ISSN : 2455-9679
SJIF Impact Factor : 6.008

ijrtsm

IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

# "DEEP LEARNING TECHNIQUE AND AODV NETWORK BASED INTRUSION DETECTION"

***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

***An ad hoc network is a temporary, self-organizing network that operates without the need for established infrastructure. As a result, it finds extensive applications in military operations and disaster relief efforts. Due to its wireless connectivity and self-organizing nature, ad hoc networks are increasingly prevalent. However, they are also more vulnerable to security breaches and attacks compared to traditional systems. One notable disruptive attack in ad hoc networks is the blackhole attack, where a rogue node falsely claims to have the best route to the destination. In this research, we used computer simulations to model a black hole attack in an ad hoc networking environment. We collected data on critical features to classify aggressive behavior. Subsequently, we developed various machine learning approaches to classify data packets as benign or malicious. Our research suggests a novel method that involves feature selection, crucial data gathering, and intrusion detection in ad hoc networks using machine learning algorithms. Our findings indicate that this method can be applied with different classifiers and can be further expanded upon. Despite advancements in security systems, the continually evolving nature of attack strategies necessitates robust detection mechanisms. The most reliable approach is to assess whether a given sample is benign or malicious based on the context of the attack. The simulations and executions were conducted using MATLAB software.***

***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)**

IDAODV uses this method to pretend to break in. AODV is the most popular routing protocol for MANETs, and it has become the de facto standard on the Internet because so many people use it. This is also why AODV has been getting more and more vulnerable to attacks over the past few years. Problem Statement and Attacks Using AODV Routing AODV gives people who want to attack different options. First, we figure out what kinds of abuse goals an inside attacker could be trying to reach [8].

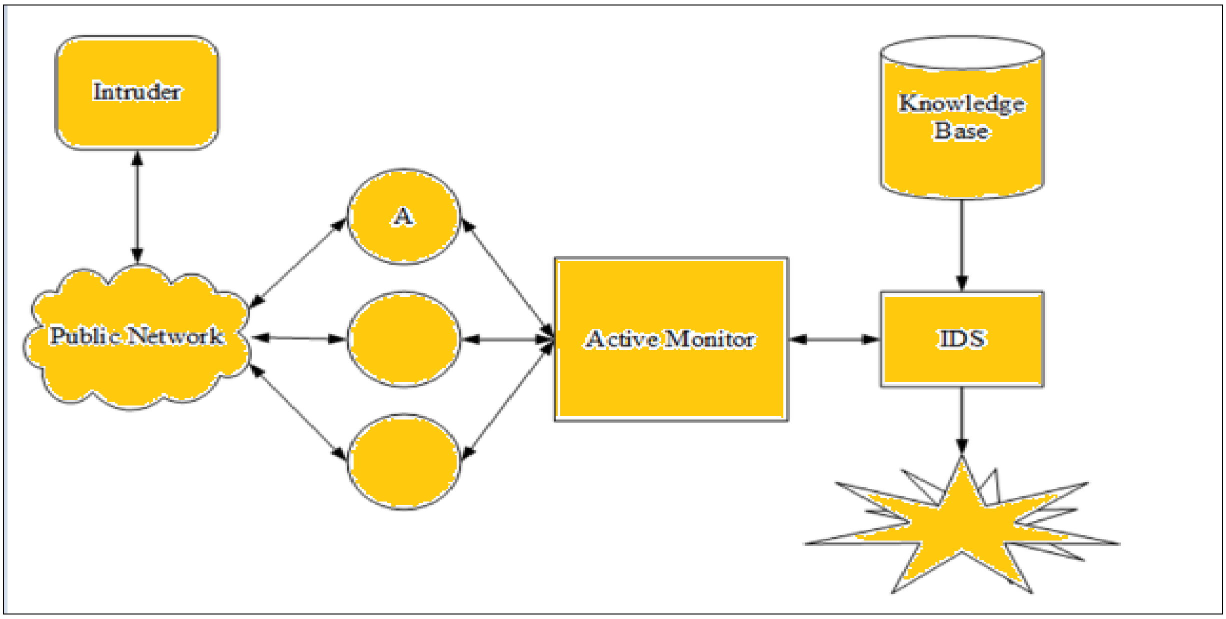


Fig. 1.1 Intrusion Detection AODV (IDAODV)

**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:

**1.3 Intrusion Detection System**

Network attacks are a group of hostile actions that try to stop, stop, slow down, or 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 [2]. 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 [12]. 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].

