International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 04, April 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Enhancing Ad Hoc Network Security through Machine Learning

Mr. Rahul Kaushik
Assistant Professor, CSE Department, Bhiwani Institute of Technology &Sciences, Bhiwani
Supriya Gope
M.tech, CSE Department, Bhiwani Institute of Technology & Sciences, Bhiwani

ABSTRACT-An ad hoc network is a transient network that is self-organizing and does not require any infrastructure. Therefore, the majority of its applications are in the field of military work and disaster assistance. Because of wireless connectivity and the ability to organize itself, ad hoc networks are becoming more common. Susceptible to a greater number of breaches or assaults than the conventional system. Blackhole assault is a significant routing disruption attack that a rogue node promotes itself as being capable of. as a step along the way to the final destination. In this research, we simulated a black hole using computer models. Assault in a setting with ad hoc networking, as well as data collection of important features for the purpose of classifying aggressive behaviour. Then, several different approaches to machine learning have been developed. utilized for the classification of information regarding benign and harmful packets. It seems to imply. a novel method for the selection of certain features, the gathering of crucial information, and the intrusion detection in an ad hoc network with the application of machine learning algorithms. As a result, we can say analysis of the relative effectiveness of several approaches to machine learning According to our findings, that this method may be utilized with a variety of classifiers and that it can be expanded upon using various. Despite the improvements made to security systems, there is a continuous change in attack strategies, which requires a robust detection mechanism. The most reliable method is determining, based on the circumstances surrounding an attack sample, whether the sample in question is benign or malicious. The simulation and execution has performed on MATLAB software.

INTRODUCTION

Vehicle ad-hoc networks (VANETs) are becoming one of the trends in smart cities that aim at minimizing transportation problems, such as traffic congestion, pollution, and car accidents [1–]. VANETs create an efficient collaboration between vehicles that allows both road operators and drivers to be informed about the current traffic incident information. This requires effective traffic coordination that involves mainly two types of communications: communication between vehicles (V2V), and interaction between vehicles and the infrastructure (V2I). Through V2V and V2I, the vehicles can broadcast warning messages and traffic management instructions to increase road safety and improve the urban environment's driving [2].AS the development of modern vehicles is now equipped with flexible computing power resources, VANET is not only used to improve safety on road, but also it is exploited to ensure the emerging need for maintaining the voluminous amount of sensing data generated in smart cities. Incorporating VANET into mobile applications plays a vital role in smart cities, such as distributing cloud applications while reducing latency and providing more bandwidth [3].Vehicles act as cloud nodes and contribute their computing resources to jointly make the data analysis with cloud computing. Furthermore, VANET offers various cloud services (e.g., storage and computing) in their vehicles' geographical location, which can reduce latency and avoid congestion in the backbone network. As a result, VANET provides opportunities for exploiting the value of big data for various smart city applications such as real-time traffic monitoring, surveillance, or infotainment [4]. Meanwhile, that also makes VANET communications valuable for attackers since they require active interaction and collaboration between vehicles and other cloud entities (like fog computing [5].To address security vulnerabilities, different intrusion detection systems (IDSs) have been proposed to

secure VANET communications .In most of the existing detection solutions, machine learning methods [6] are involved in the reasoning process of IDSs to examine the data, identify the type of attacks, and then distinguish the malicious nodes from benign ones. In VANET, there are different IDS architectures designed for vehicles and they should be lightweight to meet the intelligent monitoring demands in distributed environments. Furthermore, they deal with specific attack detection logic, such as onboard IDSs in which a vehicle can self-detect attacks by using its onboard intrusion dataset; however, false alerts may occur due to resource constraints of VANET that lead machine learning approaches to learn from small data, which can be inefficient to detect novel attacks. Furthermore, it would be insufficient to match only network connections to known specific VANET intrusion patterns to detect network intrusions since novel intrusions will appear with the fusion of VANET. Yet, it is so far not well understood how IDS-based machine learning can minimize critical-time detection and subtract just the information necessary for preventing attacks against possible gaps in security accurately [7], and how machine learning techniques can deal with huge quantities of vehicular data that keep growing in the urban environment [9].

