details of financial for fraudulent transactions. Offline and online cheating is considered to be 3rd highest economic crimes prevalent in India according to world's economic crime survey in the year of 2011. In 2014 more than thousand million personal details were illegally accessed by intruders. The most widely accessed databases are health, financial, email and home address, and other personal identity. That is more than fifty-four percentage on year prior records. In Japan is topper list with the most elevated online banking malware attacks this quarter due to VAWTRAK. The US saw 5,000 malware attacks during the month, taken after by India at Three thousand attacks. Still continuously start developed in response to previous and nowadays intrusion on frequently famous online websites and networks, along with the particular eBay, Yahoo Mail, Face book, Google, NASA, the White House, NATO and All defense department. To troubleshoot this kind of problem have to identify and developed a software is called an intrusion detection system. It is software used for observing, protecting the network from malicious attacks. Any encounter movement or misbehavior is mostly announced to system administrator immediately. Malicious detection system can be classified are two types that is Network intrusion detection system(NIDS) and Host-based intrusion detection systems(HIDS). A system that monitor the attacks within a company or local systems used HIDS, while a system that detects malicious attacks from incoming network traffic is used as a NIDS.

2. Machine Learning

The artificial intelligent gains knowledge by training the data based on known aspects. Study and analysis is one of the machine learning processes that let on computer system to make realize after start compile as named by Arthur Samuel in 1959. Prediction is important rule needed future can define very easy way so research mostly focuses on Machine learning approach. ANN are used in various and import field utilization in control, robotics, weather forecasting, predict wind speed, load large number of data like medicine details, automatic driving control, system optimization, digital signal processing [1].

ANN classified into three types are supervised, Unsupervised and Reinforcement learning.

3. Single Classifier

The machine learning algorithm for developing IDS software. Which can also be used as a standalone classifier. Most of the machines learning techniques have deliberated in this work which was used as frequently used one-classifiers.

Neural Network

Artificial Neural Network is a processing element which was stimulated by human brains works. Neural networks are controlled by layers which are built using number of interconnected nodes. Then the Patterns are characterized to the network through the input layers which are used to communicate with one or more hidden layers. Then the hidden layers are link to an output layer to produce a discovery result as output [5]. The feed forward ANN shown in figure 1.

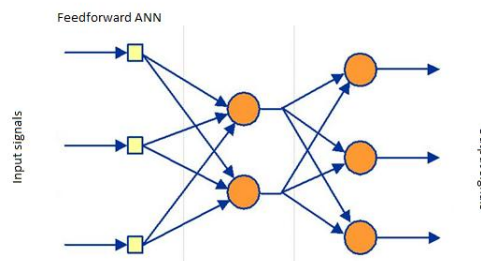


Figure 1

Fuzzy Logic

The restrictions are optimized to minor in fuzzy logic, where dual logic values are accurately zero (0) or one (1) which means in Fuzzy logic the degree range and statement can hold the value between 0 and 1.

4. Hybrid Classifiers

Both single and multi classifiers are combined a create a algorithm which is called as hybrid classifiers Using clustering procedures the pre-processing samples can be used to train the data for removing non illustrative training examples. The results we got from clustering procedures are used as training examples for pattern recognition in order to project a classifier.

5. Ensemble Classifiers

The system is better performance than a different classifier is known as weak learners. When a multiple low end performers begins to learn for greater implementations and improving the routine of a classifier expressively then it is called as Ensemble classifier. The higher count, capturing and enhancing are some mutual policies for uniting low end beginners. Superficially the

disadvantages of the classifiers get collected in the ensemble classifier and it will be keep creating an immersive performance in some consolidation. Examiners are fetching supplementary interested ensemble classifiers in routine.

6. Network IDS Tool

Network intrusion detection systems (NIDS) was placed in the top of the list and the inbound and outbound traffic from all devices in the network can be observed. But scanning all traffic could lead to the creation of bottlenecks, which impacts the overall speed of the network.

HIDS: Host intrusion detection systems run on separate machines or devices in the network, and provide safeguards to the overall network against threats coming from the outside world [10].

Signature based IDS: All the data stored in the databases are read using pre-configured and pre-determined software, this check for unwanted contents that are used by the intruders this is most likely a virus signature database protection [10].

