ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"DEEP LEARNING TECHNIQUE BASED INTRUSION DETECTION SYSTEM FOR AODV NETWORK"

***Pushpendra Kumar Chandel* [1], *Prof. Varsha Thakur* [2]**
[1] *M.Tech Scholar, Mittal Institute of Technology Bhopal, India*
[2] *Assistant Professor, Mittal Institute of Technology Bhopal, India*
Pc60832@gmail.com , *Anantha.thakur@gmail.com*

ABSTRACT

In the realm of network security, Intrusion Detection Systems (IDS) play a pivotal role in safeguarding networks against various threats and attacks. In particular, Ad hoc On-Demand Distance Vector (AODV) networks, known for their dynamic and decentralized nature, require robust intrusion detection mechanisms to ensure their security. This study delves into the performance evaluation of an Intrusion Detection System tailored for AODV networks, leveraging the VGG16 architecture, a well-established deep learning model. Our research encompasses comprehensive experiments and analyses to assess the effectiveness of this IDS in detecting and mitigating intrusions within AODV networks. The study scrutinizes critical metrics such as detection accuracy, false-positive rates, and computational efficiency, providing insights into the system's efficacy. The results offer valuable guidance for enhancing the security of AODV networks through advanced intrusion detection techniques.

Keyword: *AODV, Intrusion Detection, Wireless network, VANET, Routing Protocol.*

I. INTRODUCTION

Information Security is a key concern in the modern information process due to expanding computer technology with the threat it faces – loss of stored, processes and transmit information through the network. In the 90's, the beginning of an Internet era is providing a huge transformation on information technology, because of the data transmission and communication channel to become more easily usable. It was a fixed network of computers that allowed the first millions of Internet users to communicate via e-mail. However, with the arrival of the Internet, personal computers and computer networks vulnerability increases to various kinds of attacks.
Heavy reliance on the Internet and worldwide connectivity has greatly increased the potential damage that can be inflicted by remote attacks launched over the Internet. And results of using Internet become with threat on information hijack and lose stored data. Intruders make use of the security breaches present in the system or network to attack it [1]. Intrusion is a purposefully illegal attempt to access information, manipulate information or render a system untrustworthy or inoperative. Computer and network security is become a major concern in our daily life experience on the Internet. According to Kaspersky 2019 statistical reporting period, network attacks continued to be one of the most common types of attacks [2]. Kaspersky solutions repelled attacks launched from online resources located all over the world. So, there should be mitigation for this threat. One of the major goals of network security is to detect an attack on network traffic. There are different ways to prevent and protect organizations network resources due to confidentiality, availability and integrity. Some of them are installing anti-virus software, firewalls, cryptography, intrusion detection system, and authentication and authorization. Amongthem, intrusion detection system (IDS) has been considered to be one of the most

promising methods for defending complex and dynamic intrusion behaviors.

Intrusion Detection AODV (IDAODV)

Intrusion Detection Systems (IDS) play a crucial role in safeguarding the integrity and security of network communications, particularly in the context of Ad hoc On-Demand Distance Vector (AODV) networks. AODV is a popular routing protocol widely used in Mobile Ad hoc Networks (MANETs) due to its adaptability to dynamic and decentralized network environments. However, the very attributes that make AODV efficient also render it susceptible to security threats.

In this context, IDS tailored for AODV networks are indispensable. These systems are designed to detect and thwart various intrusion attempts that could compromise the stability and confidentiality of data transmissions within the network. They employ a range of techniques, including anomaly detection and signature-based methods, to monitor network traffic and identify deviations from normal behavior.[3-4]

The primary objective of an IDS in an AODV network is to promptly recognize and respond to unauthorized access, malicious activities, or anomalies in the routing and data forwarding processes. By doing so, they help mitigate potential threats, maintain the integrity of routing tables, and ensure the reliable functioning of the network.

These IDSs serve as a critical line of defense in securing AODV-based networks, assisting in the prevention and containment of potential attacks, and contributing to the overall robustness of MANETs in dynamic and challenging environments. Their effectiveness in detecting and mitigating threats in AODV networks is paramount for ensuring the continued reliability and security of these decentralized communication systems.[5]

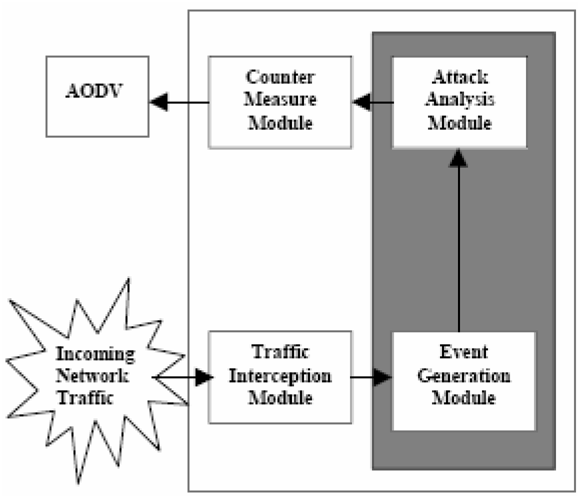

Fig. 1.Intrusion Detection AODV (IDAODV)

1) Route Disruption: Route Disruption refers to either destroying an existing route or blocking the establishment of a new one. Route Disruption refers to either destroying an existing route or blocking the establishment of a new one.

2) Route Invasion: A route invasion occurs when an inside attacker inserts themselves into a communication path between two endpoints.

3) Node Isolation: Isolating a node means blocking it from connecting with other nodes in the network. Node isolation varies from Route Disruption in that Route Disruption targets a route with two specified endpoints, whereas node isolation targets all conceivable routes.

