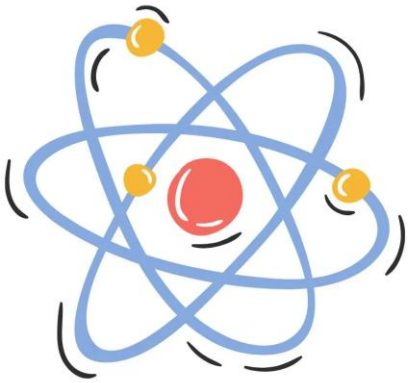

ISSN: 1672 - 6553

JOURNAL OF DYNAMICS AND CONTROL

VOLUME 9 ISSUE 7: 210 - 220

ELEVATING SECURITY MEASURES IN AD HOC NETWORKS: AN INTRUSION DETECTION APPROACH WITH DEEP LEARNING

[1]Meenakshi Nawal, [2]Medha Khenwar

[1]Associate Professor, Swami Keshwanand Institute of Technology, Management & Gramothan, Jaipur, India

[2]Assistant Professor, Suresh Gyan Vihar University, Jaipur, India

JOURNAL OF DYNAMICS AND CONTROL
DOI: https://doi.org/10.71058/jodac.v9i7015

ELEVATING SECURITY MEASURES IN AD HOC NETWORKS: AN INTRUSION DETECTION APPROACH WITH DEEP LEARNING

[1]Meenakshi Nawal, [2]Medha Khenwar

[1]Associate Professor, Swami Keshwanand Institute of Technology, Management & Gramothan, Jaipur, India

[2]Assistant Professor, Suresh Gyan Vihar University, Jaipur, India

[1]meenakshi.nawal@skit.ac.in, [2]Medhakhenwar.mk@gmail.com

ABSTRACT: Ad hoc networks, characterized by their ability to spontaneously establish connections without infrastructure, are increasingly utilized in disaster relief and military operations due to the ubiquity of wireless technology. However, their decentralized nature renders them vulnerable to attacks, such as the black hole assault, where rogue nodes disrupt routing. This study employs computer modeling to simulate such attacks and proposes a novel intrusion detection system based on machine learning algorithms, particularly utilizing the VGG architecture. The system aims to categorize network packets as safe or dangerous, enabling the identification of intrusions. Through experimentation, it is demonstrated that this method shows promise across various classifiers and can adapt to evolving attack strategies. The need for robust detection mechanisms persists amidst continuous changes in attack methodologies.

Keywords: Intrusions, Adhoc, networks, Data Sets, Deep Learning.

I INTRODUCTION

In the era of ubiquitous internet usage, safeguarding our computers and networks requires meticulous consideration. According to Kaspersky's findings [1], network attacks remained prevalent in 2019, with their security solutions successfully thwarting 975,491,360 risks originating from websites in 195 different countries. Consequently, robust defenses must be in place to counteract this persistent threat. The term "IDS" denotes an "intrusion detection system," a mechanism or device that diligently monitors system or network operations to identify unauthorized or unverified behavior [2]. Typically, this involves automatically collecting data from various system and network sources and scrutinizing it for potential vulnerabilities. Given the inherent uncertainty, ensuring the perpetual safety of data on internet-connected networks is an impractical guarantee. To mitigate risks, it is advisable to employ a variety of methods, as outlined by the IEEE x.805, where eight security factors align with potential security threats. Intrusion detection systems employ two primary approaches: "Signature" and "Anomaly" detection. In the signature-based detection process [3], samples' signatures are compared with those in a signature database, with the challenge lying in devising effective signatures. On the other hand, anomaly-based intrusion detection systems (IDS) aim to establish a normal behavior profile and subsequently identify abnormal behaviors based on deviations from this established norm [4]. Its primary function has been to identify previously undiscovered attacks. At the moment, most researchers in the field of network security are focusing on finding things that are out of the ordinary. Machine learning algorithms have been used a lot to improve IDS because they are very effective, flexible, and easy to use. Machine learning-based intrusion detection systems are now the standard in the industry. Instead of making a huge database

DOI: https://doi.org/10.71058/jodac.v9i7015

of signatures and turning the world into a data-driven organization, both the public and private sectors should focus on making decisions based on data. But because malicious attacks are so big and complicated, traditional machine learning algorithms have been fixed to fix some of their flaws. These flaws include a focus on processing low-dimensional data, an inability to deal with high-dimensional data, and a need for manual feature selection. Because there are so many and different kinds of malicious attacks, these flaws have been fixed.

