ISSN 1533-9211

DOI 10.17605/OSF.IO/YAFW6

HYBRID INTRUSION DETECTION SYSTEM COMBINING OF SELF-ORGANIZING MAP AND BACKPROPAGATION WITH GANS NEURAL NETWORKS

LAMA SADI AWAD [1] and Dr. SAMI SARHAN [2]

[1, 2] King Abdullah II School of Information Technology, The University of Jordan Amman, Jordan.
Email: [1]Lam9220481@ju.edu.jo, [2]samiserh@ju.edu.jo

Abstract

The increasing complexity of network cyber-attacks has made intrusion detection systems (IDS) a vital component of network security. This paper proposes a hybrid IDS that combines Self-Organizing Map (SOM) and Back propagation neural networks with Generative Adversarial Networks (GANs) for improved network security. By utilizing the SOM and Back propagation neural network, the traffic patterns can be classified and anomalies can be detected. The detection system's accuracy is improved by training it with synthetic data generated by GANs. The expected results demonstrate that the hybrid system achieves higher accuracy and detection rates compared to using each individual component alone. GANs enable the system to learn and adapt to new attack patterns, making it a robust and effective tool for enhancing network security. The proposed system offers a hopeful method for the timely detection and prevention of potential network intrusions.

Keywords: Self-Organization Map; Back Propagation Artificial Neural Networks; Intrusion Detection; Generative Adversarial Networks.

I. INTRODUCTION

In General, the network security mechanisms are originally designed to prevent and detect any unauthorized manipulations of system data and resources. The need for designing a system that aims at protecting networks and computers from these attacks is becoming important. These systems are generally known as Intrusion Detection Systems (IDS).

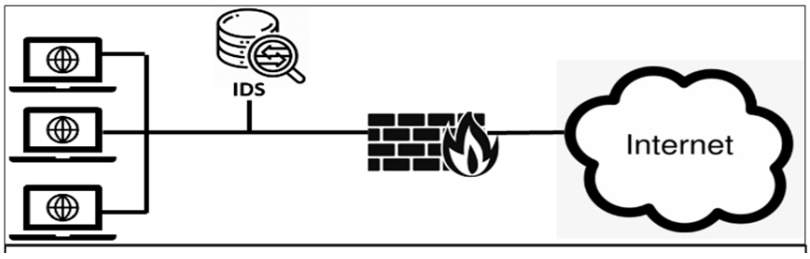

Fig 1: Intrusion Detection System as a network component

The design of intrusion detection systems has been a highly active field of research and development, primarily due to its significant impact on overall IT security. The detection reliability of malicious activities in a network and dealing efficiently with a large amount of network traffic are the most principal challenges that face intrusion detection. The precision and the stability of detection are the most important metrics that evaluate intrusion detection

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YAFW6

performance. Once IDS is installed on a network, it will collect information from different network resources, analyze the collected traffics and make decisions on potential security threats. Artificial Neural Network (ANN) is a machine learning algorithm which mainly employed to analyze the collected information and detect intrusion in IDS.

II. THEORETICAL BACKGROUND AND LITERATURE REVIEW

1. Intrusion Detection Systems

The process of monitoring and analyzing the actions taking place within a computer system or network in order to identify intrusions in order to safeguard the networks is known as intrusion detection systems, and they are a key part of the security architecture for networks linked to the internet. [2].

IDS is regarded as one of the firewall functions, but they are different. A firewall is considered a shield that defends the flow of information and prevents intrusions, whereas IDS discovers if the network has been attacked or if attackers penetrate the network security imposed by the firewall. As shown in the figure (1), Firewalls and IDS promote network security [3].

2. Intrusions and Attacks

Attacks fall into one of five categories: Denial of Service, Probe, User to Root; and Remote to Local [9].

- Denial of Service (DoS): The intruder (hacker) tries to prevent legitimate users from using a service.
- Probe: The intruder tries to gain information about the target host.
- Remote to Local (R2L): Intruder does not have an account on the victim machine, hence tries to gain access.
- User to Root (U2R): Intruder has local access to the victim machine and tries to gain superuser privileges.

3. Detection Systems Methodologies

In general, IDS utilizes three distinct methodologies to detect possible attacks: anomaly detection, misuse detection, and hybrid detection. Hybrid detection is a sort of combination of anomaly and misuse detection approaches [5]. In case of misuse detection or as known, *signature-based*, the intrusion detection system enfolds the identification of known attack sequences of causal events and matches it to the incoming events. If the pattern of the incoming event matches the signature of an intrusion, then there is a positive match which is labeled for further processing. While in the case of anomaly detection methodology, the detection is conducted based on a preliminary idea that the attack signature is unknown. Therefore, the IDS responds if there is any deviation from a pre-specified computer system state is detected. Many different approaches were used to build the anomaly detection system. However, all of them are composed of basic modules or phases, as illustrated in Figure (2).