4) Resource Consumption: Resource consumption refers to the utilization of network communication bandwidth or individual node storage space. For instance, an inside attacker could use network bandwidth by creating a network loop.

5) Denial of Service: The following misuse activities or attacks may be employed to attain objectives

Intrusion Detection System-Network attacks are a group of hostile actions that try to stop, stop, slow down, or

ISSN : 2455-9679
SJIF Impact Factor : 6.008

damage information and services that are stored in computer networks. An attack on a network is done by changing the way data flows through the network. The goal is to make computer network systems less available, less secure, or less secret. Computer attacks include viruses that come with emails, unauthorized use of a system, Internet worms, and denial of service attacks, which are done by abusing a feature of a system or taking advantage of a bug in software to change system data. Several attack identification systems have been made, and they are used by a lot of people today. These systems look at the data of a network to see if it is different from what a system or user would normally do [6-7]. Hackers have come up with a wide range of methods, from simple to complicated, to carry out their illegal activities. Also, the vast majority of attacks take advantage of weaknesses in different hardware and software parts of network systems that are connected to each other [8-10]. Some people might also look through the data for a pattern of an attack that they already know. Intrusion Detection Systems (IDS) are the name for these kinds of systems.

II. RELATED WORK

S. Shinly Swarna Sugi (2020) et.al Internet of Things (IoT) combines the internet and physical objects to transfer information among the objects. In the emerging IoT networks, providing security is the major issue. IoT device is exposed to various security issues due to its low computational efficiency. In recent years, the Intrusion Detection System valuable tool deployed to secure the information in the network. This article exposes the Intrusion Detection System (IDS) based on deep learning and machine learning to overcome the security attacks in IoT networks. Long Short-Term Memory (LSTM) and K-Nearest Neighbor (KNN) are used in the attack detection model and performances of those algorithms are compared with each other based on detection time, kappa statistic, geometric mean, and sensitivity. The effectiveness of the developed IDS is evaluated by using Bot-IoT datasets [11].

Indrajit Das (2021) et.al Cyber-attacks have been the major concern with the growing advancement in technology. Complex security models have been developed to combat these attacks, yet none exhibit a full-proof performance. Recently, several machine learning (ML) methods have gained significant popularity in offering effective and efficient intrusion detection schemes which assist in proactive detection of multiple network intrusions, such as Denial of Service (DoS), Probe, Remote to User (R2L), User to Root attack (U2R). Multiple research works have been surveyed based on adopted ML methods (either signature-based or anomaly detection) and some of the useful observations, performance analysis and comparative study are highlighted in this paper. Among the different ML algorithms in survey, PSO-SVM algorithm has shown maximum accuracy. Using RBF-based classifier and C-means clustering algorithm, a new model i.e., combination of serial and parallel IDS is proposed in this paper. The detection rate to detect known and unknown intrusion is 99.5% and false positive rate is 1.3%. In PIDS (known intrusion classifier), the detection rate for DOS, probe, U2R and R2L is 99.7%, 98.8%, 99.4% and 98.5% and the False positive rate is 0.6%, 0.2%, 3% and 2.8% respectively. In SIDS (unknown intrusion classifier), the rate of intrusion detection is 99.1% and false positive rate is 1.62%. This proposed model has known intrusion detection accuracy similar to PSO - SVM and is better than all other models. Finally, the future research directions relevant to this domain and contributions have been discussed[12].

Abhinav Singhal (2021) et.al this paper outlines an approach to build an Intrusion detection system for a network interface device. This research work has developed a hybrid intrusion detection system which involves various machine learning techniques along with inference detection for a comparative analysis. It is explained in 2 phases: Training (Model Training and Inference Network Building) and Detection phase (Working phase). This aims to solve all the current real-life problem that exists in machine learning algorithms as machine learning techniques are stiff they have their respective classification region outside which they cease to work properly. This paper aims to provide the best working machine learning technique out of the many used. The machine learning techniques used in comparative analysis are Decision Tree, Naïve Bayes, K-Nearest Neighbors (KNN) and Support Vector Machines (SVM) along with NSLKDD dataset for testing and training of our Network Intrusion Detection Model. The accuracy recorded for Decision Tree, Naïve Bayes, K-Nearest Neighbors (KNN) and Support Vector Machines(SVM) respectively when tested independently are 98.088%, 82.971%, 95.75%, 81.971% and when tested with inference detection model are 98.554%, 66.687%, 97.605%, 93.914%. Therefore, it can be concluded that our inference detection model helps in improving certain factors which are not detected using conventional machine learning techniques [13].

ISSN : 2455-9679
SJIF Impact Factor : 6.008

III. Proposed Approach

The proposed IDS, powered by deep learning techniques, is engineered to continuously monitor network traffic, scrutinize routing updates, and detect deviations from normal behavior. It has the capacity to identify various intrusion attempts, ranging from packet spoofing and routing attacks to denial-of-service (DoS) assaults, with a high degree of accuracy and responsiveness. The deep learning model's ability to adapt and self-learn from evolving threats sets it apart, making it a dynamic defense mechanism for AODV networks.By integrating this state-of-the-art IDS into AODV networks, we aim to fortify their resilience against emerging security threats. This proactive approach enables real-time threat detection and mitigation, reducing the potential impact of security breaches on network performance and data confidentiality. The proposed system represents a significant step toward achieving a more secure and reliable AODV network infrastructure in the face of evolving cyber threats and adversarial challenges

IV. Network Model

The network model for Vehicular Ad Hoc Networks (VANETs) can be categorized into three key components, each serving a specific role in the network ecosystem:

1. Application and Authorization Servers:

These servers are high-performance computing systems responsible for managing and delivering service-related data within the VANET. The authority, or the entity overseeing the network, possesses all the necessary cryptographic keys and assumes responsibility for network maintenance and planning.

