The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/B6APM

EFFECTIVE NETWORK INTRUSION DETECTION MODELING

NANCY THOMAS[1] and Dr. V. SANGEETHA[2]

[1]Research Scholar, Karpagam Academy of Higher Education (Deemed to be University), Coimbatore, India.
[2]Research Guide, Karpagam Academy of Higher Education (Deemed to be University), Coimbatore, India.
Email: [1]nancyjismon@gmail.com, [2]drsangeetha.v@kahedu.edu.in

Abstract

In recent years there have been immense advancements in the internet and in relevant statement fields which have led to the uplift in the network size and the information related to it. This has led to the fact that there are more and more novel attacks happening today which have created problems for the security of a network. The ability to detect hacks and intrusions is essential for network security setup. The existence of malicious intruders who aim to commence attacks from inside the system of networks and this fact can't be disregarded. Recently there has been a system of intruder detection also known as IDS which works to stop malicious intruder attacks by inspecting the heavy frequency of traffic inside the vast network. The signature process helps in detecting intrusions on specific blueprints based on numbers in the network traffic. Signatures can easily help in detecting distrustful incoming attacks. The network intrusion detection system helps in identifying distrustful happenings and works as a vigilant detection system for the system administrator. The network intrusion detection system assists in the overall improvement of the performance of the network system. The system to detect network traffic monitors the vast network model of the computer to identify malicious activity. It studies the information that comes through the network to identify the blueprint and symptoms of malicious factors.

Keywords: IDS, Network Anomaly, Malicious Attacks, System Detection

I.INTRODUCTION

In recent years there have been immense advancements in the internet and in relevant statement fields which have led to the uplift in the network size and the information related to it. This has led to the fact that there are more and more novel attacks happening today which have created problems for the security of the network. The ability to detect hacks and intrusions is essential for network security setup [1]. The existence of malicious intruders who aim to commence attacks from inside the system of networks and this fact can't be disregarded. Recently there has been a system of intruder detection also known as IDS which works to stop malicious intruder attacks by inspecting the heavy frequency of traffic inside the vast network. The whole system's discretion, honesty and accessibility depend on the working of the network intrusion model.

ISSN 1533-9211

DOI 10.17605/OSF.IO/B6APM

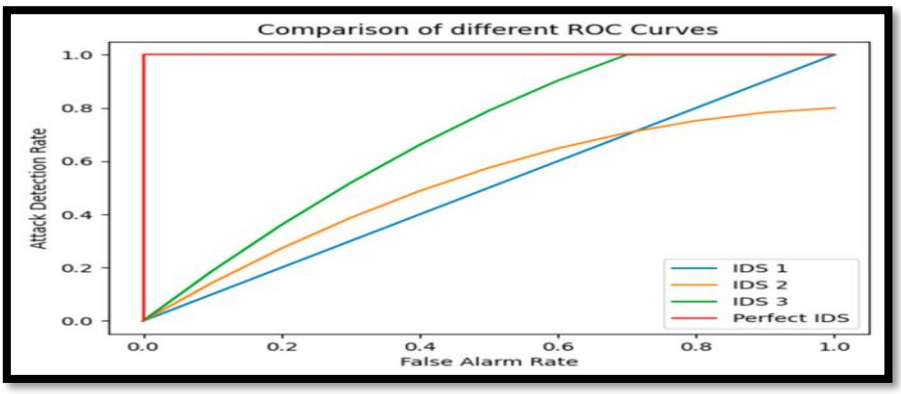

Figure 1: Detection rates of the network detection system

(Source: Influenced by 11)

Figure 1 shows the detection rates of the network detection system with the IDS 3 value being the highest

II.OBJECTIVES

In this analysis, basic primary goals are recognized in this study and described. All of these goals are associated with the network intrusion detection model. The goals are as follows

- To evaluate the effect of the network intrusion detection model on the vast network traffic
- To understand the basic causes of network disruptions and related cyber attacks
- To analyze the ethical considerations of the network intrusion model
- To understand the basic impact of network intrusion detection systems on internet security

III.METHODOLOGY

Secondary data collection method has been used to analyze the effect of network detection system modeling. Data from statistical journals and articles have been used for referencing. The system modular networks and malicious attack frequencies have been compared and analyzed.