II LITERATURE SURVEY

Anish Halimaa A (2019) et.al [10] In order to examine malicious activity that occurs in a network or a system, intrusion detection system is used. Intrusion Detection is software or a device that scans a system or a network for a distrustful activity. Due to the growing connectivity between computers, intrusion detection becomes vital to perform network security. Various machine learning techniques and statistical methodologies have been used to build different types of Intrusion Detection Systems to protect the networks. Performance of an Intrusion Detection is mainly depending on accuracy. Accuracy for Intrusion detection must be enhanced to reduce false alarms and to increase the detection rate. In order to improve the performance, different techniques have been used in recent works. Analyzing huge network traffic data is the main work of intrusion detection system. A well-organized classification methodology is required to overcome this issue. This issue is taken in proposed approach. Machine learning techniques like Support Vector Machine (SVM) and Naïve Bayes are applied. These techniques are well-known to solve the classification problems. For evaluation of intrusion detection system, NSL- KDD knowledge discovery Dataset is taken. The outcomes show that SVM works better than Naïve Bayes. To perform comparative analysis, effective classification methods like Support Vector Machine and Naive Bayes are taken, their accuracy and misclassification rate get calculated.

Tommaso Zoppi (2020) et.al[11]Anomaly detection aims at identifying patterns in data that do not conform to the expected behavior, relying on machine-learning algorithms that are suited for binary classification. It has been arising as one of the most promising techniques to suspect intrusions, zero-day attacks and, under certain conditions, failures. This tutorial aims to instruct the attendees to the principles, application and evaluation of anomaly-based techniques for intrusion detection, with a focus on unsupervised algorithms, which are able to classify normal and anomalous behaviors without relying on input data with labeled attacks.

Muawia A. Elsadig 2023[12]the main reasons for the fast growth of wireless sensor networks (WSNs) in many areas are their features and how well they work. However, these networks are very open to many types of security threats, including denial-of-service (DoS) attacks, which are very common in these networks. A focus on DoS attacks, this study throws light on WSN limitations, flaws, and security risks. Researchers have carefully looked into new methods for finding DoS attacks and pointed out both their pros and cons. This gives us important information about the latest study in this area. So, this study suggests a simple

machine learning method for finding DoS attacks in WSNs that uses the Gini feature selection method and a decision tree (DT) algorithm.

PROPOSED APPROACH

This article proposes the utilization of simulation as a means to represent typical communication scenarios, some of which might be susceptible to malicious intrusion. A distributed and cooperative architecture characterizes the proposed system; each node employs an intrusion detection system (IDS) agent to identify and eliminate any nodes exhibiting suspicious behavior. Each IDS agent is composed of four distinct components. The initial module is referred to as the "data collection module," and its primary function is to collect data and determine the route between the source and destination of each node. A module that detects intrusions constitutes the second component of the system. In addition to the threshold value, it endeavors to determine whether anything unusual is occurring in the check nodes by utilizing the information provided by the module that preceded it. Third is the voting module, which is responsible for granting approval to the discovered information. Before isolating the accused node, a node in this module that asserts that another node is behaving improperly must obtain permission from every other node in the network. In contemporary times, Deep Learning (ML) has emerged as a prominent methodology that not only offers potential but also is preferable for achieving practical efficacy in a wide range of contexts. Vehicular networks are one of the most critical application domains, and it has been demonstrated that ML-based techniques are extraordinarily useful for resolving a variety of issues in this domain. Due to the utilization of WSN for communication between its vehicle nodes and other components, this system is susceptible to a variety of attacks. ML and its variants are gaining popularity as a method for detecting intrusions and resolving a vast array of communication security issues in vehicles.

Network Modeling: Involves creating a representation of the ad hoc network, considering the nodes, connections, and communication patterns. This model serves as the foundation for subsequent analyses and simulations.

Node Deployment: the strategic placement or arrangement of nodes within the ad hoc network. Proper node deployment can impact network coverage, connectivity, and overall efficiency.