## III. Proposed approach

This paper suggests using simulation as a way to model common communication situations, some of which may be open to attacks by bad people. The proposed system has a distributed and cooperative architecture in which each node uses an intrusion detection system (IDS) agent to find and get rid of any nodes that aren't acting right [5]. Each IDS agent has four different parts that make it up. The first module is called the "data collection module," and its main job is to gather data and figure out the path from each node's source to its destination. The second part of the system is the module that looks for intrusions. It uses the information made available by the module that came before it as well as the threshold value to try to figure out if there is anything unusual going on in the monitoring nodes. The voting module is the third one, and it is in charge of approving what has been found. In this module, a node that says another node is acting wrongly must get permission from all the other nodes in the network before isolating the accused node. The result of the voting module is used by the fourth module, which is called the intrusion response module, to figure out how to separate the nodes that are acting wrongly.

Module for Intrusions Detection The main goal of this module is to look at the data that was collected by another module and figure out which nodes in the network are bad. The module figures out what the acceptable threshold is and then uses it to find any bad nodes in the network. In this case, the threshold value is a very important part of figuring out how the nodes fit together. After that, it's clear that the network could have at least one rogue node and maybe even more than one. The intrusion detection module shouldn't immediately label as malicious any nodes it finds that look suspicious.

Deep Learning (ML) has recently come to the forefront as an approach that is not only desirable but also possible to provide efficient solutions for a wide range of application areas. One of the most important application domains is vehicular networks, and ML-based techniques have been shown to be very helpful in solving a wide range of problems in this domain. Since it uses wireless communication between its vehicle nodes and/or its infrastructure, it can be attacked in many different ways. In this situation, ML and its variations are becoming more and more popular as a way to find attacks and solve a wide range of communication security problems in vehicles.

## IV. NETWORK MODEL

In VANET [10], network artefacts can be separated into three groups. These groups include servers for application and authorization, facilities on the road side, and nodes/vehicles.

**Application and Authorization Servers-** These are powerful workstations, responsible respectively for managing and providing service data. The authority knows all the keys and is accountable for maintenance planning. For cars, device servers provide operation details. The government or foreign operators will fund them. We assume there are powerful processing capabilities for authorization and application servers. So, here we ignored computation time.

**Road Side Infrastructure -**Road Infrastructure consists of power supplies located near roads and responsible for the collection and dissemination of data. Through wired networks, RSUs are connected to power and communicate via radio with vehicles.

**Nodes/ Vehicles -**Nodes or Vehicles are moves in the road and communication with the RSU or also their information exchange information is received by RSU in network. Every vehicle is presumed to be fitted with a differential GPS receiver with meter-order accuracy and an on-board computer (OBU) [11] responsible for all communication and computing task