IV.WORKING OF A SYSTEM FOR THE DETECTION OF NETWORK INTRUSION

The system to detect network traffic monitors the vast network model of the computer to identify malicious activity. It studies the information that comes through the network to identify the blueprint and symptoms of malicious factors. The detection system compares the activity of the network to a pre-decided policy and blueprints to analyze any work that may specify a malicious intrusion.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/B6APM

Table: Host-based detection system and network-based detection system

Features	Host	Network
Deterrence	Strong for insiders	Strong for outsiders
Detection	Strong inside, weak outside	Strong outside, Weak inside
Response	Weak real-time response	Strong response

(Source: Influenced by 11)

On detection of any malicious activity, the system creates vigilant efforts to manage the system administrator. The network intrusion detection system helps in identifying distrustful happenings and works as a vigilant detection system for the system administrator [2]. The network intrusion detection system assists in the overall improvement of the performance of the network system. The network monitoring system helps in meeting the fulfillment of prerequisites by recognizing network function and form description. The network detection model forms important ideas inside the network system and this system will be used to recognize any limitations and the security of the network can be improved.

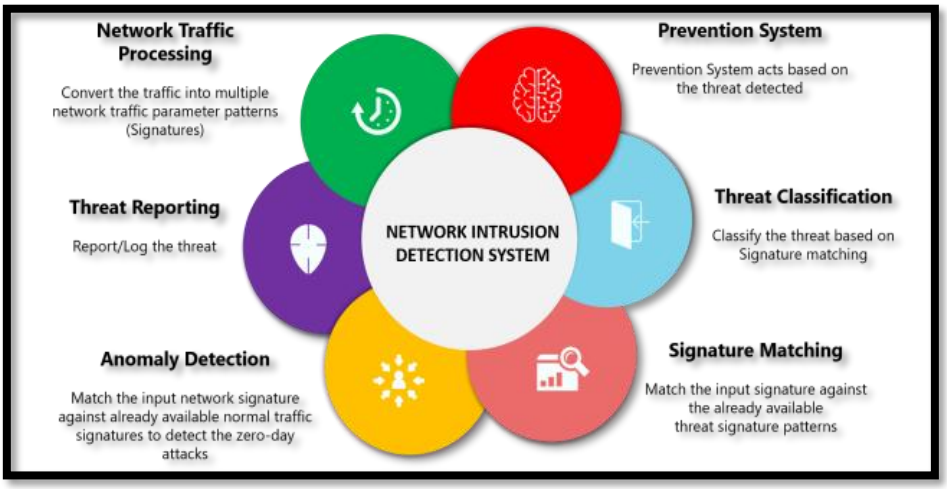

Figure 2: Working criteria of the network detection system

(Source: Influenced by 8)

Figure 2 shows the Working criteria of the network detection system and its various outlines.

V. CLASSIFICATION OF NETWORK INTRUSION DETECTION SYSTEM

These intrusion detectors are classified into 5 types which are as follows. Network intrusion detection, host intrusion detection, protocol-based intrusion system and application protocol intrusion system are the examples. These are set in a planned place within which the vast networking system can be able to examine malicious attacks from hackers and intruders [3]. Host intrusion detector analyzes the inward and outwards attacks on the system networks and works as a vigilant detector for the administrative network. The application-based system recognizes the attacks by creating a monitoring system and identifies the announcement.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/B6APM