Anomaly based IDS: The anomaly detection technique centers on the concept of a baseline for network behavior. This baseline is a description of accepted network behavior, which is learned or specified by the network administrators, or both. Events in an anomaly detection engine are caused by any behaviors that fall outside the predefined or accepted model of behavior [11].

7. Literature Review

Table 1

S.No	Name of the title	abstract	Result
1	Hardware Realization of Artificial Neural Network Based Intrusion Detection & Prevention System	in this paper, a new methodology towards implementing an Intrusion Detection & Prevention System (IDPS) based on Artificial Neural Network (ANN) onto Field Programmable Gate Array (FPGA) is proposed.	system that is highly useful for mankind and organizations (e.g., military, defense etc.) in today's world of network defenselessness.
2	Simulation of Denial of Service (DoS) Attack using Matlab	The proposed model is tested with the predefined source and target dataset to obtain desired or fluctuation in result and also to determine the kind of predefined DoS attack.	confusion matrix Successive rate 99% and Failure rate
3	NETWORK INTRUSION DETECTION SYSTEM USING FUZZY	In the proposed system, we have designed fuzzy logic-based system for effectively identifying the intrusion activities within a network.	90%
4	Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic	In this progression, here I have designed an Intrusion Detection System (IDS), by applying genetic algorithm (GA) and fuzzy logic to efficiently detect various	92%
5	Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm	This mutual information based feature selection algorithm can handle linearly and nonlinearly dependent data features. named Least Square Support Vector Machine based IDS (LSSVM-IDS), is built using the features selected by our proposed feature selection algorithm.	99%

Types of Network Attacks

Denial of service: The attacker makes the computing or memory resources too busy or full to handle legitimate requests or denies legitimate users access.

User to Root: The attacker, starting out with access to a normal user account, tries to gain root access and privileges.

Remote to User: The attacker gains access as a local user of the network

Probing(Scanning):The attacker scans the network to gather information or detect vulnerabilities[7].

Table 2

Attack Type	Class	Group	Sub attacks types
Normal	1	A	Normal
DoS	3	B	smurf, teardrop, pod, back, land, apache2, udpstrom, mailbomb, processtable, Neptune
Probe	4	C	ipsweep, portsweep, nmap, satan, saint, mscan
R2L	2	D	dictionary, ftp_write, guess_password, imap, named, sendmail, spy, xlock, xsnoop, snmpgetattack, httptunnel, worm, snmpguess, multihop, phf, wrarezclient, wrarezmaster
U2R	5	E	perl, ps, xterm, loadmodule, eject, buffer_overflow, sqlattack

8.Simulation Result

First Step1

Create number of nodes as per requirement then give connection between each node if it is trans and receiver go for duplex otherwise simplex connection . Choose agent require reliable communication use TCP otherwise UDP here I used TCP. After fixed all details include antenna simulated without malicious node generate normal data figure 2.

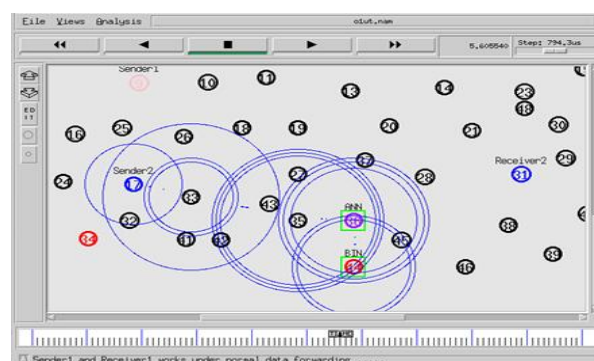


Figure 2

The result shown in Figure no.3 Detection of Intrusion

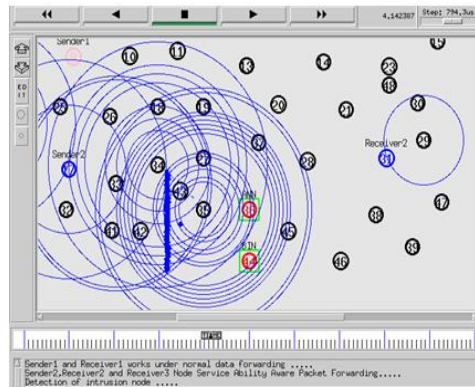


Figure 3

Energy consumption one of the important parameter shown in figure.4. that is comparison performance better than other algorithm.