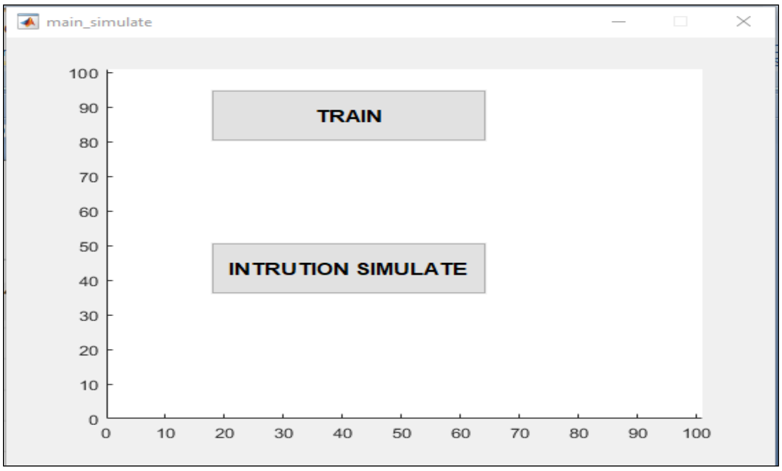
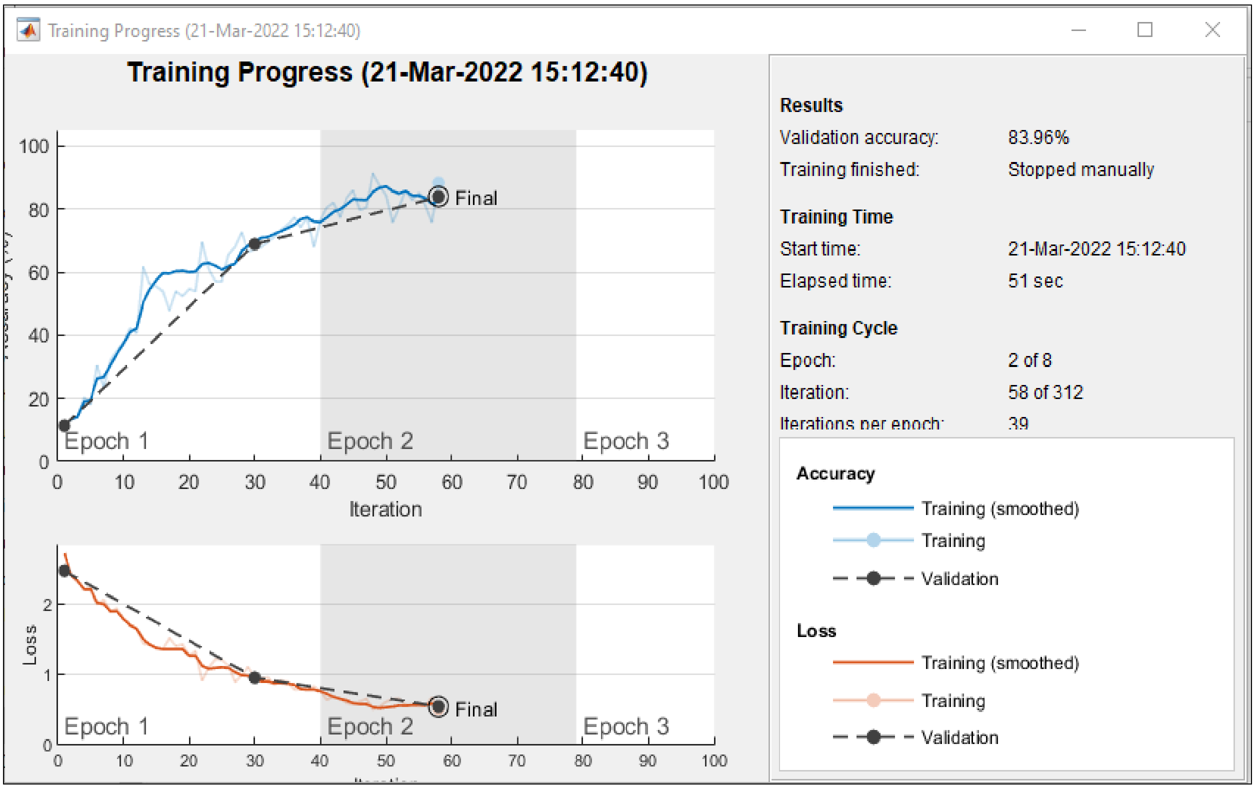