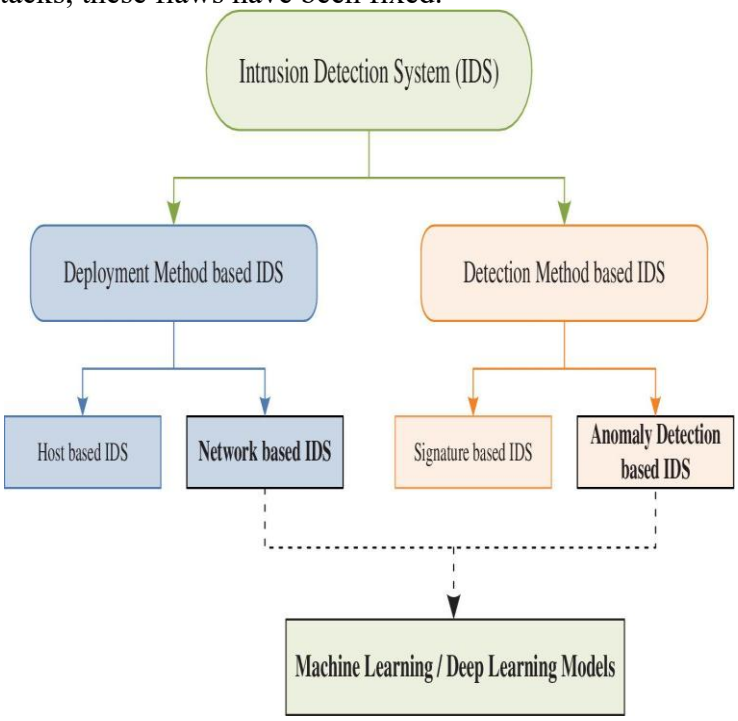

Figure 1.3: Classifications of IDS adopted from

Figure 1. Shows a description of the five steps that are taken to find an anomaly. It is known that machine learning has different steps, such as getting data from the network, the host, or both. Also, during data processing, the total amount of data is cut down. This is done through the processes of feature selection, feature extraction, and, finally, dimensionality reduction.

In the regular profiling learning stage [5], which looks at the data, the usual behavior is learned. During the process of anomaly detection, methods are used to find strange behaviors and patterns of behavior that are different from the norm. Last, it responds to the alarm in a different way depending on whether the profile is normal or abnormal. Intrusion Detection Systems are security systems that gather information from different sorts of system and network sources and then analyze this information to try to discover activity that could constitute an attack or intrusion on the system. The information that is gathered by Intrusion Detection Systems [6] comes from a wide variety of system and network backgrounds. Most of the time, the attacks are not just aimed at one computer. Instead, they are aimed at multiple hosts at the same time. Because of this, there is a chance that some incursions will behave strangely at the network layer, while others may behave strangely at the application layer. Data source-based approaches, which look at where the data source came from or where it is in a network, are used to put IDS into groups. Some examples of data source-based methods are network packets, payload, operating system logs, firewall logs, and network sensors. Intrusion detection systems can be either based on the host or on the network. A host-based intrusion detection system, also called a host-based intrusion detection system (HIDS) or host-based intrusion

DOI: https://doi.org/10.71058/jodac.v9i7015

detection system (IDS), is a piece of software that, once installed, monitors a single host for potentially malicious behavior by looking at what happens on that host [7]. HIDS are usually set up as software that runs on the protected host. This means that they need to be installed on each machine and set up in a way that is specific to the operating system. One of the benefits is that this proposed system is able to keep an eye on encrypted communication. It can also see what all users are doing, find out where attacks that come from within the host come from, and look at decrypted traffic to find attack signatures. On the other hand, one of the problems with host-based intrusion detection systems is that they take up a lot of storage space and extra processing power on the host where they are installed. [8]

II RELATED WORK

Pragathi Yelanki et al. (2021) The Vehicle Ad Hoc Network makes it possible for cable-driven vehicles to move around in a safer way (VANET). VANETs are known for being able to send data securely in limited amounts and on time over networks with changing topologies. Because the VANET system is wireless, attacks that send messages that aren't controlled by a protocol are more likely to work. So, it is important for the VANET protocol to have reliable message transport. After a lot of study of routing algorithms, a protocol called SOLSR (Security Optimized Link State Routing) was made for a Virtual Private Network (VANET). Elliptic Curve Cryptography (ECC) uses elliptically curved features to get the encryption key, while RSA uses different methods to get the key. The results show that SOLSR combined with ECC is the best way to encrypt messages while also cutting down on delays.