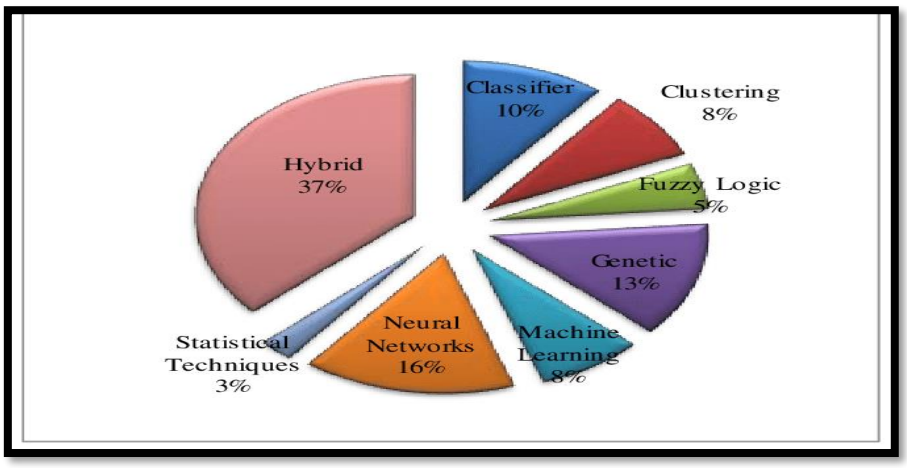

Figure 3: Intrusion detection system

(Source: Influenced by 9)

Figure 3 shows the intrusion detection system and its shares among networks

VI. ADVANTAGES OF NETWORK INTRUSION DETECTION SYSTEM

The network intrusion detection system helps in identifying distrustful happenings and works as a vigilant detection system for the system administrator. The network intrusion detection system assists in the overall improvement of the performance of the network system [4]. The system to detect network traffic monitors the vast network model of the computer to identify malicious activity. It studies the information that comes through the network to identify the blueprint and symptoms of malicious factors.

Table: Comparison of Anomaly-based and signature based detection system

Anomaly Based system	Signature-based system
No updates	Updates present
Can detect attacks	Only previous attacks can be detected
High false alarms	Low amount of alarms
High risk	Low risk
Need less calculation	Need extra calculation

(Source: Influenced by 11)

The detection system compares the activity of the network to a pre decided policy and blueprints to analyze any work that may specify a malicious intrusion. On detection of any malicious activity the system creates vigilant efforts to manage the system administrator. The network intrusion detection system helps in identifying distrustful happenings and work as a vigilant detection system for the system administrator [5]. The network monitoring system helps in meeting with fulfillment of prerequisites by recognizing network function and forms description. Network detection model forms important ideas inside network system and this system will be used to recognize any limitations and the security of network can be improved.

ISSN 1533-9211

DOI 10.17605/OSF.IO/B6APM

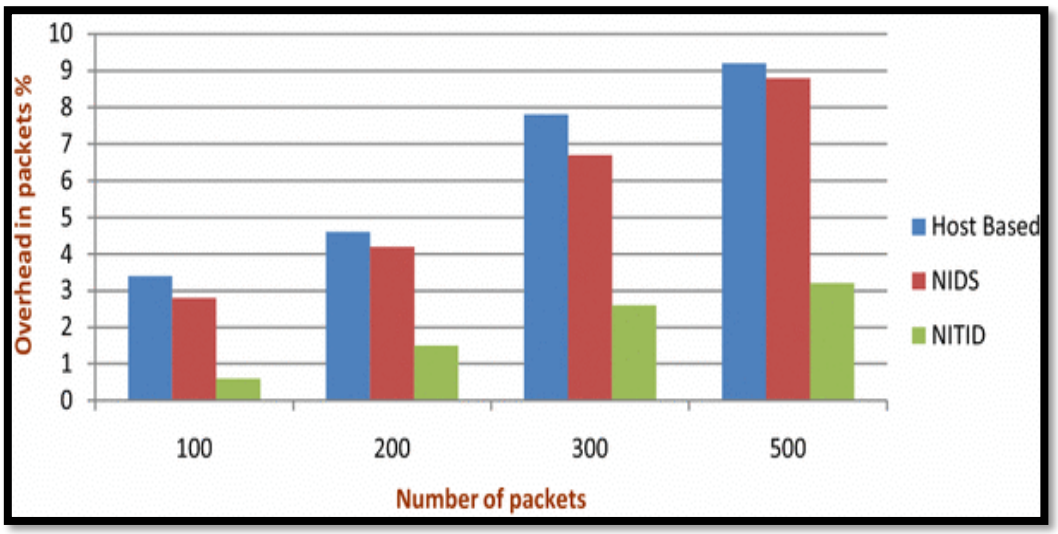

Figure 4: Network detection model packets vs overhead in packets

(Source: Influenced by 11)