Fig.1 Training and Simulation Window

ISSN : 2455-9679
SJIF Impact Factor : 6.008



**Results**

Validation accuracy: 83.96%

Training finished: Stopped manually

**Training Time**

Start time: 21-Mar-2022 15:12:40

Elapsed time: 51 sec

**Training Cycle**

Epoch: 2 of 8

Iteration: 58 of 312

Iterations per epoch: 39

Fig.2 Training Process Window

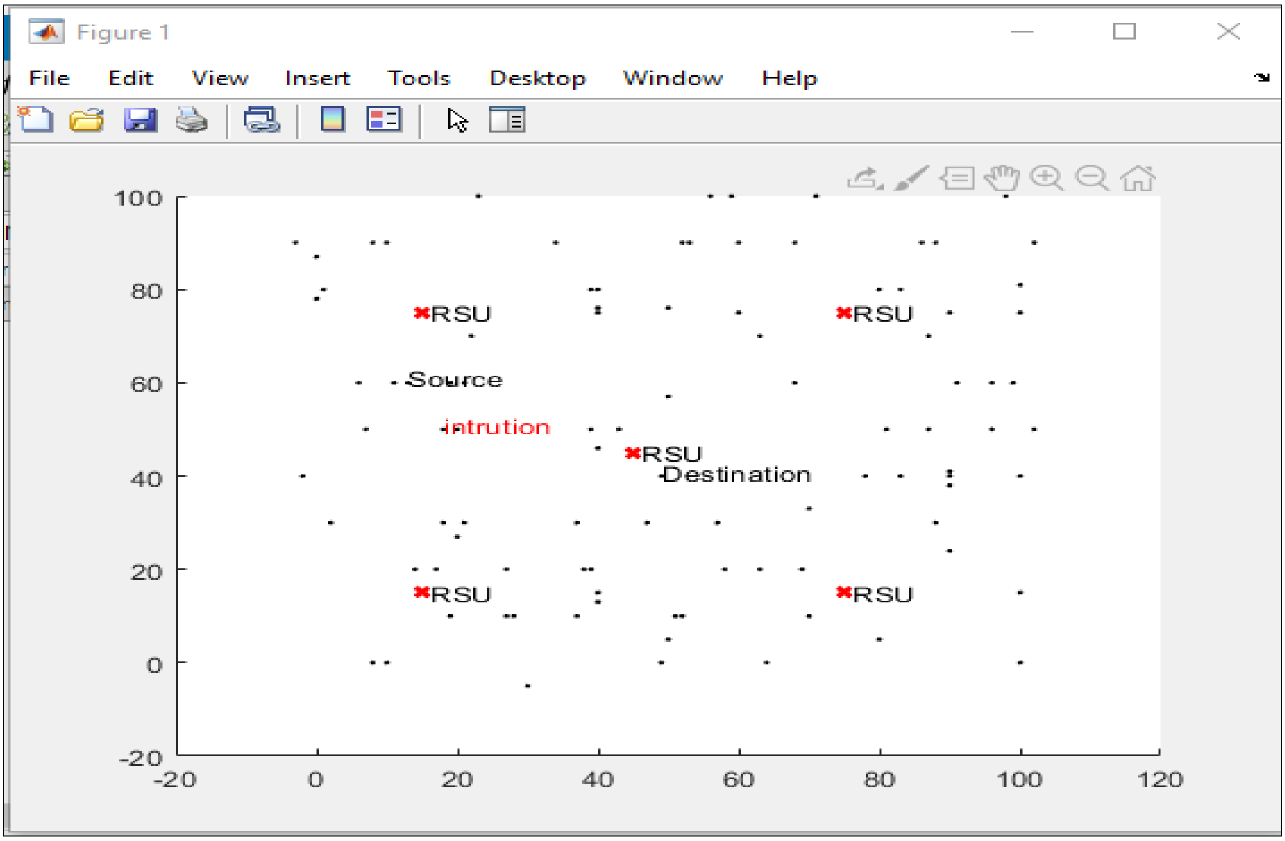


Fig.3 Network Architecture

ISSN : 2455-9679
SJIF Impact Factor : 6.008

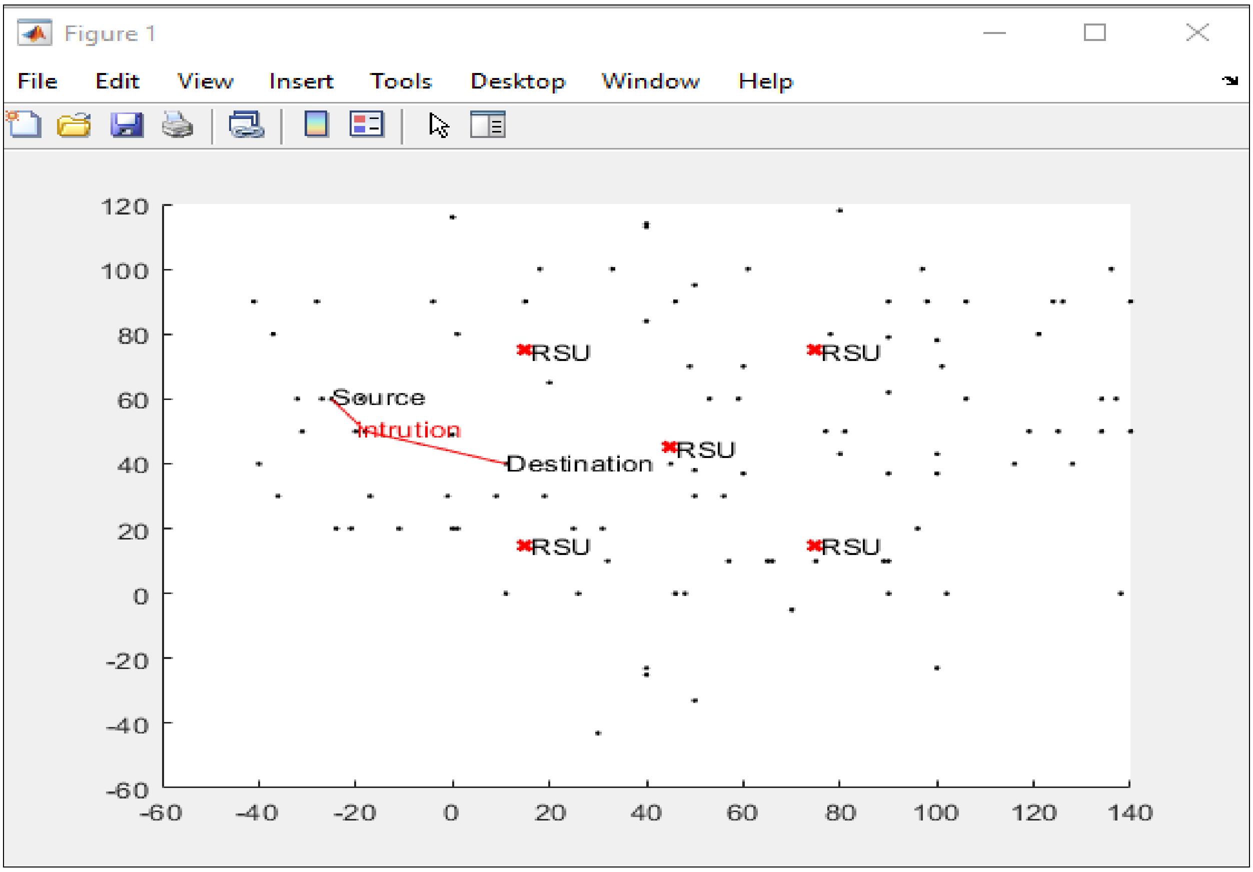


Fig.4 Network Architecture

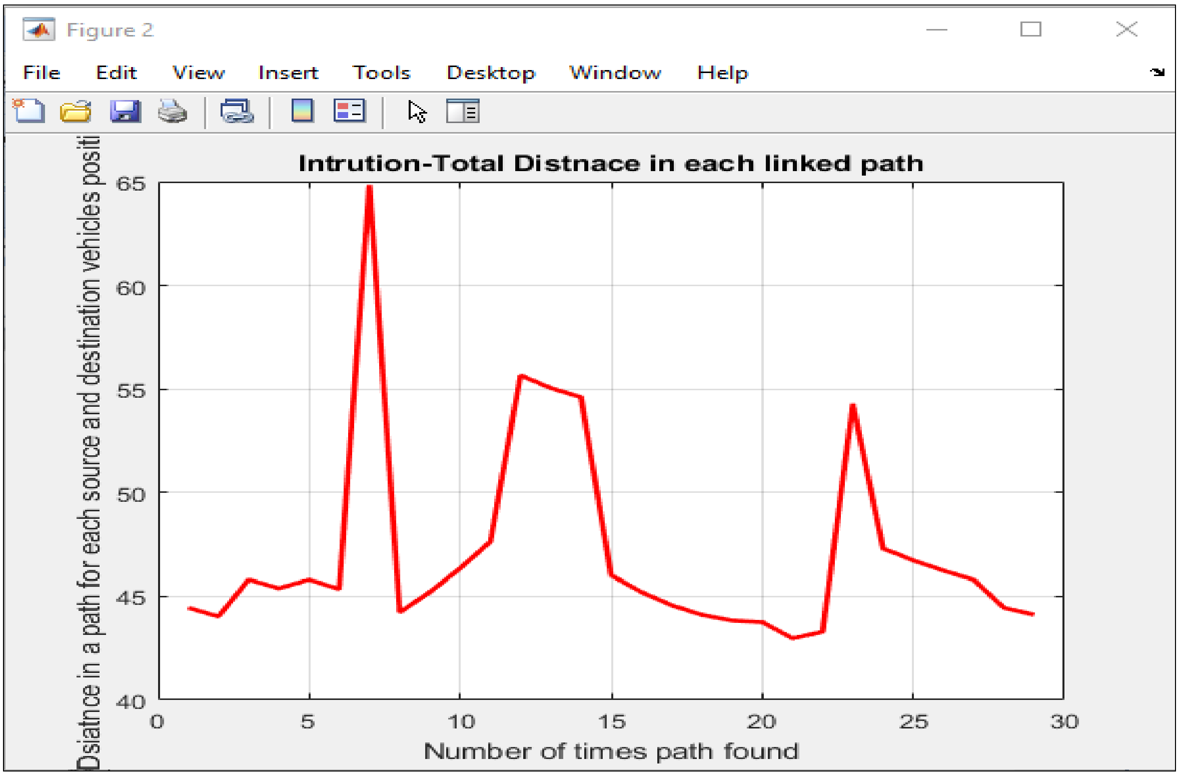


Fig.5 Total Number Of Linked Path

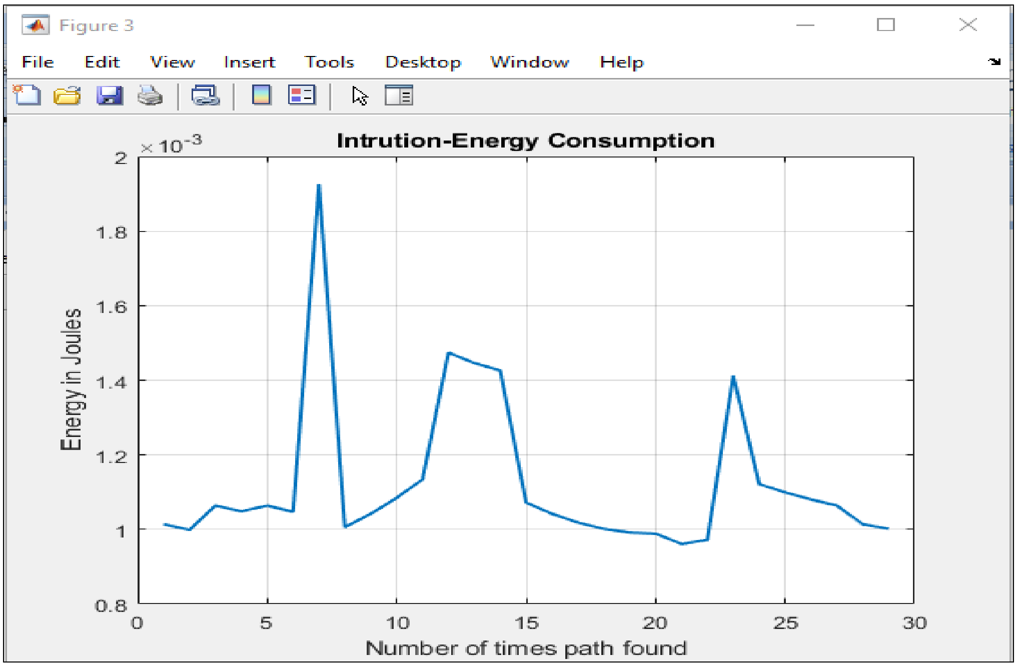


Fig.6 Intrusion Energy Consumption