In the context of vehicles, device servers provide operational details and facilitate communication. Funding for these servers can be provided by government entities or foreign operators. It is assumed that these servers have significant processing capabilities, and computational time is not a limiting factor in this model.

2. Road Side Infrastructure (RSU)

Road Side Infrastructure is composed of power supply units strategically located along roadways. These RSUs play a vital role in collecting and disseminating data within the VANET. RSUs are typically connected to power sources via wired networks and communicate wirelessly with vehicles. Their primary function is to act as intermediaries between the application and authorization servers and the vehicles on the road.[14]

3. Nodes/Vehicles

Nodes or vehicles represent the mobile entities within the VANET[15]. They move along roadways and engage in communication with RSUs as well as with each other. Each vehicle is equipped with a differential GPS receiver, offering meter-level accuracy in location tracking.

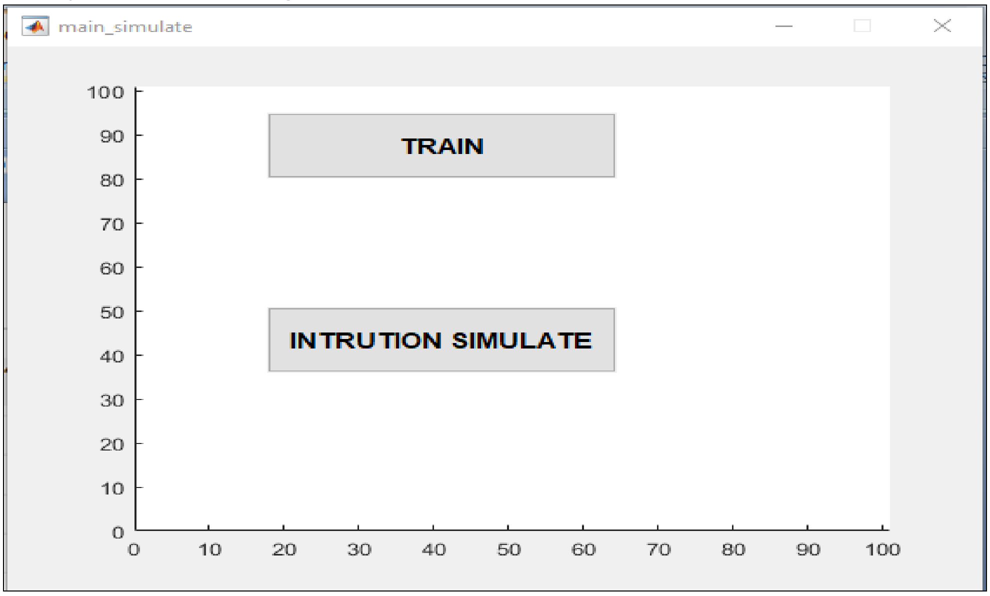

Fig.2 Training and Simulation Window

ISSN : 2455-9679