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YAFW6

Modules of the Anomaly Intrusion Detection System Functional Architecture (Estevez-Tapiador, et al., [4]):

- Phase (1) **Parameterization**: in this phase, the observed samples of the target system are represented in a form that is suitable as an input to the proposed detection algorithm.
- Phase (2) **Training**: The normal (or abnormal) activities on the network systems characterization take place in this phase.
- Phase (3) **Detection**: the behavior of the system model that builds in phase (2) is compared with input (observed) traffic and an alarm will be generated if any deviation is observed.

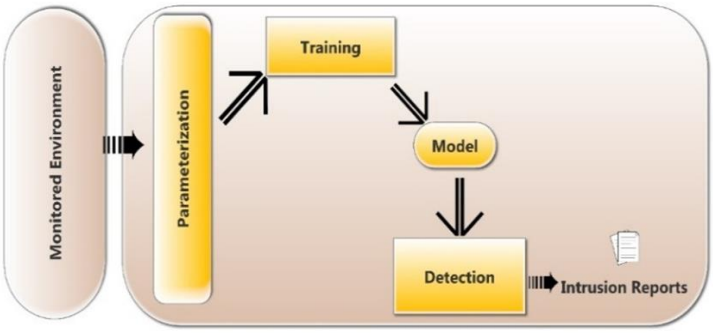

Figure 2: Generic Anomaly IDS functional architecture

Several machine learning-based techniques have been employed to implement a range of Anomaly Intrusion Detection Systems, as depicted in Figure (3). This research utilizes a selection of machine learning algorithms to construct the proposed system, incorporating two artificial neural networks: SOM and Backpropagation.

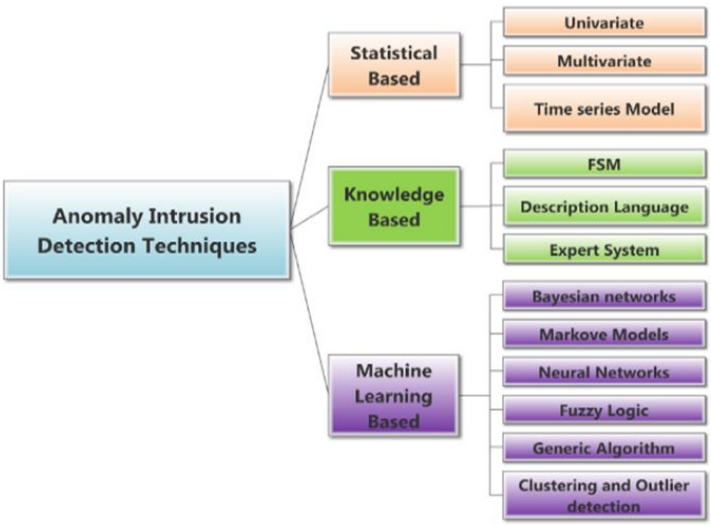

Figure 3: Classification of the anomaly detection techniques

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YAFW6

4. Artificial Neural Network (ANN)

Is a machine learning algorithm that is inspired by the structure and role of the Biological Neural System. In General, Artificial neural networks can be classified into main categories: Unsupervised and Supervised Artificial Neural Networks depending on the nature of the learning process.

In the case of Unsupervised ANN, the learning mechanism comes in a sort of self-organized behavior. Weight adjustment of this type of neural network is not affected by an external agent. Thus, the desired or correct outputs are not available during the process of training.

GANs and SOM are considered typical examples of such types of artificial neural networks (ANNs), and they will serve as the initial detection layer in the proposed system. (Kayacik, et.al, [4]) applied the self-organized map to building an intrusion detection system. These research experiments demonstrate that satisfactory results can't be obtained if traditional SOM is directly applied to intrusion detection due to the fact that traditional SOM can't classify with high precision.

The other type of ANN is the supervised one. This type of ANN needs a supervisor through the process of training activities that lead to the final convergence.

Back Propagation Neural Network (BPNN) algorithm also known as the error backpropagation algorithm could be considered the most well-known and oldest supervised learning multilayer neural network that is proposed by (McClelland & Rumelhart, 1986) [12].