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.6

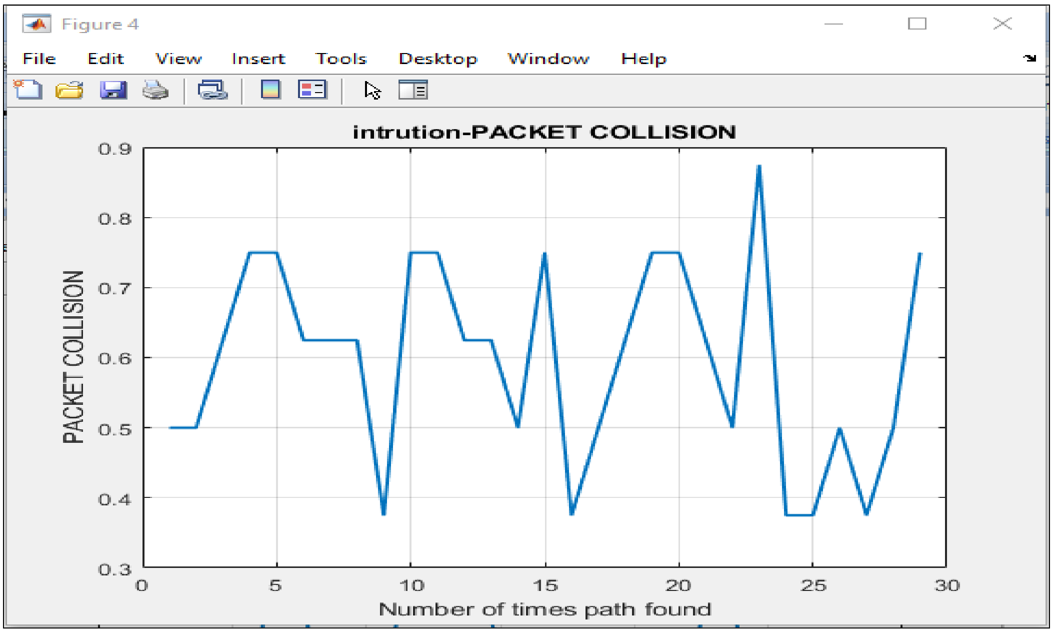


Fig.7 Packet Collision

Fig.7 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

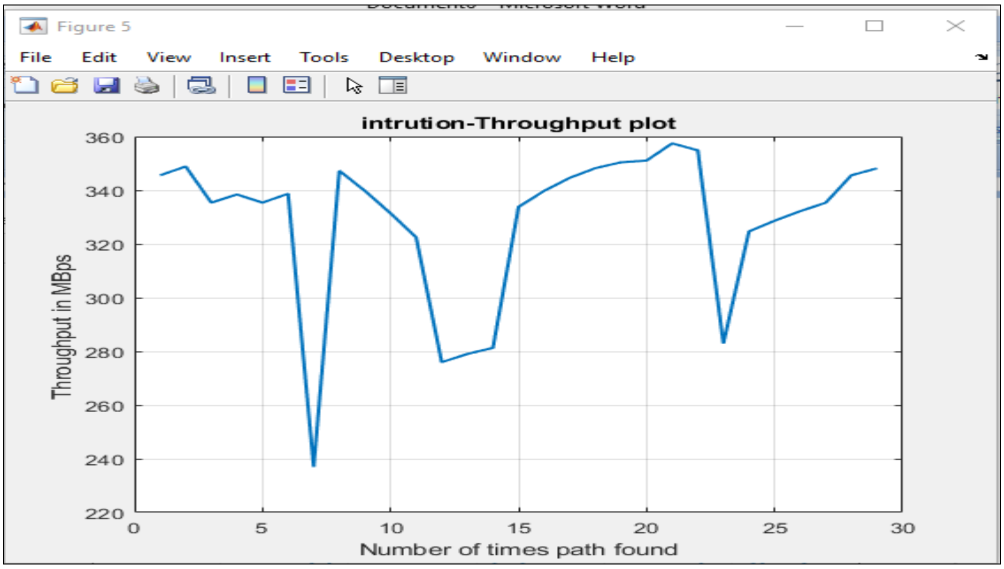


Fig.8 Intrusion Throughput

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 8

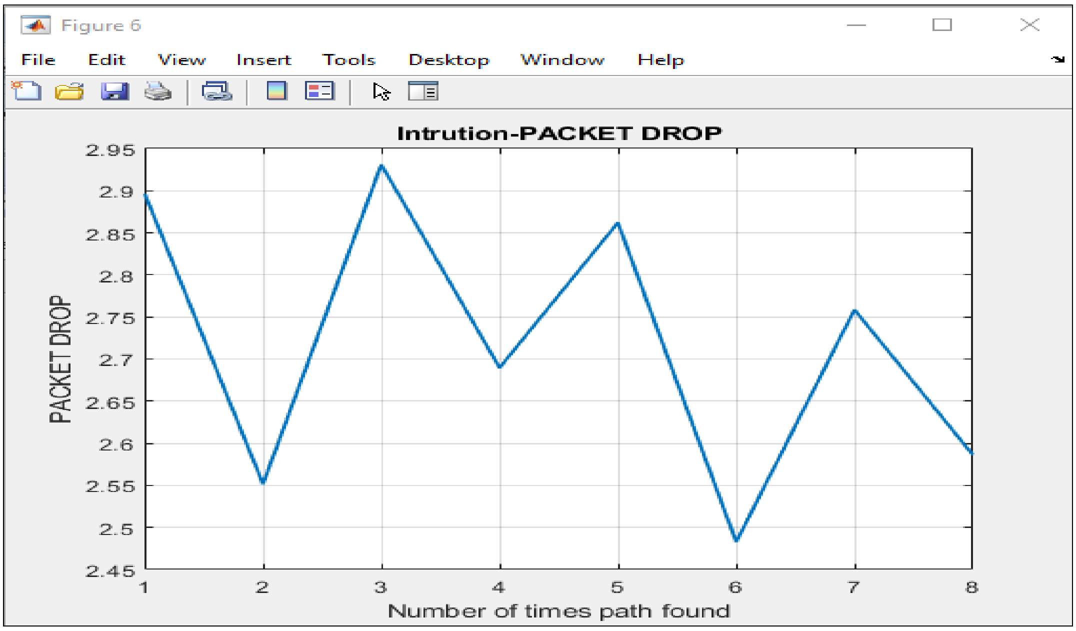