Saad Ali Alfadhli et.al (2020) The security of the Vehicle Ad Hoc Network depends a lot on the verification of vehicle data, as well as the integrity and privacy of the messages that are sent (VANET). Unfortunately, many of the ways that data is protected in VANETs do not offer the level of security and efficiency that is needed. It's also important to note that many of these methods depend heavily on system keys and long-term data stored in hardware that works well. Depending on the situation, such as accidental duplication or physical attacks, this could help or hurt on-board controlled devices (OBUs). So, any good authentication scheme must take into account these security concerns and the fact that some nodes have limited resources. To meet these needs, offer a full VANET privacy and authentication solution. Physical copy protection (PUF) and a single active doctor ID are used to make sure the item is real. A regional deployment of the CA also makes the region less dependent on system keys and makes the controls stronger. a unique identifier for a specific domain. When look closely, it can be seen that VANET is better than traditional methods in terms of cost-effectiveness, computing power, and meeting security criteria.[10]

Jianhong Zhang et.al (2021). To achieve minimum transmission delays and SSK updates at the same time, VANET has introduced a lightweight confidentiality authentication protocol. To reduce overhead communication, their project uses a signature strategy that requires message retrieval to achieve message validation. And they claim that the signatures used are secure against attacking selected messages and provide security credentials in detail. Unfortunately, this work is done by analyzing their guards. These systems show that the user is insecure and can be fraudulent in general. In other words, anyone can create a valid signature on any message. And finally, after considering the cause of the attack, to came up with possible suggestions to overcome the attack.[11]

III PROPOSED WORK

The proposed system aims to enhance network intrusion detection by leveraging the VGG16 architecture, a deep convolutional neural network renowned for its effectiveness in image

DOI: https://doi.org/10.71058/jodac.v9i7015

classification tasks. By adapting this architecture to analyze network traffic data, the system aims to detect and classify anomalous patterns indicative of intrusion attempts. This approach harnesses the power of deep learning to automatically learn and identify complex features within network traffic, enabling more accurate and efficient detection of malicious activities. By incorporating VGG16-based models into the intrusion detection system, the proposed framework aims to enhance network security by promptly identifying and mitigating potential threats, thereby bolstering overall network resilience and fortifying defenses against cyber-attacks—an approach increasingly adopted to address communication security issues prevalent in automotive environments.

Network Architecture: The components constituting the VANET [13] network can subscribe to three distinct categories. These encompass roadside facilities, servers handling applications and authorization, and nodes along with vehicles.

Server Devices - Operating as powerful entities, each server in this setup manages its own organization and service data. The overarching authority vested in these servers necessitates the establishment of a comprehensive care plan [17]. These computing devices provide crucial information about vehicle operations [14]. Funding from global governments and corporations supports these endeavors. The bulk of responsibilities lies with permission and application servers, although the duration required for computational tasks remains uncertain.

Roadside Infrastructure - The term "road infrastructure" denotes the activities involved in collecting and transmitting information, as well as situating power sources in proximity to roads. Radio waves facilitate communication between Roadside Units (RSUs) and vehicles, while wired networks supply the necessary power. Both radio waves and wired networks are indispensable for the effective functioning of RSUs [15][16].

Parameter	Value
Number of Nodes	100
Source node	20
Destination node	30
Data rate	8 packets/sec
City size	100
Bulk size	30