SJIF Impact Factor : 6.008

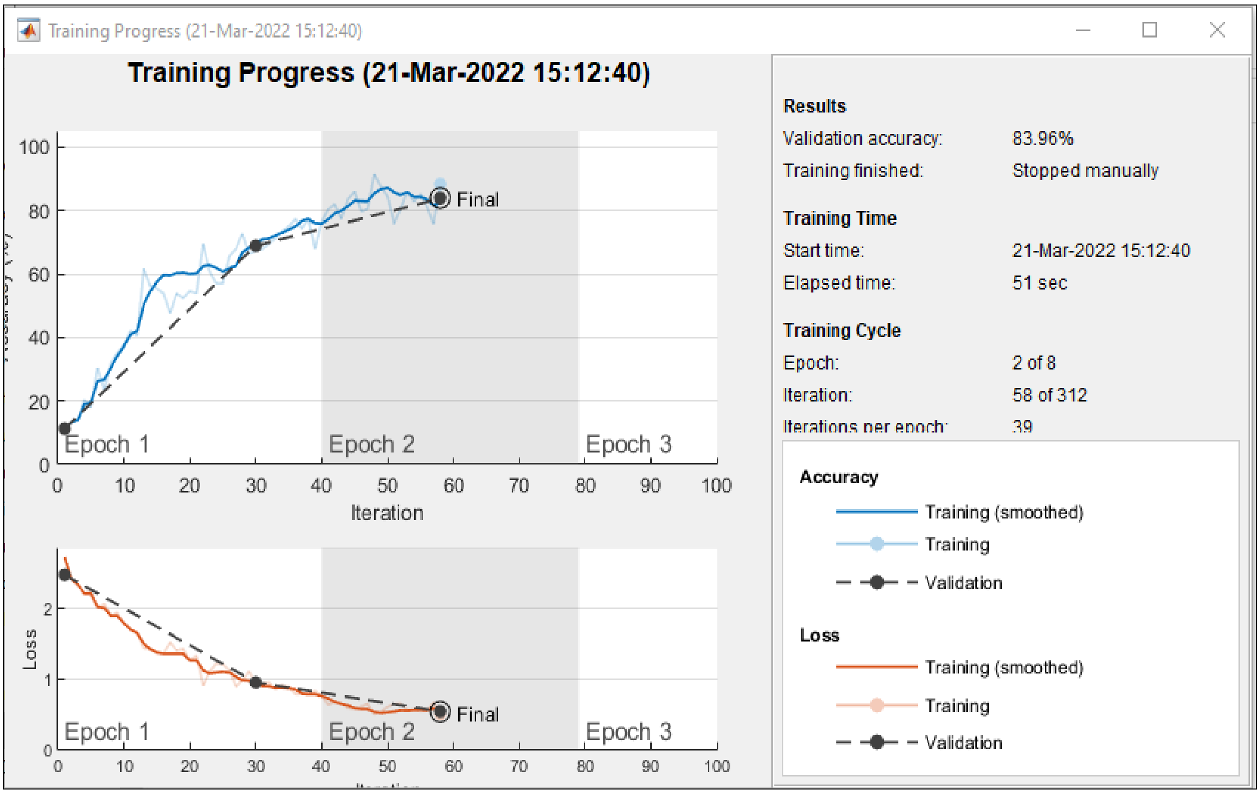

Fig.3 Training Process Window

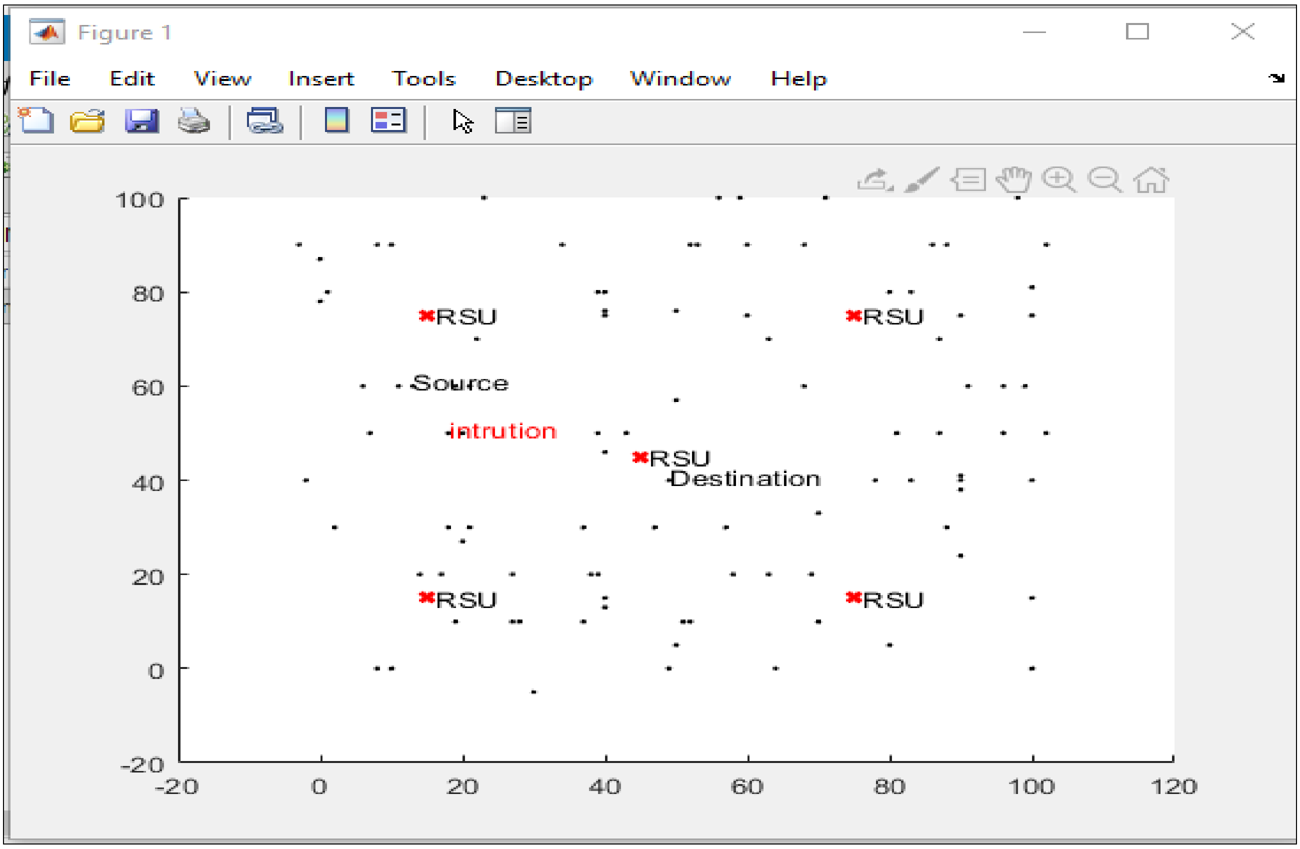

Fig.4 Network Architecture

ISSN : 2455-9679
SJIF Impact Factor : 6.008

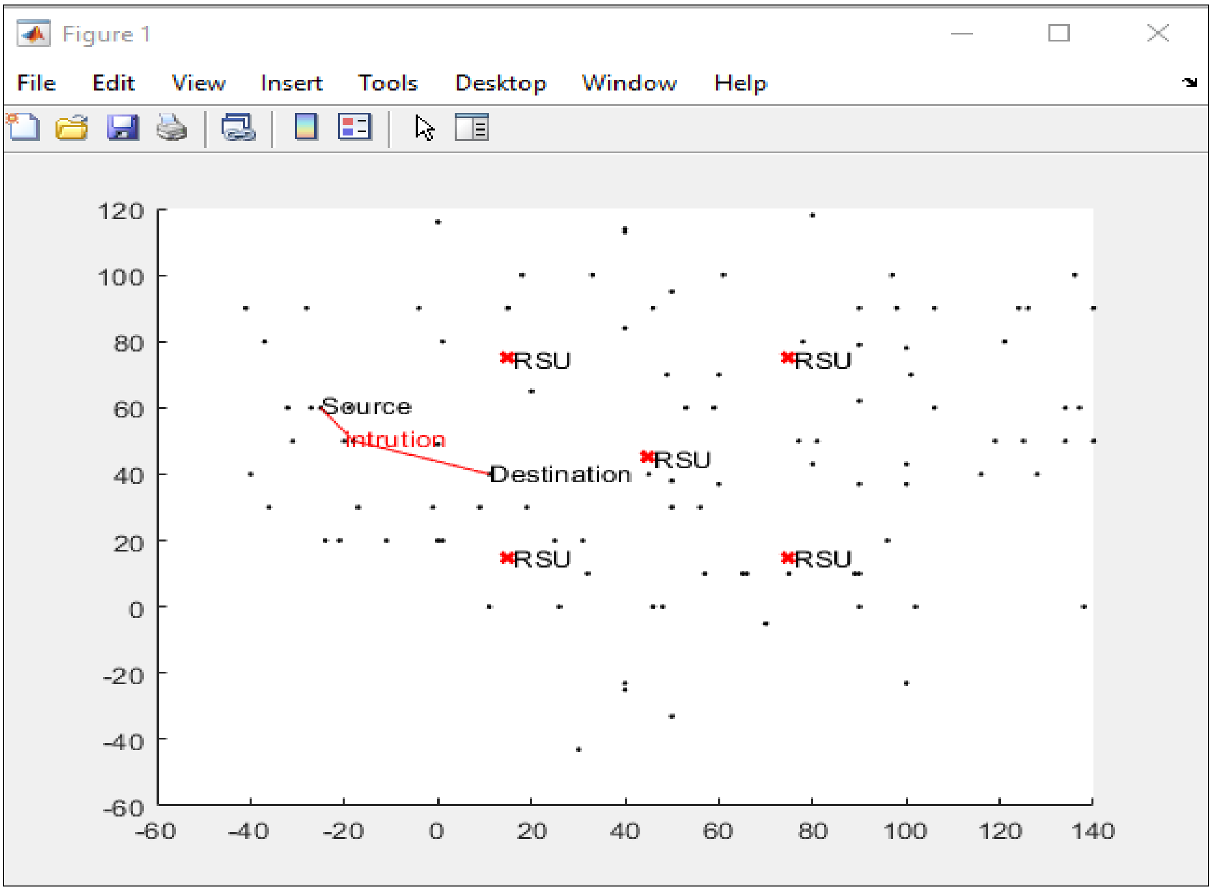

Fig.5 Network Architecture

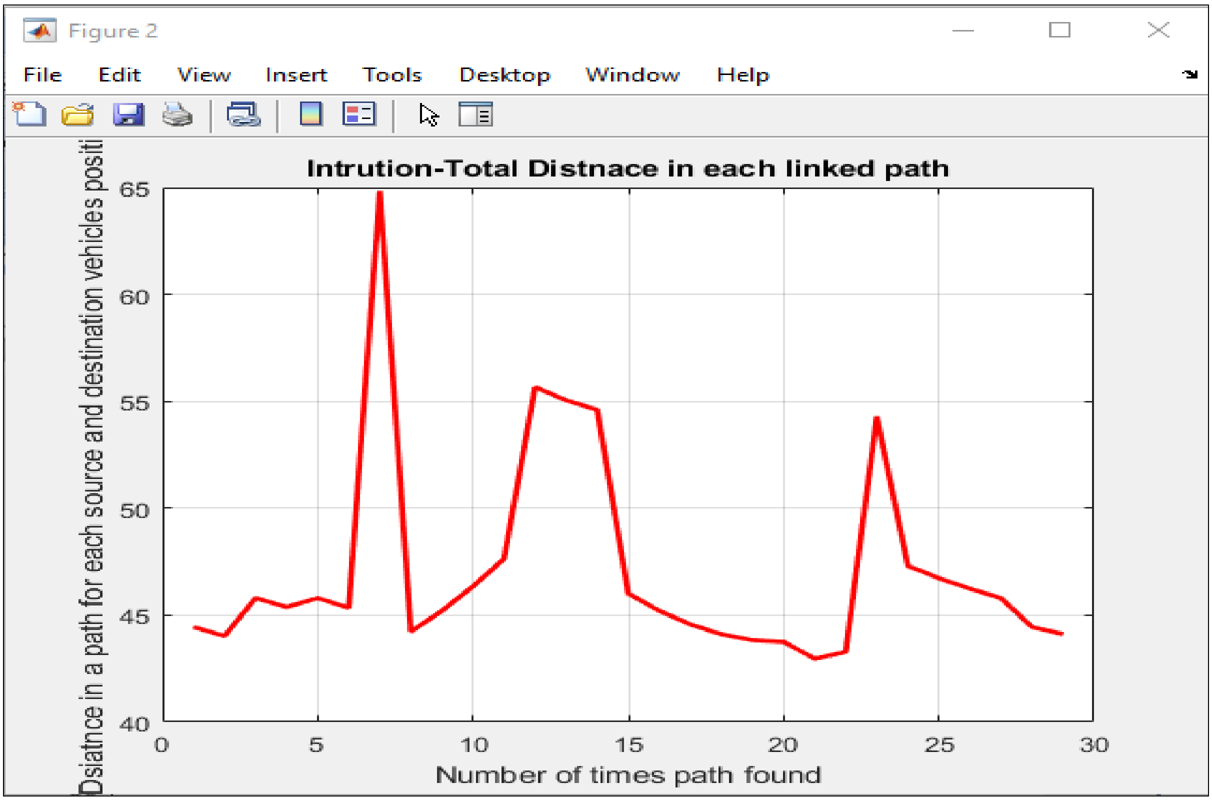

Fig.6 Total Number of Linked Path

ISSN : 2455-9679
SJIF Impact Factor : 6.008

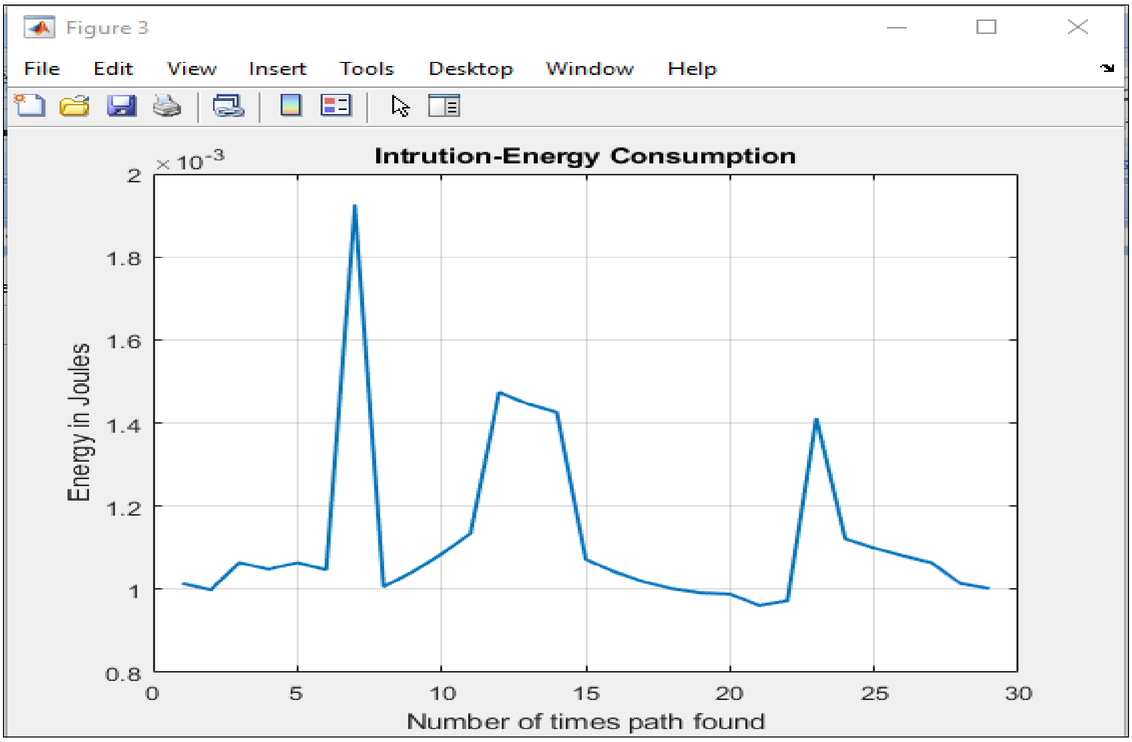

Fig.7 Intrusion Energy Consumption

Energy consumption in general is one of biggest challenges when it comes to wireless sensor networks (WSNs). Since