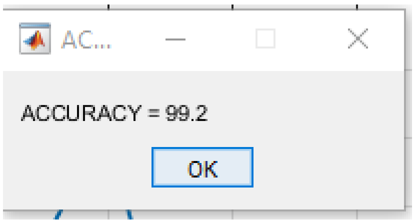


Fig.9 Intrusion Packet Drop

intrusion packet drop showing in the fig.9 Packet loss can be caused by congestions due to heavy traffic, collisions at link layer, buffer overflows,



ACCURACY = 99.2

Fig.10  Accuracy of the System

ISSN : 2455-9679
SJIF Impact Factor : 6.008

**Table 1 Comparison result with the exixsting system**

| | **Techniques** | **Accuracy (%)** |
|---|---|---|
| Proposed system | **ResNet50** | **99.2** |
| **Existing system** | **SVM** | **97.29** |

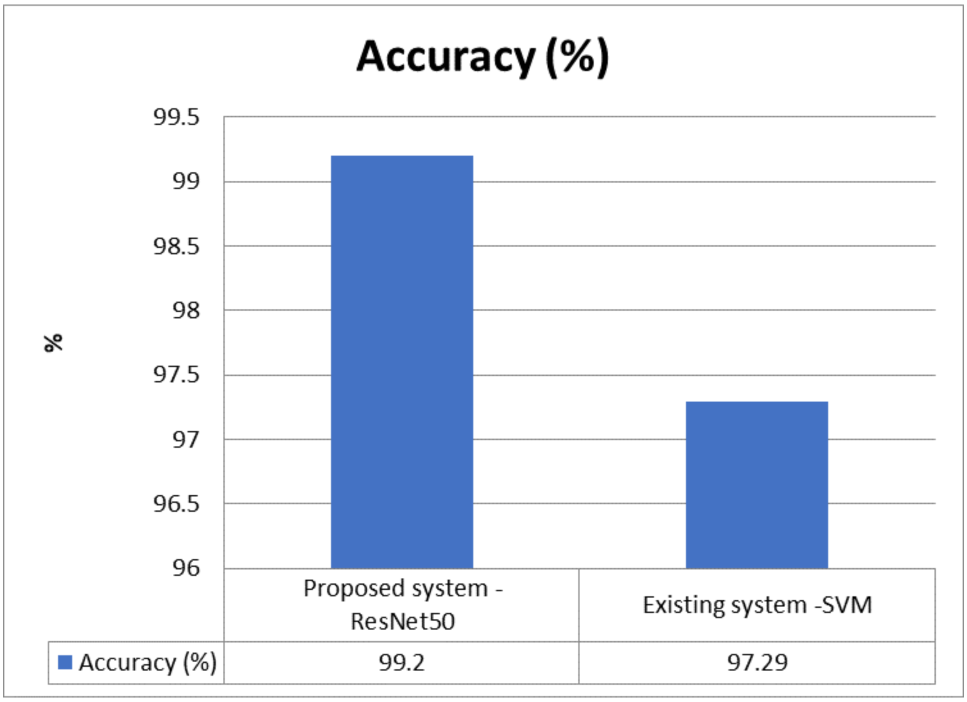


Fig. 11 comparison result with the existing system

## 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," 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