Figure 4 shows number of packets with host based, NIDS and NITID systems

VII. DETECTION METHOD OF NETWORK INTRUSION DETECTION SYSTEM

Signature process helps in detecting intrusions on the specific blueprints on the basis of numbers in the network traffic. Signatures can easily help in detecting distrustful incoming attacks. The network intrusion detection system helps in identifying distrustful happenings and work as a vigilant detection system for the system administrator. The network intrusion detection system assists in overall improvement of performances of network system [6]. The system to detect network traffic monitors the vast network model of computer in order to identify the malicious activity. It studies the information that comes through network to identify the blueprint and symptoms of malicious factors. Anomaly method helps recognizing attacks from hackers and potential malicious intruders by using machine learning.

ISSN 1533-9211

DOI 10.17605/OSF.IO/B6APM

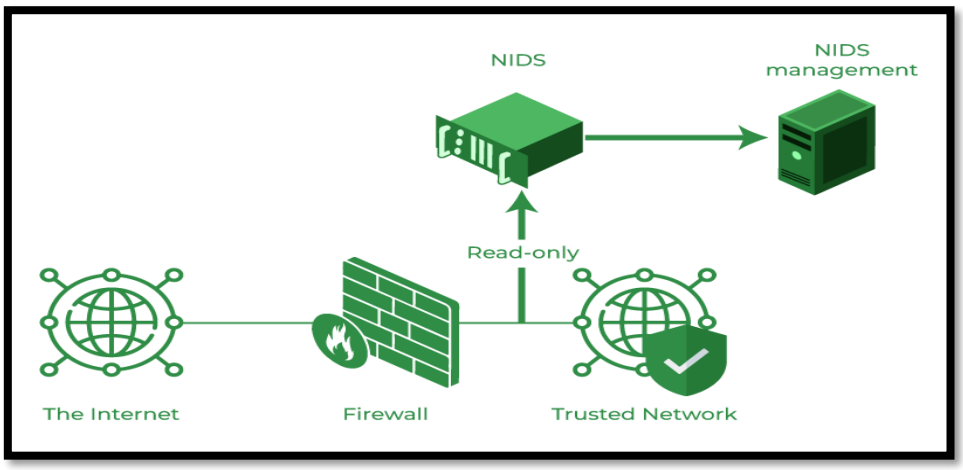

Figure 5: Detection method of detector system

(Source: Influenced by 8)

Figure 5 shows detection method and the working principles of networking system

VIII. NETWORK DETECTION SYSTEM AND ITS COMPARISON

Network detection system works mostly after the happening of malicious attack and windows firewall works to stop the attacks beforehand [7]. Network detection model forms important ideas inside network system and this system will be used to recognize any limitations and the security of network can be improved.