Parameter Selection:

Involves choosing and configuring relevant parameters that govern the behavior of the ad hoc network. This could include factors such as transmission power, data rates, and routing protocols.

Data Transmission: Encompasses the process of sending and receiving data among nodes in the ad hoc network. Understanding and optimizing data transmission are critical for network performance and reliability.

Attack Detection: Focuses on identifying and mitigating security threats or attacks within the ad hoc network. This could involve the application of intrusion detection systems or machine learning algorithms to recognize abnormal behavior indicative of an attack.

Re-route Path: Addresses the dynamic nature of ad hoc networks by exploring methods to reroute communication paths when disruptions or attacks are detected. This adaptive response is crucial for maintaining network connectivity and ensuring data delivery.

Performance Analysis: Involves evaluating the overall performance of the ad hoc network. This assessment could include metrics such as throughput, latency, packet loss, and energy efficiency. Performance analysis provides insights into the effectiveness of the deployed strategies and mechanisms.

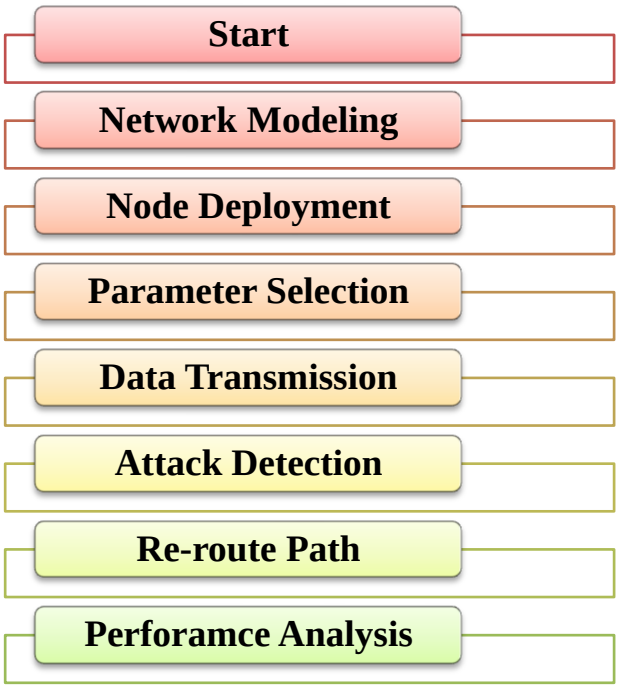

Fig. 1 system flow diagram

Network Model

The things that make up the VANET [10] network be able to be put addicted to three different group. Facilities on the side of the road, application and authorization servers, and nodes and cars fall into these groups.

Server Device -These are very powerful workstations, and each one is in charge of organization and providing service data on its own. The power has the entire key and is in charge of setting up a schedule for maintenance. Device servers give information about how cars work. Either the government or companies from around the world will give them money. We are working with the idea that the authorization and application servers can handle a lot of work. So, we haven't thought about how long it takes to do the math.

Road Side Infrastructure -The term "road infrastructure" refers to the collection and distribution of information, as well as the placement of power sources near roads. RSUs get power from wired networks and talk to vehicles over radio, both of which are done with the help of wired networks.

