iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** VIII **Month of publication:** August 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.46247

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue VIII Aug 2022- Available at www.ijraset.com*

# A Distributed Intrusion Detection System for AODV Network

Ms. Rashmi Jaiswal[1], Ms. Chandramala Amarji[2]
[1]*M.Tech.Scholar, Swami Vivekanand College of Engineering, Indore*
[2]*Assistant Professor, Swami Vivekanand College o Engineering, Indore*

***Abstract:*** ***The Ad hoc On-Demand Distance Vector (AODV) routing protocol, designed for mobile ad hoc networks, offers quick adaptation to dynamic link conditions, low processing and memory overhead, and low network utilization. However, without keeping in mind the security issues in the protocol design, AODV is vulnerable to various kinds of attacks. This thesis analyzes some of the vulnerabilities, specifically discussing attacks against AODV that manipulate the routing messages. We propose a solution based on specification-based intrusion detection to detect attacks on AODV. Briefly, our approach involves the use of finite state machines for specifying correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. In addition, one additional field in the protocol message is proposed to enable the monitoring. We illustrate that our algorithm, which employs a tree data structure, can effectively detect most of the serious attacks in real time and with minimum overhead. Routing attacks will have distressing effects over the network and bequest a significant challenge once planning strong security mechanisms for vehicular communication. In this paper, we examine the effect and malicious activities of a number of the foremost common attacks and also mention some security schemes against some major attacks in VANET. The attacker's aim is only to modify the actual route or provides the false data about the route to the sender and also some attackers are only flooding unwanted packets to consume resources in available network. Various routing approaches are also mentioned in the paper because the routing of data is very important to deliver the traffic information to leading vehicles. It's advised that a number of the ways that to approach this made field of analysis issues in VANET might be to fastidiously design new secure routing protocols in which attacks are often rendered meaningless and because of the inherent constraints found in the network, there's a desire for light-weight and sturdy security mechanisms.***

***Keywords: 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. Among them, intrusion detection system (IDS) has been considered to be one of the most promising methods for defending complex and dynamic intrusion behaviors.

An Intrusion Detection mechanism for Wireless Mobile Ad Hoc Networks. IDAODV is based on State Transition Analysis Technique, which was initially developed to model host-based and network-based intrusions in a wired network environment. Of all the routing protocols proposed for MANETs, AODV has been very popular and has become an Internet standard.

This also has been the reason for AODV becoming more and more vulnerable to attacks. Problem Statement/ AODV Routing Attacks AODV present many opportunities to attackers. We first identify a number of misuse goals that an inside attacker may want to achieve [3].

1) *Route Disruption:* Route Disruption means either breaking down an existing route or preventing a new route from being established.
2) *Route Invasion:* Route invasion means that an inside attacker adds itself into a route between two endpoints of a communication channel.
3) *Node Isolation:* Node isolation refers to preventing a given node from communicating with any other node in the network. It differs from Route Disruption in that Route Disruption is targeting at a route with two given endpoints, while node isolation is aiming at all possible routes.
4) *Resource Consumption:* Resource consumption refers to consuming the communication bandwidth in the network or storage space at individual nodes. For example, an inside attacker may consume the network bandwidth by either forming a loop in the network.
5) *Denial of Service:* To achieve goals, the following misuse actions or attacks may be performed

### A. *Overview of Intrusion Detection System*

Network attacks are defined as a set of malicious activities to disrupt, deny, degrade or destroy information and service resident in computer networks [4].A network attack is executed through the data stream on networks and aims to compromise the integrity, confidentiality or availability of computer network systems. Examples of computer attacks include viruses attached to emails, probing of a system to collect information, Internet worms, unauthorized usage of a system, and denial of-service by abusing a feature of a system, or exploiting a bug in software to modify system data. Many attack recognition systems have been developed and are in use widely which inspect network data for any variation from the ordinary action of a system or user of the system [5]. Hackers have developed several mechanisms ranging from simple to sophisticated techniques to perpetuating their criminal acts.

In addition, the majority of attack, leverage on the loopholes found in some of the hardware and software components of the interconnected network systems [6]. Some might also look for an already recognized behavior of an attack within the data. These systems are termed as Intrusion Detection Systems (IDS) and use different techniques varying from statistical methods to machine learning algorithms. IDS are an important tool for network system to detect security holes in the network. Before further investigation, we will define important and usually used terms related with IDS from authors in [7]

Network Intrusion refers to any unauthorized activity on a digital network. Network intrusions often involve stealing valuable network resources and almost always jeopardize the security of networks and their data.

Intruder: it can be any person, system or program that tries to or is successful to break into the network and perform illegal actions. The intruders may be an entity from outside or may be an inside user of the system trying to access unauthorized information.

Intrusion Detection: is the process of identifying and (possibly) responding to malicious activities targeted at computing and network resources by the observation of the information available about the state of the system and monitoring the user activities. Detection of break-ins or attempts by intruders to gain unauthorized access of the system is intrusion detection.

Anomaly intrusion detection (AID): is to determine if an activity is unusual enough to suspect an intrusion. A basic assumption of anomaly detection is that attacks differ from normal behavior. A normal behavior is the one used in the network which has valid access. Machine learning is used to adapt the environment however the one that tries to access outside from the normal or allowed is considered as malicious without changing the environment.

Intrusion detection system (IDS) is a kind of security management system for computers systems and networks. An Intrusion Detection System gathers the information from certain areas within a network or computers and analyzes it to find potential security breaches.