Back Propagation ANN achieves high accuracy and detection rate for the records of the highest frequency such as Normal, DoS, and Probe. In this research, we will use the Backpropagation algorithm to classify the Normals and Attacks records that come from SOM (first detection layer) into its basic four categories: DoS, Probe, U2R, and R2L.

5. Literature Review

Intrusion detection systems are designed with many techniques and use different algorithms depending on the scenario and application under study.

5.1 Intrusion Detection Systems based on SOM

Peter Lichodzijewski (May 2002) [13] designs a simple intrusion detection system based on an unsupervised machine learning algorithm: Self-Organized Map that operates in real-time, the model consists of two layers of SOM to obtain a higher level of detection.

5.2 Intrusion Detection systems based on Backpropagation Artificial Neural Networks

Sen and Chattopadhyay (2014) [11] designed an intrusion detection system built using a Multi-Layers Back Propagation Neural Network (MLBPNN) The objective of their system was to detect intrusion activities and classify them based on their type. The experimental results of the designed system showed its capability of record classification between (98.5 %) and (99%).

ISSN 1533-9211

DOI 10.17605/OSF.IO/YAFW6

5.3 Intrusion Detection systems based on Hybrid Algorithms

An intelligent algorithm supported by (Khodaie, et.al. 2014)[14] that built based on an artificial neural network and self-organizing map. The proposed system consists of two principal detection layers. The first layer consists of one SOM that classifies the dataset into two main categories: Normal and Attacks. Then they passed to the second detection layer that consists of two feed-forward ANNs for further attack classification. The experimental results proved the high accuracy and speed of detection achieved by the proposed techniques.

(Paulo M. Mafra 2010) [8] Proposed an intelligent intrusion detection system call Octopus IIDDS that consists of two layers:

The first layer (Classifier Layer / KNN Layer): This layer has been used to reduce the false negative rate. It analyzes and classifies the network traffic into many types of attack (DOS, Probe, R2L, and U2R). The Second Layer (Decision Layer / SVM Layer): Support Vector Machines (SVM) can be used to improve the detection rate, in the octopus model, the detection ratio is very good by using the KDD data set.

5.4 Intrusion Detection Systems based on GAN

One of the most notable Machine Learning tools is the Generative Adversarial Network (GAN), and it has great potential for tabular data synthesis, (Nelly Leligou 2021) [15] used this tool to design a model that can generate new data that preserve the characteristics of the training data. As a result, GANs improved speed and training performance.

III. PROPOSED HYBRID INTRUSION DETECTION SYSTEM METHODOLOGY

The general framework of the proposed Hybrid intrusion detection system will be based on three powerful artificial neural networks: self-organizing map and Back- Propagation Artificial Neural Networks with Generative Adversarial Networks (GANs).

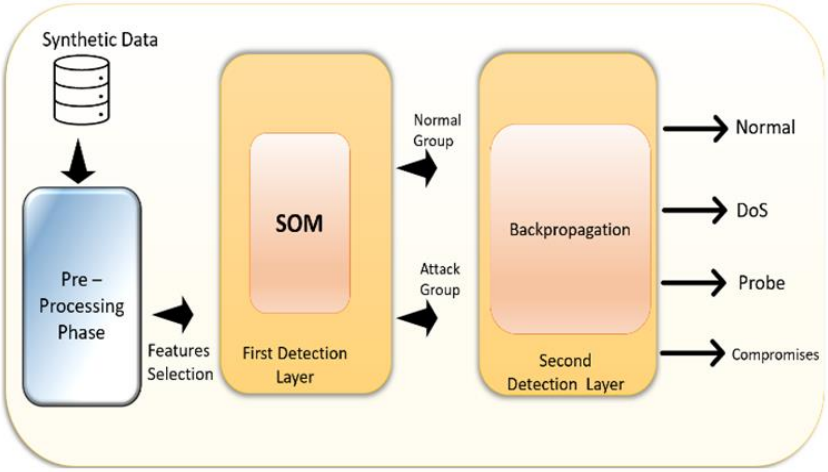

Figure 4: Framework of the proposed Hybrid Intrusion Detection System

ISSN 1533-9211

DOI 10.17605/OSF.IO/YAFW6

As shown in Figure (4), the proposed system uses two detection layers used to first isolate and then detect attacks. The first layer of a self-organizing map and the next layer of Backpropagation were separately taken.

In this way, the attack traffic is separated from the normal ones utilizing the detection layers. Where the SOM is taught by the Normal and Attack traffic to cluster the normal connection records and the intrusion connection records separately in two large groups.