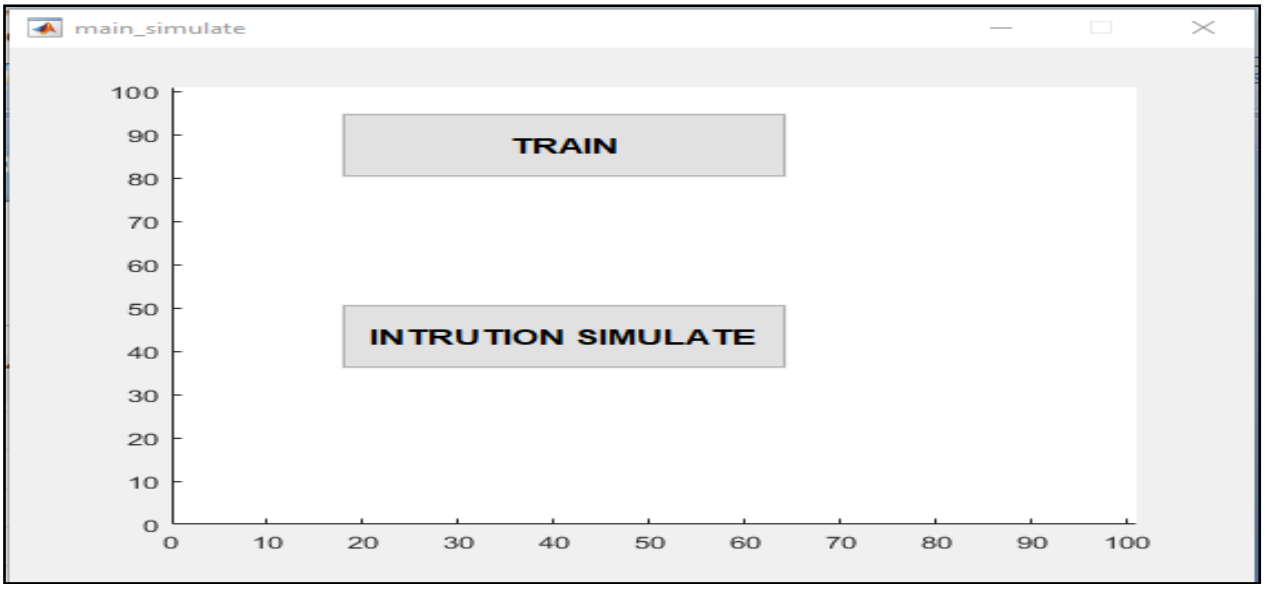

Fig.4.1 Training and Simulation Window

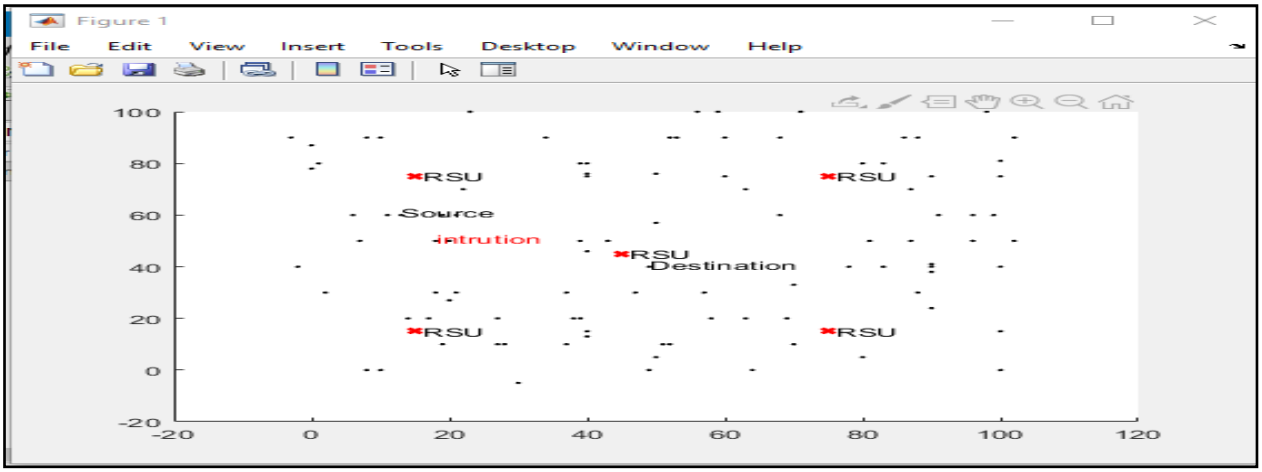

Figure.4.3 Network Architecture

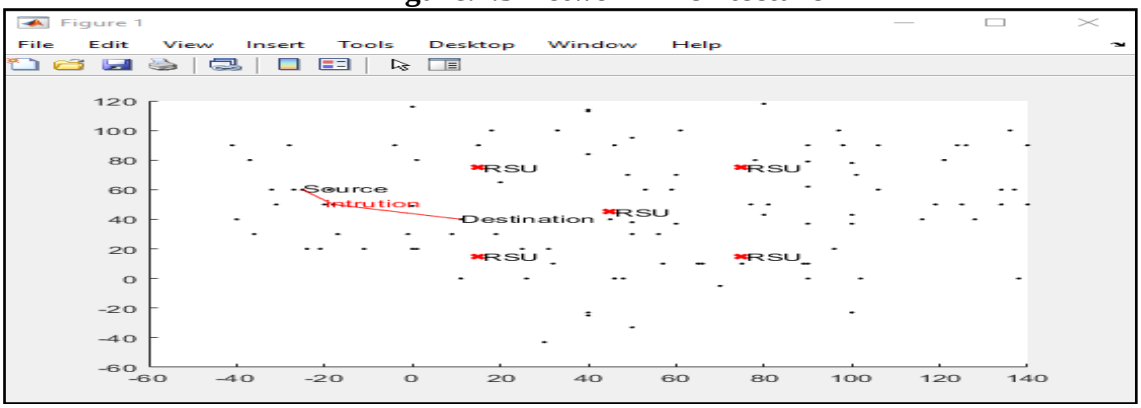

Figure .4.4 Network Architecture

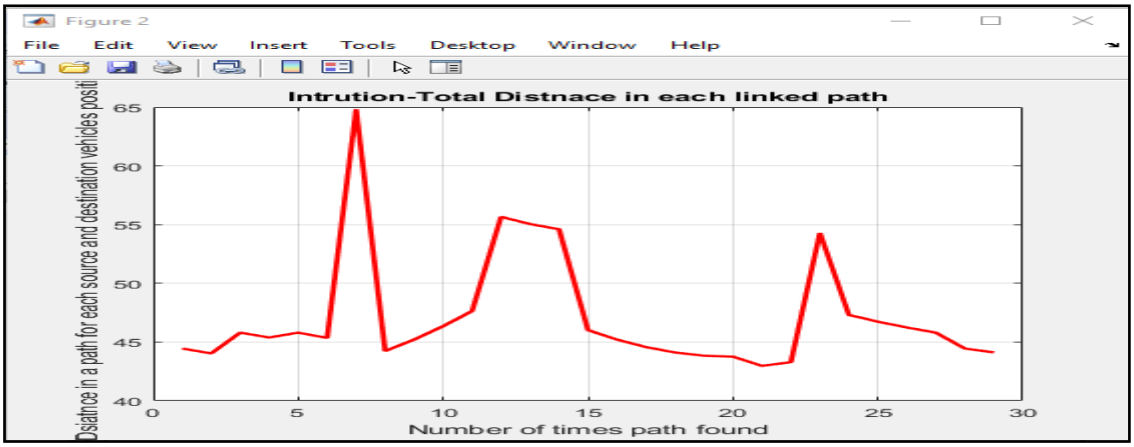

Figure.4.5 Total Number of Linked Path