the biggest amount of energy is used for communication, the most logical way to reduce the energy consumption is to reduce the number of packets transmitted between sensor and sink node. In the fig less energy consumption showing in fig.7

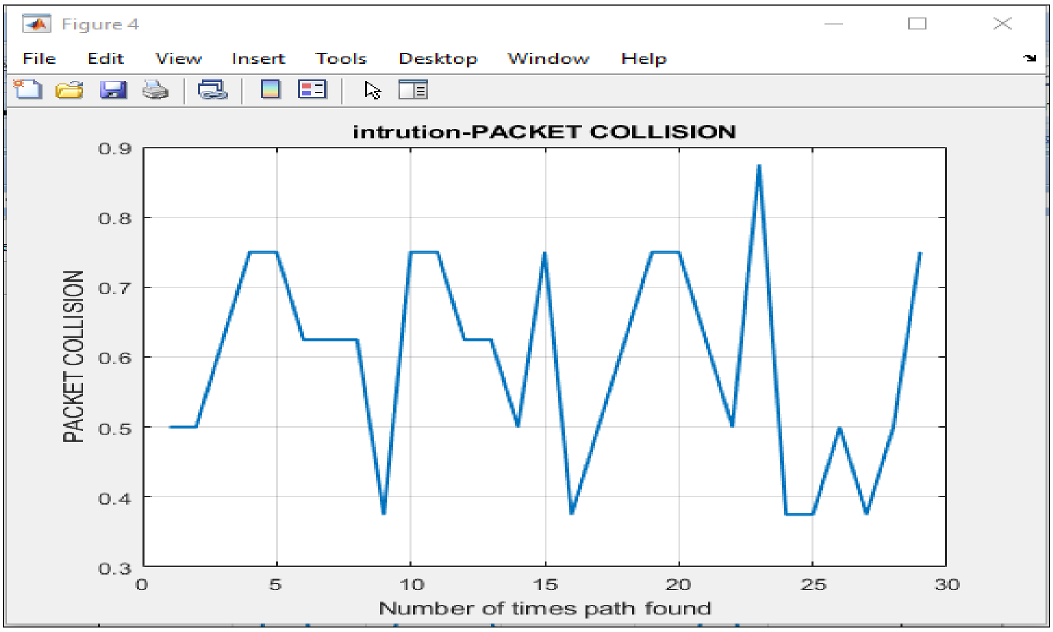

Fig.8 Packet Collision

Fig.8 showing the packet collision occurs when two or more nodes attempt to transmit a packet across the network at the same time. The transmitted packets must be discarded and then retransmitted, thus the retransmission of those packets increases the energy consumption and the latency