Thus, the main task of the first layer is separating the normal traffic from the attack traffic. The next layer can be considered the output layer of the proposed system, where in general, two routes one for normal traffic (normal group) and the other one for the attack traffic (attack group). Then, Normal records will have passed to the backpropagation layer then classified as normal, whereas the attack traffic will be fed into the backpropagation layer to be further classified into its main types, DoS, Probe, and compromises attacks namely, U2R, or R2L.

A. Pre-processing Phases of the Proposed Hybrid IDS

The pre-processing proposed system consists of two main phases:

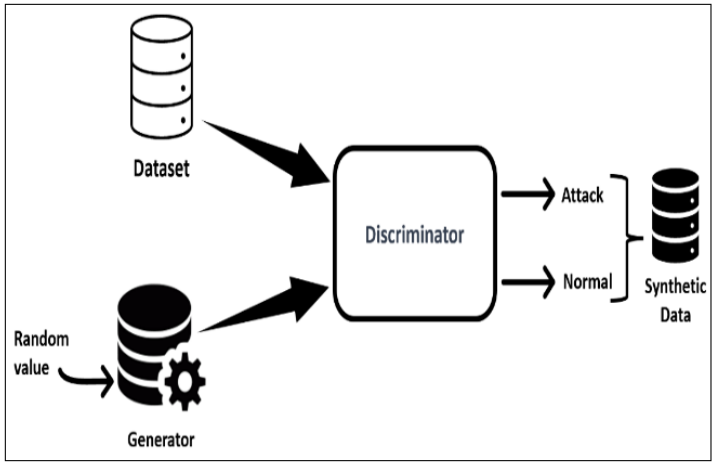

Figure 5: Generate Synthetic data

- **Generate synthetic data phase:**

Generative Adversarial Networks (GANs) are not directly used for detecting the attacks. Instead, they are used as a part of the hybrid intrusion detection system to improve the accuracy of anomaly detection. GANs generate synthetic data that resembles real network traffic, which is then used to train the detection system. By generating synthetic data, GANs enable the system to learn and adapt to new attack patterns that may not have been previously encountered, making the detection system more robust and effective. Figure (5) shows the phase of generating synthetic data.

As we see, GAN neural network architecture that consists of two networks: a generator network and a discriminator network. The generator generates network traffic data that resembles the network traffic patterns and characteristics of real-world network traffic. Whereas, the

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YAFW6

discriminator takes in both output from the generator and dataset and then tries to distinguish between normal and up-normal traffic.

The dataset used in this proposal is the NSL-KDD dataset which has many advantages over the original KDD and it can be considered an effective benchmark dataset.

Synthetic data refers to artificial data that is generated by the GAN model. This synthetic data is then used to train the intrusion detection system to improve its accuracy in detecting anomalies or attacks.

- Data pre-processing phase proceeds in two main phases: the Data Codification stage, and the Data Normalization stage. Which is the process of raw qualitative data being examined in a way that assigns codes or labels to any piece of data that comes in the form of words, phrases, sentences, or paragraphs.

The dataset records contain fields (features) that need to be transformed into numerical values in order to be in an appropriate format suitable to our classification techniques. The NSL-KDD dataset has a total of 42 features, that represent the label of the record, or it classifies the connection record as whether it is normal or attack one. The label of record can be either "normal" or "attack" and belongs to one of more than forty different intrusions classified into four main categories: DoS, R2L, U2R, and Probing Attack.

IV. PROPOSED SYSTEM EVALUATION CRITERIA

The performance of the proposed IDS system is evaluated using true positive (TP), true negative (TN), false negative (FN), false positive (FP), Accuracy, False Positive Rate (FPR), Detection Rate (DR), False Negative Rate (FNR), and Precision.

True positive indicates the number of attack connection records that are correctly classified by IDS and it is considered a sign of proper detection of attack. Whereas the true negative indicates the number of legal records that are correctly classified.

False positive indicates the connection records that were incorrectly classified as invalid records and it represents the accuracy of the detection system.

False negative indicates connection records that were incorrectly classified as legal activities whereas they are intrusion activities (attacks). A false negative is a direct sign of the inability of IDS to detect the intrusion.

The detection rate (DR) is the number of attacks detected by the IDS divided by the number of attacks in the dataset,

DR=$Detection\ Rate = TP/(TP + FN)$

Precision = TP/ (TP+FP)

Accuracy = (TP+TN)/ (TP+TN+FP+FN)

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YAFW6

V. EXPERIMENTAL RESULTS OF THE PROPOSED INTRUSION DETECTION SYSTEM

The proposed system was implemented using MATLAB 2015 as a powerful integrated development environment, the following tables present the experimental results obtained by running the first detection layer: SOM of the proposed intrusion detection system, and then running the second detection layer: Back Propagation of proposed intrusion detection system.