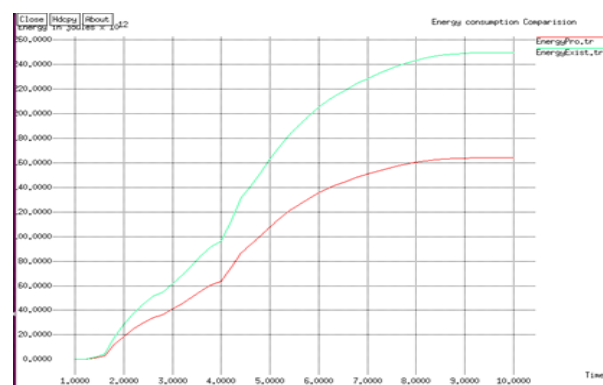


Figure 4: Packet Delivery Ratio

Other important parameter is Packet delivery ration figure.5 shown comparison performance better than other algorithm.

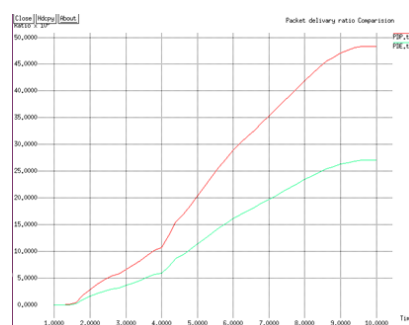
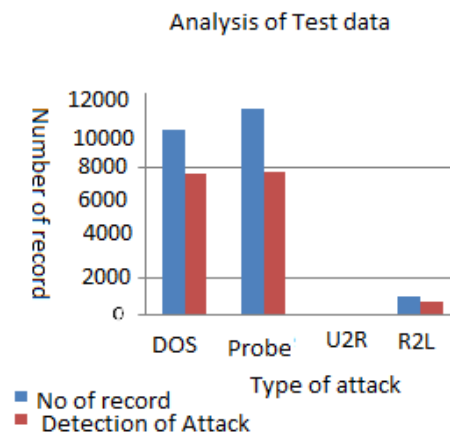


Figure 5



9. Conclusion

Safe guard computer and mobile data need to find suitable intrusion detection system model require. in this paper many algorithm, feature selection, model and types of attacks are discussed so our proposed work is detect intrusion using neural network, our model is give better detection rate, reduced false rate, energy consumption and packet deliver rate than other traditional algorithm.

References

- [1] Mitra P., et al. Unsupervised Feature Selection Using Feature Similarity, IEEE Transactions on Pattern Analysis and Machine Intelligence 24 (2002), 301–312.
- [2] Stolfo S.J., et al., KDD cup 1999 data set, Irvine: University of California, KDD repository, <http://kdd.ics.uci.edu>.
- [3] KDD Cup 1999 Intrusion detection dataset: <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>
- [4] Zainal A., et al. Feature selection using rough set in intrusion detection, Proc. IEEE TENCON (2006), 1-4.
- [5] Li J., Wang H., Yu J., Research on the Application of CRFs Based on Feature Sets in Network Intrusion Detection, Proceedings of IEEE International Conference on Security Technology, Hainan Island (2008), 194-197.
- [6] Mohammed A. Ambusaidi, Xiangjian He, Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm IEEE Transactions on Computers 65(10) (2016).
- [7] Tan Z., Jamdagni A., He X., Nanda P., Ping Ren L.R., Hu J., Detection of denial-of-service attacks based on computer vision techniques, IEEE Trans. Comput. 64(9) (2015), 2519–2533.

- [8] Hussain Ahmad Madni Uppal, Memoona Javed, Arshad M.J., An Overview of Intrusion Detection System (IDS) along with its Commonly Used Techniques and Classifications, International Journal of Computer Science and Telecommunications 5(2) (2014).
- [9] <https://machinelearningmastery.com/support-vector-machines-for-machine-learning/>
- [10] <https://opensourceforu.com/2017/04/best-open-source-network-intrusion-detection-tools/>
- [11] <https://searchsecurity.techtarget.com/tip/IDS-Signature-versus-anomaly-detection>