Table 1 Initial Parameters

DOI: https://doi.org/10.71058/jodac.v9i7015

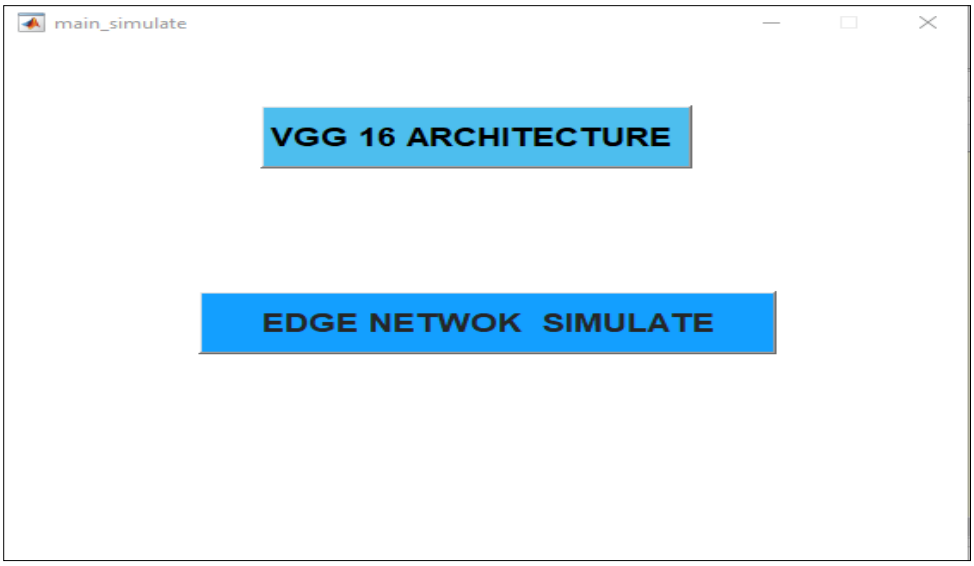

Fig.1 Training and Simulation Window

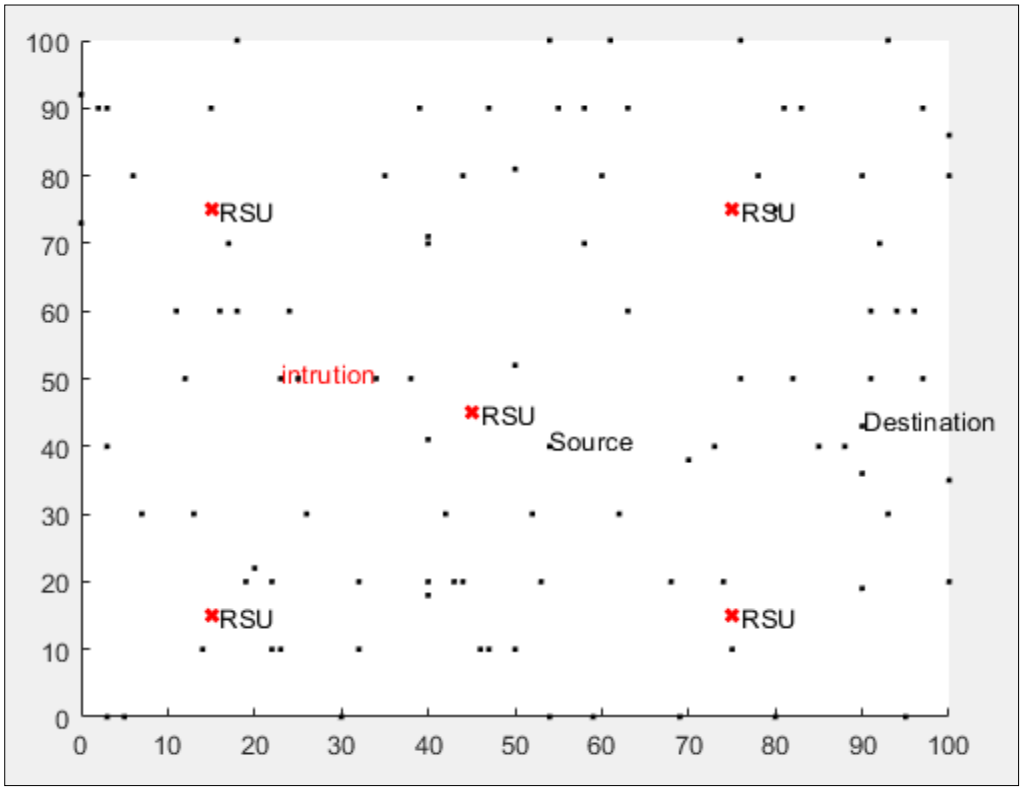

Fig. 2 network initialization

DOI: https://doi.org/10.71058/jodac.v9i7015

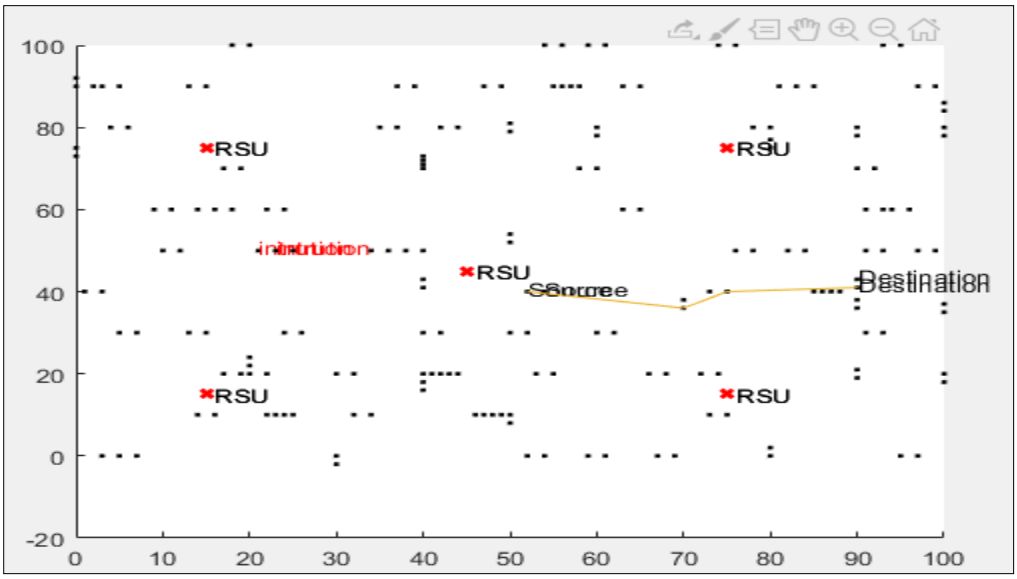

Fig.3 data transmission

```
original_path =

    20     5    30

ATTACK FOUND

new_path =

    20    11    30


original_path =

    20    32     5    30

ATTACK FOUND

new_path =

    20    32    30


original_path =

    20    32     5    30
```

Fig.4 Attack detection a mitigation

DOI: https://doi.org/10.71058/jodac.v9i7015

The original path was from node 20 to node 5 to node 30. An attack was found, prompting a change in the path to go from node 20 to node 11 to node 30. In the second case: The original path was from node 20 to node 32 to node 5 to node 30. An attack was found, resulting in the removal of node 5 from the path, so the new path goes from node 20 to node 32 directly to node 30.