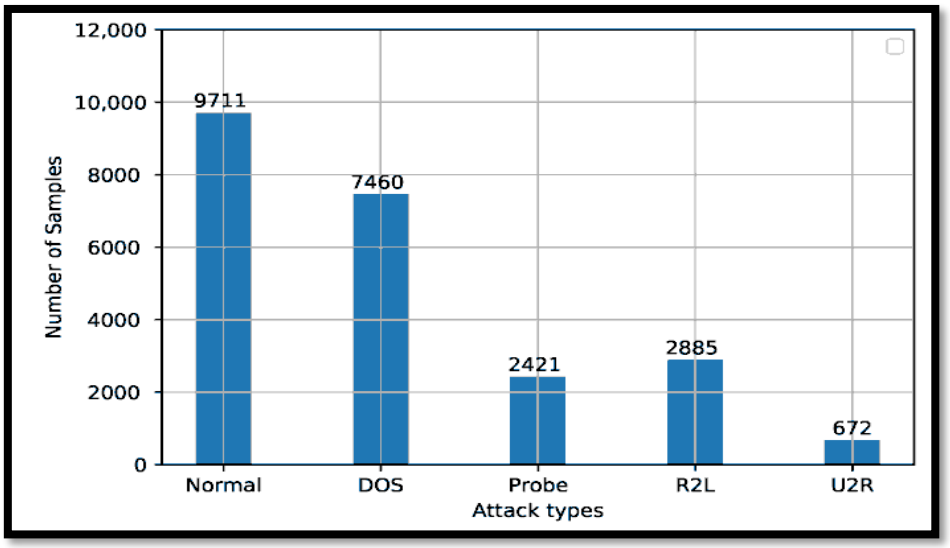

Figure 6: Attacks on network systems according to types

(Source: Influenced by 10)Figure 6 shows attacks on network systems according to types in which normal and DOS attacks are the highest

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/B6APM

IX. PROBLEM STATEMENT

During the study only secondary analysis method based information were obtained and studied so a lot of statistical data was not possible to obtain. External networking issues were not considered in the study so a lot of external attacks statistics were not considered during the analysis. Only secondary data journals and articles were available for selecting data.

X. CONCLUSION

In conclusion it can be said that the existence of malicious intruders who aim to commence attacks from inside the system of networks and this fact can't be disregarded. Recently there has been a system of intruder detection also known as IDS which works to stop the malicious intruder attacks by inspecting the heavy frequency of traffic inside the vast network. The whole system's discretion, honesty and accessibility depend on the working of network intrusion model.

References

1. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4150 Retrieved on 9th May 2023
2. Devan, P., & Khare, N. (2020). An efficient XGBoost–DNN-based classification model for network intrusion detection system. Neural Computing and Applications, 32, 12499-12514. https://link.springer.com/article/10.1007/s00521-020-04708-x Retrieved on 9th May 2023
3. Elmasry, W., Akbulut, A., & Zaim, A. H. (2020). Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. Computer Networks, 168, 107042. https://www.sciencedirect.com/science/article/pii/S138912861930800X Retrieved on 9th May 2023
4. Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. Journal of Network and Computer Applications, 169, 102767. https://www.sciencedirect.com/science/article/pii/S1084804520302411 Retrieved on 9th May 2023
5. Khan, F. A., Gumaei, A., Derhab, A., & Hussain, A. (2019). A novel two-stage deep learning model for efficient network intrusion detection. IEEE Access, 7, 30373-30385. https://ieeexplore.ieee.org/abstract/document/8643036/ Retrieved on 9th May 2023
6. Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., ... & Cui, L. (2020). Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. Measurement, 154, 107450. https://www.sciencedirect.com/science/article/pii/S026322411931317X Retrieved on 9th May 2023
7. Qiu, H., Dong, T., Zhang, T., Lu, J., Memmi, G., & Qiu, M. (2020). Adversarial attacks against network intrusion detection in IoT systems. IEEE Internet of Things Journal, 8(13), 10327-10335. https://ieeexplore.ieee.org/abstract/document/9311132/ Retrieved on 9th May 2023
8. Song, H. M., Woo, J., & Kim, H. K. (2020). In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications, 21, 100198. https://www.sciencedirect.com/science/article/pii/S2214209619302451 Retrieved on 9th May 2023
9. Su, T., Sun, H., Zhu, J., Wang, S., & Li, Y. (2020). BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset. IEEE Access, 8, 29575-29585. https://ieeexplore.ieee.org/abstract/document/8988230/ Retrieved on 9th May 2023

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/B6APM

10. Taher, K. A., Jisan, B. M. Y., & Rahman, M. M. (2019, January). Network intrusion detection using supervised machine learning technique with feature selection. In 2019 International conference on robotics, electrical and signal processing techniques (ICREST) (pp. 643-646). IEEE. https://ieeexplore.ieee.org/abstract/document/8644161/ Retrieved on 9th May 2023

11. Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2020). Building an efficient intrusion detection system based on feature selection and ensemble classifier. Computer networks, 174, 107247. https://www.sciencedirect.com/science/article/pii/S1389128619314203 Retrieved on 9th May 2023