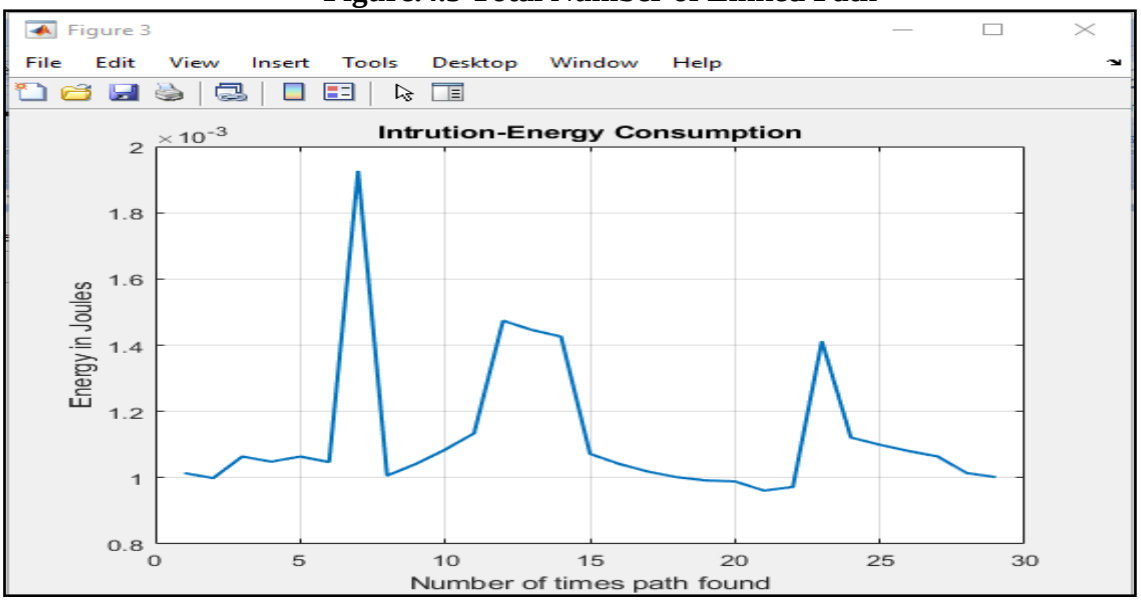

Fig.4.6 Intrusion Energy Consumption

One of the most important things to think about when it comes to WSN is how much energy they use .Communication uses the most energy, so the best way to use less energy is to decrease the figure of packet sent among the sensor in addition to the sink node. Figure 4.6 shows