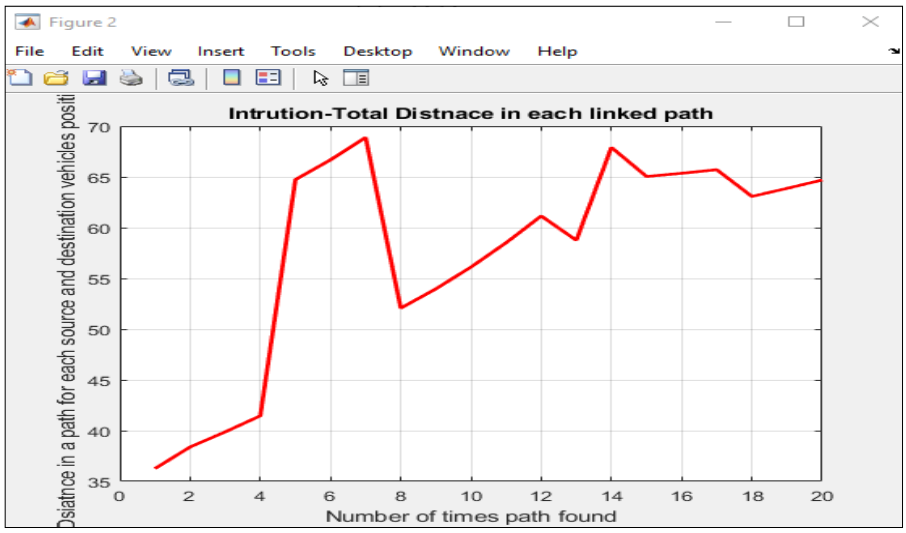

Fig. 5 Total Number of path of simulation

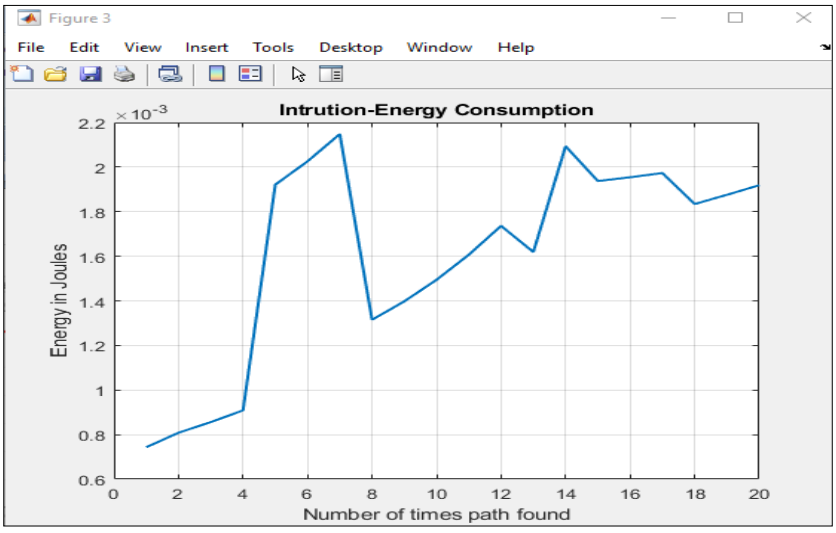

Fig.6 performance of Energy Consumption

DOI: https://doi.org/10.71058/jodac.v9i7015

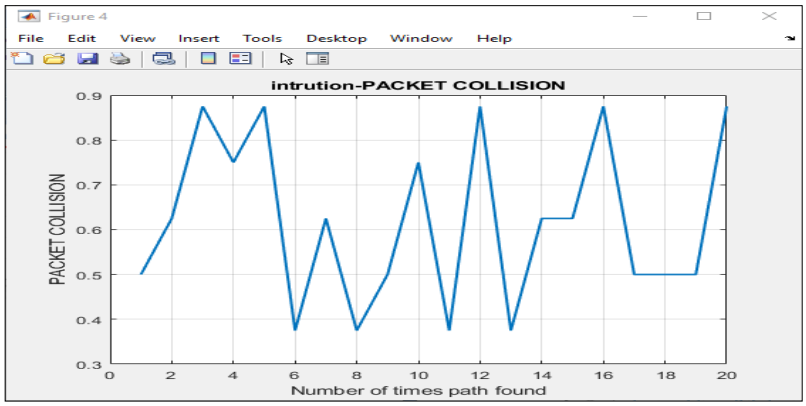

Fig. 7 performance of Packet Collision

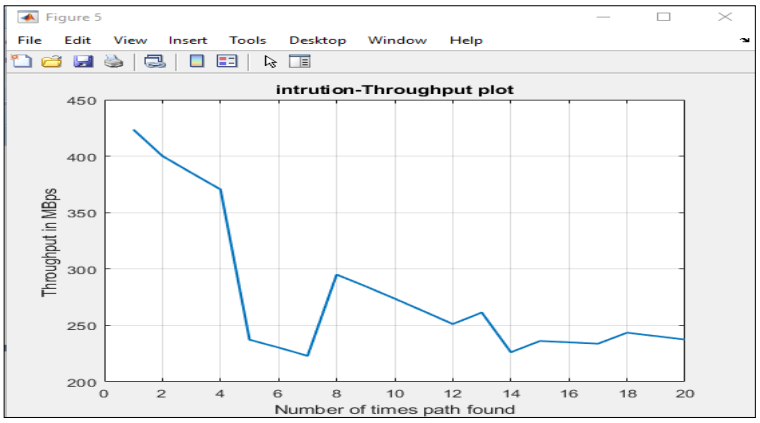

Fig. 8 performance of throughput

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.