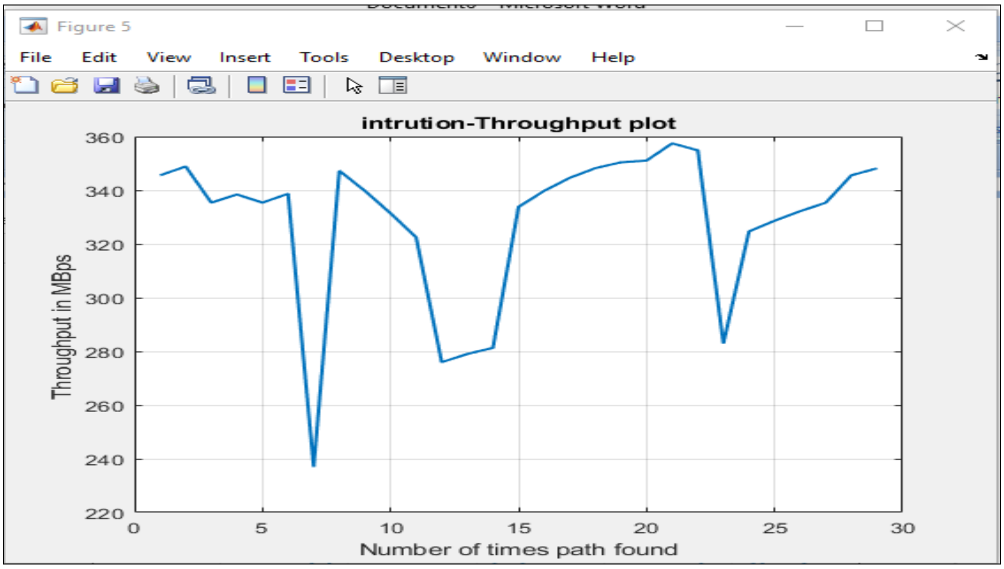

Fig.9 Intrusion Throughput

Throughput is a measure of total units of information a system can process in a given amount of time the intrusion throughput of the network showing in the fig 9

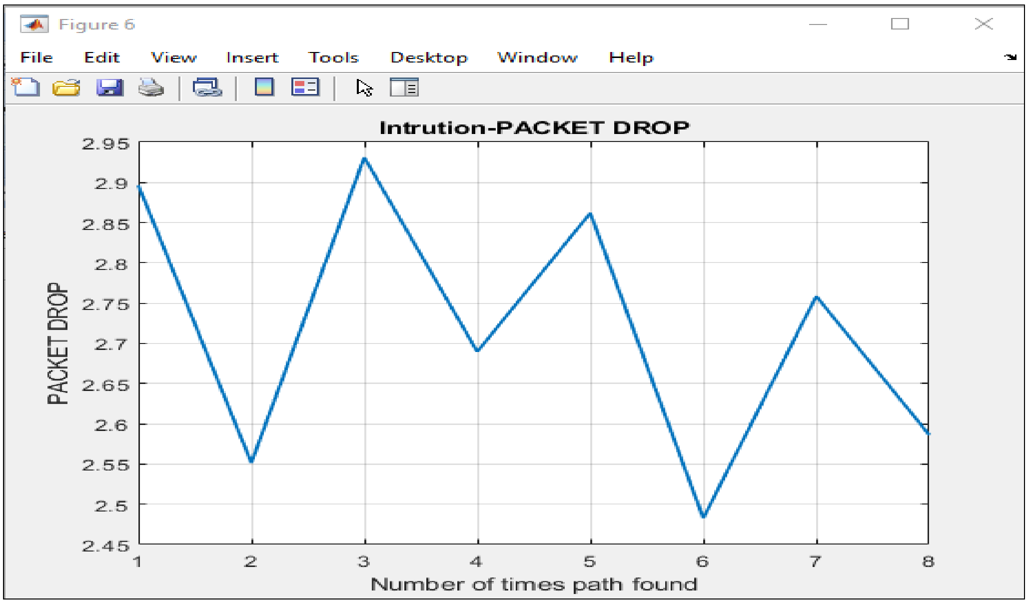

Fig.10 Intrusion Packet Drop

intrusion packet drop showing in the fig.10 Packet loss can be caused by congestions due to heavy traffic, collisions at link layer, buffer overflows,

Performance accuracy is often expressed as a ratio or percentage, representing the number of correct predictions divided by the total number of predictions made by a model. The formula for accuracy is as follows:

Accuracy = (Number of Correct Predictions) / (Total Number of Predictions)

Table 1 Comparison result with the exixsting system

	Techniques	Accuracy (%)
Proposed system	**VGG16**	**99.2**
Existing system	**LSTM**	**97.28**