that less energy was used overall than in the previous figures.

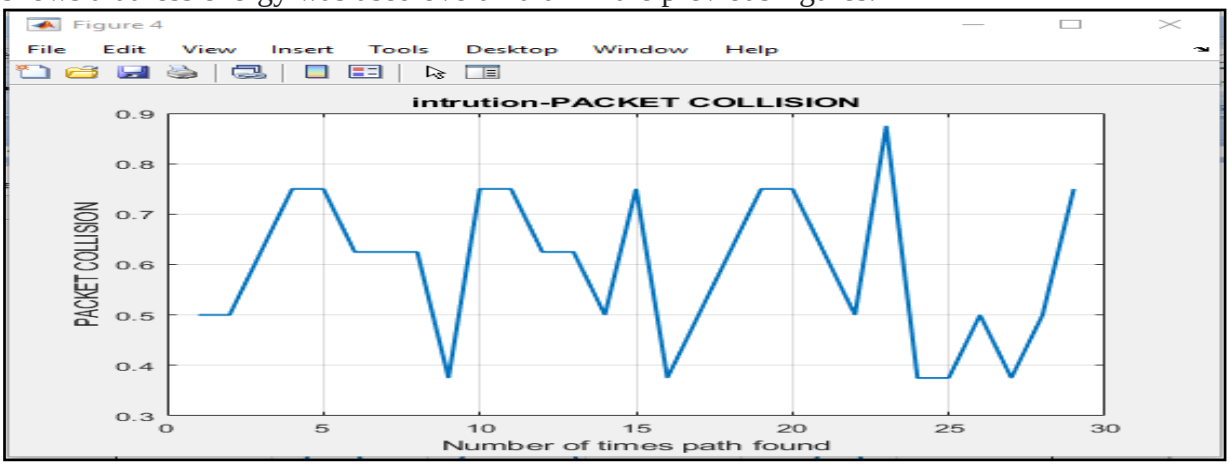

Figure.4.7 Packet Collision

Figure 4.7 shows "packet collision."Because the packets that have already been sent have to be rejected and then sent again, the process of resending those packets uses more energy and takes longer.