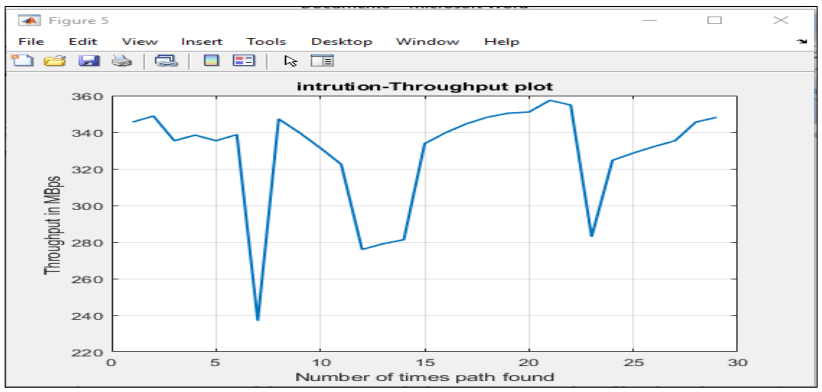

Fig. 9 Intrusion Throughput

DOI: https://doi.org/10.71058/jodac.v9i7015

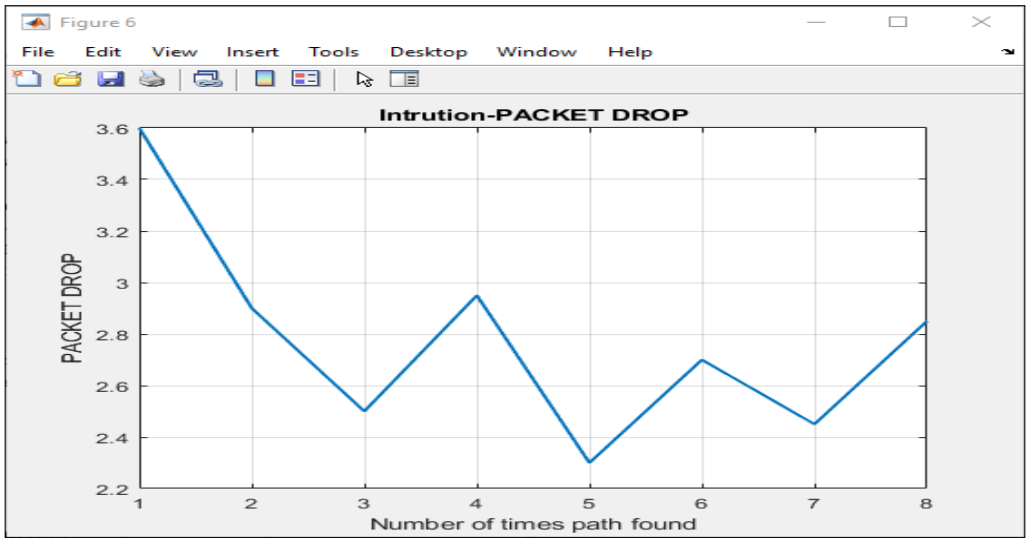

Fig. 10 performance Intrusion Packet Drop

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.

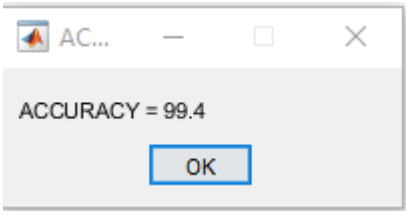

Fig. 11 Accuracy of the System

Table 2 performance of the proposed system

	Studies	Accuracy (%)
VGG16-Based Intrusion Detection (Proposed)	VGG16	99.4 %
Machine leaning (existing work)	long short-term memory networks	97 %
	K-Nearest Neighbors	92 %

This table 2 shows the accuracy performance of different approaches in work, where Deep Learning with VGG16 achieved the highest accuracy at 99.4%, while previous work involved

DOI: https://doi.org/10.71058/jodac.v9i7015

Machine Learning approaches with LSTM achieving an accuracy of 97% and K-Nearest Neighbors (KNN) achieving an accuracy of 92%.