Table 1: The Performance Evaluation First Detection Layer

Actual	Normal	Attack
Normal	13894	43
Attack	917	10340

Table 2: The Performance Evaluation Second Detection Layer

Actual	Normal	DoS	Probe	U2R &R2L
Normal	2146	6	25	9
DoS	17	3972	0	1
Probe	18	1	1568	2
Compromises (U2R& R2L)	4	0	3	22

The performance evaluation for the entire system can be found in Table 3 provided below:

Table 3: The Performance Evaluation of the proposed hybrid system

Attack Type	TN	FP	FN	TP	Detection Rate	Accuracy	Precision
Dos	**5843**	**6**	**93**	**3972**	**0.977**	**0.99**	**0.998**
Probe	**5843**	**25**	**18**	**958**	**0.981**	**0.993**	**0.974**
R2L & U2R	**5843**	**9**	**68**	**22**	**0.24**	**0.987**	**0.709**

VI. CONCLUSION

The proposed detection technique can achieve a high detection rate, accuracy, and precision which cannot be achieved via a non-hybrid intrusion detection system. The SOM will process the detection rate accuracy whereas back propagation ANN will deal with the issues of accuracy and precision. Moreover, the suggested technique enables the detection system to detect the most difficult intrusions and penetrations, namely, R2L and U2R attacks and with high accuracy.

References

1) Anderson, J. P. (1980). **Computer security threat monitoring and surveillance** (Vol. 17).

2) Brahmi, I., Brahmi, H., & Yahia, S. B. (2015). **A Multi-Agents Intrusion Detection System Using Ontology and Clustering Techniques**. In Computer Science and Its Applications (pp. 381-393). Springer International Publishing.

3) Chow, T. W. and Cho, S. Y. (2007). **Neural Networks and Computing: Learning Algorithms and Applications**, (1st ed.). London: Imperial College Press.

4) Estevez-Tapiador, J. M., Garcia-Teodoro, P., & Diaz-Verdejo, J. E. (2004). Anomaly detection methods in wired networks: a survey and taxonomy. **Computer Communications, 27(16), 1569-1584.**

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YAFW6

5) Gollmann, D., & Meier, J. (2006). **Computer Security–ESORICS 2006: 11th [6] European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006, Proceedings** (Vol. 4189). Springer Science & Business Media.

6) Ilgun, K., Kemmerer, R., & Porras, P. (1995). State transition analysis: A rule-based intrusion detection approach. **Software Engineering, IEEE Transactions on**, *21*(3), 181-199.

7) Javidi, M. M., & Nattaj, M. H. (2013). A New and Quick Method to Detect DoS Attacks by Neural Networks. **The Journal of Mathematics and Computer Science**, 6, 85-96.

8) Kayacik, H. G., Zincir-Heywood, A. N., & Heywood, M. I. (2007). **A hierarchical SOM-based intrusion detection system**. **Engineering Applications of Artificial Intelligence**, *20*(4), 439-451.

9) Kayacik, H., Zincir-Heywood, A. and Heywood, M. (2005). Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets. **In Proc. of the third annual conference on privacy, security and trust**, Canada, 1-6.

10) Khodaie, F., Jamali, M., & Farazan, A. (2014). The Use of Intelligent Algorithms to Detect Attacks in Intrusion Detection System. **International Journal of Computer Applications Technology and Research.** 9(3), 579-584.

11) McClelland, J. L., & Rumelhart, D. E. (1986). **Parallel Distributed Processing. Explorations in the Microstructure of Cognition**. Volume 2: Psychological and Biological Models. Cambridge, MA: MIT Press

12) Lichodzijewski, P., Zincir-Heywood, A. N., & Heywood, M. I. (2002, May). **Host-based intrusion detection using self-organizing maps**. In *IEEE international joint conference on neural networks* (pp. 1714-1719).

13) Wu, W., Cheng, N., & Wang, Y. (2014, November). **Application Research on Retrospective Analysis System in Network Intrusion Detection**. In Computational Intelligence and Security (CIS), 2014 Tenth International Conference on (pp. 624-627). IEEE.

14) Stavroula Bourou, Andreas El Saer, Terpsichore, Artemis Voulkidis &Theodore Zahariadis (2021). **A Review of Tabular Data Synthesis Using GANs on an IDS Dataset**. https://doi.org/10.3390/info12090375