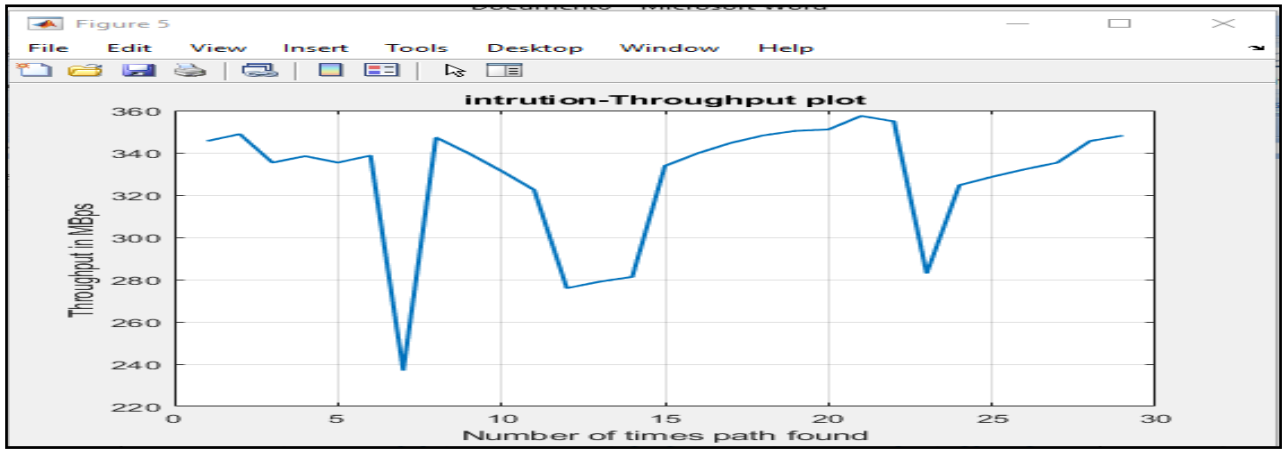

Figure.4.8 Intrusion Throughput

The network's intrusion throughput, depicted in fig. 4.8, is a measure of how much data can be processed in a given length of time.

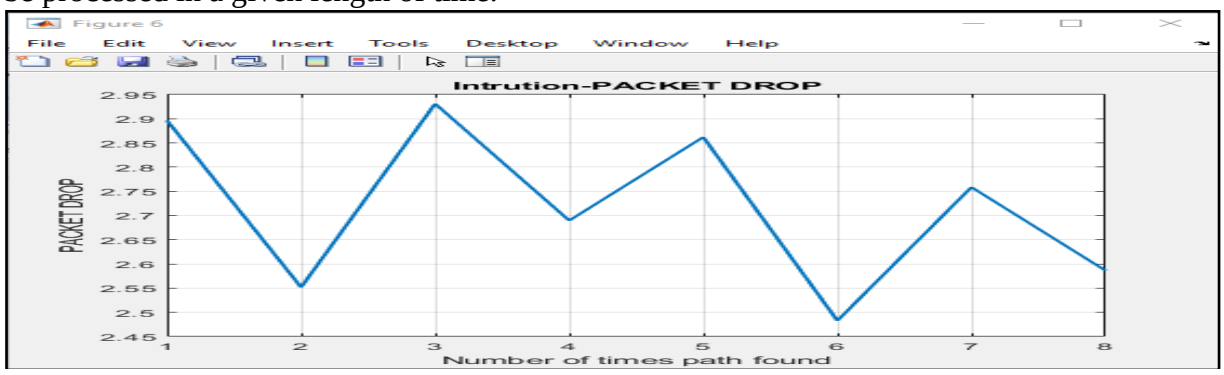

Figure.4.9 Intrusion Packet Drop

A decrease in intrusion packets is depicted in Fig.4.9. Congestions from high traffic, collisions on the connection layer, and buffer overflows are all potential causes of packet loss.

Table 4.1 Comparison result with the existing system

	Approaches	Accuracy performance (%)
Implementation work	Deep learning ResNet50	99.98
Previous Work [12]	Machine learning Xgboost	92.6

This table 4.1 shows the accuracy performance of different approaches in your work, where Deep Learning with ResNet50 achieved the highest accuracy at 99.98%, while previous work involved Machine learning Xgboost achieving an accuracy of 92.6 %.