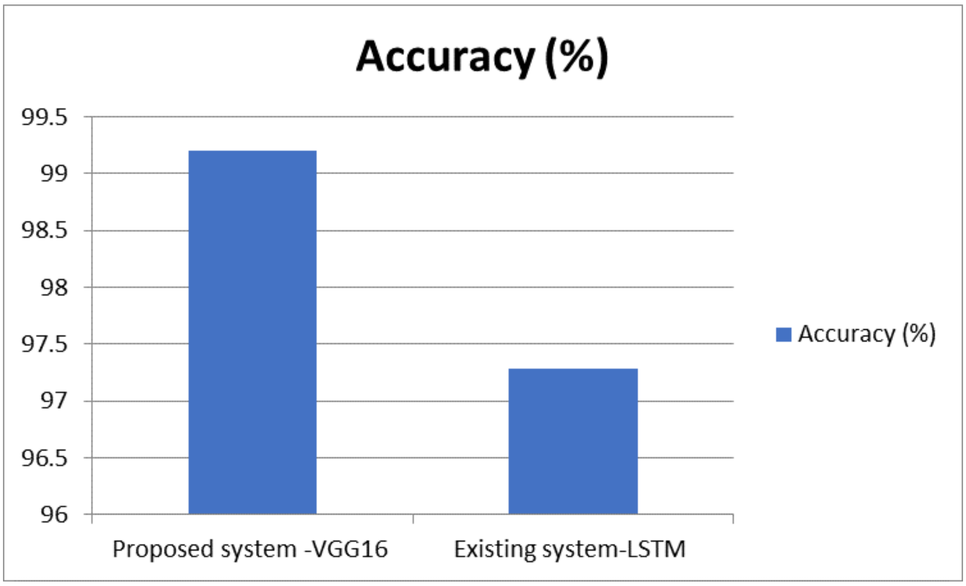

Fig. 11 comparison result with the existing system

V. Conclusion

Nowadays a growing of interconnected devices and services lead a world communication environment more complex and undetermined by human capability. Computer networks are dynamic, growing, and continually evolving with assisting human communication and integration of systems and services. Hackers or intruders have been affecting this interconnected environment by disrupting or break up with steal of information for personal purpose or advance. As complexity grows, it becomes harder to effectively communicate to human decision-makers the results of methods and metrics for monitoring networks, classifying traffic, and identifying malicious or abnormal events. Security experts require tools that support them understand the reason for, and make decisions about the information their analytic systems produce. In order to support security experts, in this data driven world using deep learning algorithms as back-end engine is more support automatically to identify malicious and normal network traffics. An Intrusion Detection System aiming at securing the AODV protocol has been developed using specification based technique. We have proposed an intrusion system tool for preventing some internal attacks in AODV. The results of our implementation show that the performance of AODV routing protocol is improved significantly under attacks. In all the cases, the attack was detected as a violation to one of the AODV protocol specifications. The work can be extended to study the robustness of Wireless Ad Hoc Networks for all types of protocols. A study can be conducted on the relationship between the average detection delay and the mobility of the nodes. More types of attacks including group attacks can be studied and their relations to the vulnerability of the protocols can be ascertained.

REFERENCES

[1] Peng Ning, Kun Sun, "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Adhoc Routing Protocols," in Proceedings of the 4th Annual IEEE Information Assurance Workshop, pages 60-67, West Point, June 2003.

[2] S. Bouchegger and J. –Y. L. Boudec. Performance Analysis of the Confidant Protocol. In Proceedings of the 3rd ACM Symposium on Mobile Ad Hoc Networking and Computing. Pp 226-236, 2002.

[3] L. Buttyán and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks Technical Report No. DSC/2001/046, Swiss Federal Institute of Technology, Lausanne, August 2001

[4] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks. In Proceedings of the Eighth ACM Intl. Conf. on Mobile Computing and Networking (MobiCom '02), ACM, Atlanta, Sept. 2002, pp 12-23.

[5] R. C. Staudemeyer, "Applying long short-term memory recurrent neural networks to intrusion detection,"

ISSN : 2455-9679
SJIF Impact Factor : 6.008

South African Computer Journal, vol. 56, no. 1, p. 136–154, 2015.

[6] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," pp. 1–5, 2016 International Conference on Platform Technology and Service (PlatCon), 2 2016.

[7] T. T. H. Le, J. Kim, and H. Kim, "An effective intrusion detection classifier using long short-term memory with gradient descent optimization," pp. 1–6, 2017 International Conference on Platform Technology and Service (PlatCon), 2 2017.

[8] P Illavarason;B Kamachi Sundaram A Study of Intrusion Detection System using Machine Learning Classification Algorithm based on different feature selection approach 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) Year: 2019 | Conference Paper | Publisher: IEEE DOI: 10.1109/I-SMAC47947.2019.9032499

[9] Wei Zhong;Ning Yu;Chunyu Ai Applying big data based deep learning system to intrusion detection Big Data Mining and Analytics Year: 2020 | Volume: 3, Issue: 3 | Journal Article | Publisher: TUP DOI: 10.26599/BDMA.2020.9020003

[10] Nimmy Krishnan;A. Salim Machine Learning Based Intrusion Detection for Virtualized Infrastructures 2018 International CET Conference on Control, Communication, and Computing (IC4) Year: 2018 | Conference Paper | Publisher: IEEE DOI: 10.1109/CETIC4.2018.8530912

[11] S. Shinly Swarna Sugi;S. Raja Ratna Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) Year: 2020 | Conference Paper | Publisher: IEEE DOI: 10.1109/ICISS49785.2020.9315900

[12] Indrajit Das;Shalini Singh;Ayantika Sarkar Serial and Parallel based Intrusion Detection System using Machine Learning 2021 Devices for Integrated Circuit (DevIC) Year: 2021 | Conference Paper | Publisher: IEEE DOI: 10.1109/DevIC50843.2021.9455936

[13] Abhinav Singhal;Akash Maan;Daksh Chaudhary;Dinesh Vishwakarma A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) Year: 2021 | Conference Paper | Publisher: IEEE DOI: 10.1109/ICAIS50930.2021.9395918

[14] Toya Acharya;Ishan Khatri;Annamalai Annamalai;Mohamed F ChouikhaEfficacy of Machine Learning-Based Classifiers for Binary and Multi-Class Network Intrusion Detection 2021 IEEE International Conference on Automatic Control & Intelligent Systems (I2CACIS) Year: 2021 | Conference Paper | Publisher: IEEE DOI: 10.1109/I2CACIS52118.2021.9495877

[15] Chung-Ming Ou Host-based Intrusion Detection Systems Inspired by Machine Learning of Agent-Based Artificial Immune Systems 2019 IEEE International Symposium on INnovations in Intelligent SysTems and Applications (INISTA) Year: 2019 | Conference Paper | Publisher: IEEE DOI: 10.1109/INISTA.2019.8778269