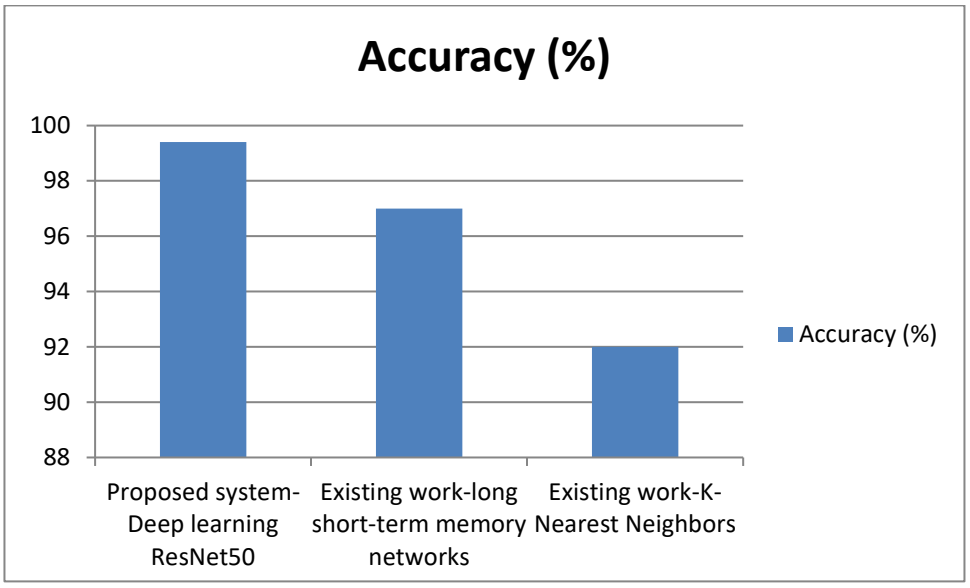

Fig.12 Comparison result with the existing system

IV CONCLUSION

In the contemporary landscape, an increasing number of products and services are interconnected through networks, making it challenging to anticipate communication patterns. This trend has facilitated easier interaction among individuals and improved collaboration between systems and services via computer networks. These networks are dynamic, continuously expanding, and undergoing substantial changes. The application of the VGG16 architecture, a deep learning model, for intrusion detection purposes holds significant potential in elevating network security, especially in contexts like vehicle networks where attacks can present substantial risks. By leveraging VGG16's capabilities in image classification and feature extraction, it becomes possible to detect anomalies or intrusions within the network traffic data. VGG16 can analyze network traffic patterns and identify deviations from normal behavior, thus alerting the system to potential security breaches.

REFERENCE

1. Wei, L., Cui, J., Xu, Y., Cheng, J., & Zhong, H. (2020). Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs. IEEE Transactions on Information Forensics and Security, 16, 1681-1695.
2. Krzysztof Stępień;Aneta Poniszewska-Marańda Security methods against Black Hole attacks in Vehicular Ad-Hoc Network 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA) Year: 2020
3. Pragathi Yellanki;M.V.S Phani Narasimham Secure Routing Protocol for VANETS using ECC 2020 International Conference on Computer Science, Engineering and Applications

DOI: https://doi.org/10.71058/jodac.v9i7015

(ICCSEA) Year: 2020
4. Hritik Sateesh;Pavol Zavarsky State-of-the-Art VANET Trust Models: Challenges and Recommendations 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) Year: 2020
5. A.M.R. Tolba Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs IEEE Access Year: 2018
6. Muhammad Umar Sattar;Rana Asif Rehman Interest Flooding Attack Mitigation in Named Data Networking Based VANETs 2019 International Conference on Frontiers of Information Technology (FIT) Year: 2019
7. Kuldeep Narayan Tripathi;S. C. Sharma;Ashish Mohan Yadav Analysis of Various Trust based Security Algoithm for the Vehicular AD-HOC Network 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE) Year: 2018
8. Sushil Kumar;Kulwinder Singh Mann Detection of Multiple Malicious Nodes Using Entropy for Mitigating the Effect of Denial of Service Attack in VANETs 2018 4th International Conference on Computing Sciences (ICCS) Year: 2018
9. Jeevitha R.;N. Sudha Bhuvaneswari Malicious node detection in VANET Session Hijacking Attack 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) Year: 2019
10. Pragathi Yellanki;M.V.S Phani Narasimham Secure Routing Protocol for VANETS using ECC 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA) Year: 2020
11. Saad Ali Alfadhli;Songfeng Lu;Kai Chen;Meriem Sebai MFSPV: A Multi-Factor Secured and Lightweight Privacy-Preserving Authentication Scheme for VANETs IEEE Access Year: 2020
12. Jianhong Zhang;Qijia Zhang On the Security of a Lightweight Conditional Privacy-Preserving Authentication in VANETs IEEE Transactions on Information Forensics and Security Year: 2021
13. Jingxuan Lyu;Chenju Chen;Hui Tian Secure Routing Based on Geographic Location for Resisting Blackhole Attack In Three-dimensional VANETs 2020 IEEE/CIC International Conference on Communications in China (ICCC) Year: 2020
14. C. Kalaiarasy;N. Sreenath;A. Amuthan Location Privacy Preservation in VANET using Mix Zones – A survey 2019 International Conference on Computer Communication and Informatics (ICCCI) Year: 2019
15. Rachael N. Nabwene Review on Intelligent Internal Attacks Detection in VANET 2018 4th Annual International Conference on Network and Information Systems for Computers (ICNISC) Year: 2018
16. Wei Li;Dongmei Zhang RSSI Sequence and Vehicle Driving Matrix Based Sybil Nodes Detection in VANET 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN) Year: 2019
17. Bhawsar, S., & Joshi, K. (2021). A Review on Clouds Security Based Encryption and Decryption Techniques. *IJERT 2021*.
18. Chang, J., Li, H., Zhao, J., Guan, X., Li, C., Yu, G., ... & Fang, Q. (2021). Tetrathiafulvalene-based covalent organic frameworks for ultrahigh iodine capture. *Chemical Science*, *12*(24), 8452-8457.