CONCLUSION

In conclusion, the utilization of machine learning for intrusion detection in ad hoc networks represents a promising and innovative approach to address the challenges posed by security threats, particularly black hole assaults. The research findings suggest that the proposed method, which involves simulating and modeling black hole attacks in an ad hoc

networking environment, coupled with the application of machine learning algorithms, yields effective results in distinguishing between benign and malicious network activity. The ability of this approach to adapt to diverse classifiers underscores its versatility and potential for deployment in real-world scenarios. Despite the continuous evolution of attack strategies, the study highlights the relative efficacy of the machine learning-based intrusion detection system, emphasizing its capacity to enhance the security of ad hoc networks and contribute to the ongoing efforts to fortify these transient, self-organizing communication infrastructures.In the ever-evolving landscape of cybersecurity, where conventional systems may fall short, the ad hoc machine learning-based intrusion detection mechanism offers a dynamic and responsive solution. By incorporating advanced computational models and leveraging machine learning algorithms, the system demonstrates a capability to analyze crucial features and patterns, enabling the classification of network packets as either benign or malicious. The adaptability of the proposed approach to different classifiers signifies its potential applicability across diverse ad hoc network configurations. As the research contributes valuable insights into the feasibility and effectiveness of such a system, it encourages further exploration and development in the realm of intrusion detection, providing a robust defense against emerging security threats in ad hoc networks.

References

1. Y. Wang, V. Menkovski, I. W.-H. Ho, and M. Pechenizkiy, “VANET meets deep learning: the effect of packet loss on the object detection performance,” in 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Jun. 2019, pp. 1-5, doi: 10.1109/VTCSpring.2019.8746657.
2. D. Tian et al., “A distributed position-based protocol for emergency messages broadcasting in vehicular ad-hoc networks,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1218-1227, 2018, doi: 10.1109/JIOT.2018.2791627.
3. L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, “Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks,” International Journal of Distributed Sensor Networks, vol. 13, no. 3, 2017. doi: 10.1177/2F1550147717700899.
4. C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, “PBA: prediction-based authentication for vehicle-to-vehicle communications,” IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 1, pp. 71-83, 2016, doi: 10.1109/TDSC.2015.2399297
5. U. Rajput, F. Abbas, H. Eun, and H. Oh, “A hybrid approach for efficient privacy-preserving authentication in VANET,” IEEE Access, vol. 5, pp. 12014-12030, 2017, doi: 10.1109/ACCESS.2017.2717999.
6. T. Saeed, Y. Mylonas, A. Pitsillides, V. Papadopoulou, and M. Lestas, “Modeling probabilistic flooding in VANETs for optimal rebroadcast probabilities”, IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 556-570, 2019, doi: 10.1109/TITS.2018.2828413.
7. D. Krishnamoorthy et al., “An effective congestion control scheme for MANET with relative traffic link matrix routing,” Arabian Journal for Science and Engineering, vol. 45, pp. 1-11, 2020, doi: 10.1007/s13369-020-04511-9.
8. R. Vadivel and V. M. Bhaskaran, “Adaptive reliable and congestion control routing protocol for MANET,” Wireless Networks, vol. 23, no. 3, pp. 819-829, 2017, doi: 10.1007/s11276-015-1137-3.

9. Anish Halimaa A.; K. Sundarakantham Machine Learning Based Intrusion Detection System 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) Year: 2019 DOI: 10.1109/ICOEI.2019.8862784
10. Aditya Phadke;MohitKulkarni;PranavBhawalkar;Rashmi Bhattad A Review of Machine Learning Methodologies for Network Intrusion Detection 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) Year: 2019 | Conference Paper | Publisher: IEEE DOI: 10.1109/ICCMC.2019.8819748
11. Tommaso Zoppi;AndreaCeccarelli;AndreaBondavalli Into the Unknown: Unsupervised Machine Learning Algorithms for Anomaly-Based Intrusion Detection 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S) Year: 2020 | Conference Paper | Publisher: IEEE DOI: 10.1109/DSN-S50200.2020.00044
12. Muawia A. Elsadig (2023) Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach Digital Object Identifier 10.1109/ACCESS.2023.3303113 VOLUME 11, 2023