### B. *IDS Approaches for Mobile Ad-hoc Net-works*

One of the first proposed approaches for an integrated IDS architecture is in [8]. They present a cooperative distributed intrusion detection and response framework for MANET. Anomaly detection is the primary ID approach discussed, including anomalies in routing updates, abnormalities at the MAC layer (number of channel requests, etc.) and at the mobile application layer ( number of requests to a service, duration of service requests etc.). [9] present systems to detect, avoid, and recover from malicious attacks.

They introduce three key ideas – a distributed firewall mechanism to limit the impact of flooding, an algorithm to detect and recover from intruder induced path failures, and a wireless router extension architecture which allows these techniques to be incorporated into existing wireless IP routers. Kachirski and Guha describe a wireless IDS for ad hoc networks based on mobile agent technology.

The system uses agents at various levels and aggregates their results at some cluster points that are elected using distributed algorithms. The idea is to distribute the IDS functionality between the nodes to minimize the total IDS-related processing time by each node.

[10] propose a statistics based approach. The idea is to estimate the congestion at intermediate nodes and decide if the intermediate node is not forwarding packets at the desired rate because of congestion or because of malicious behavior. The work described in [11] use the mechanism of assigning a value to the "reputation" of a node and using this information to weed out misbehaving nodes and use only trusted and verifiably good nodes. Primarily, the intrusive activity addressed is that of misbehaving nodes that agree to forward packets to neighbors, but fail to do so. Passive eavesdropping is employed in monitoring the nodes in the first three approaches.

This monitoring choice suits the nature of the domain where nodes can eavesdrop over other nodes within radio range and use that to isolate malicious nodes. In both [12] the authors implement their IDS approach on top of the DSR protocol. Belding-Royer [13] employs an IDS approach that is based on a stateful analysis of the data of AODV control packet streams in order to detect intrusions.

This approach is based on the State Transition Analysis Technique (STAT) developed initially to model host and network based intrusions in a wired environment. In the current implementation, a sensor is deployed individually in each of a subset of nodes, and the sensors do not communicate with each other.

### *C. Authentication Approaches*

In [14], a new cryptographic protocol, ARAN, is proposed. They assume that every node has its own public and private keys distributed by a trusted sever. The originator sends out a RREQ with its signature, and each intermediate node will verify the signatures of the previous intermediate node and the sender, and sign the packet sent by the originator. (The signature of previous intermediate node is discarded) .propose S-AODV, which shares the same approach. Both of them use signatures to protect the AODV header from being modified and keep the header readable.

### *D. Statement of the Problem*

Intrusion Detection is one way of network monitoring mechanism to prevent the resources before further damage occurs.IDS are design mostly on signature-based for known attacks, also there are depend on anomaly-based IDS for new threats. Detecting attacks masked by evasion techniques is a challenge for both Signature IDS and Anomaly IDS.These techniques are malicious activities to avoid the detection of IDS. The ability of evasion techniques would be determined by the ability of IDS to bring back the original signature of the attacks or create new signatures to cover the modification of the attacks. Robustness of IDS to various evasion techniques still needs further investigation. According to improvements in machine learning algorithms are the main means to enhance the detection effect using different feature selection methods are intended to reduce the number of input variables to those that are believed to be most useful to a model in order to predict the target variable.

### *E. Objectives*

The main objective of the study will be to design and implement a model for classification based on the Anomaly Network Intrusion Detection for network attacks.

Specific Objectives

The specific objectives of the study will be:

- Conduct a detail literature review to understand for deep learning in anomaly intrusion detection.
- To design VANET architecture for intrusion detection
- To study different types of intrusion detection approaches.
- To conduct experiments to test and evaluate the performance of the model

## 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 study proposes the use of simulation for modelling typical communication scenarios which may be subject to malicious attacks the proposed system is based on the distributive and cooperative architecture where an IDS agent is used by every node to detect and isolate the misbehaving node. Each IDS agent includes four modules. The first one is the data collection module responsible for collection of data and calculation of source to destination of each node. The second module is the intrusion detection module. It uses the information made available by the previous module and the threshold value in detecting the bad behavior of monitoring nodes. The voting module is the third module, which is responsible for detection approval, in which a node condemning another as misbehaving is required to get approval from the other nodes of the network before proceeding to isolation. The fourth module is the intrusion response module responsible for segregating the misbehaving nodes based on the outcome of the voting module

Intrusion Detection Module The main function of this module is to take the information from a data collection module and detect the malicious nodes in the network. The module identifies the malicious nodes by calculating an appropriate threshold. Here the threshold value plays a key role in scrutinizing the nodes. Then it realizes that there may be one or more malicious node in the network. Once it detects the suspicious nodes the intrusion detection module should not condemn the detected node immediately as malicious. Deep Learning (ML) has emerged as an attractive and viable technique to provide effective solutions for a wide range of application domains. An important application domain is vehicular networks wherein ML-based approaches are found to be very useful to address various problems.

The use of wireless communication between vehicular nodes and/or infrastructure makes it vulnerable to different types of attacks. In this regard, ML and its variants are gaining popularity to detect attacks and deal with different kinds of security issues in vehicular communication.

## 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.

1) *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.
2) *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.
3) *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

4) *Initial Parameters*

- Num of Nodes=100;
- Source node =10;
- Destination node=20;
- data rate=8 % packets/sec
- city size=100
- Range=20
- breadth = 0
- define attack node
- intrution_node=14
- amount of Energy consumption per bit in the transmitter or receiver circuitry = Elec=50e-9; %
- Amount of energy consumption for multipath fading =Emp=0.0015e-12;%
- Data aggregation energy =EDA=5e-9; %.
- parameters for energy calculation using ratio model of message transmission

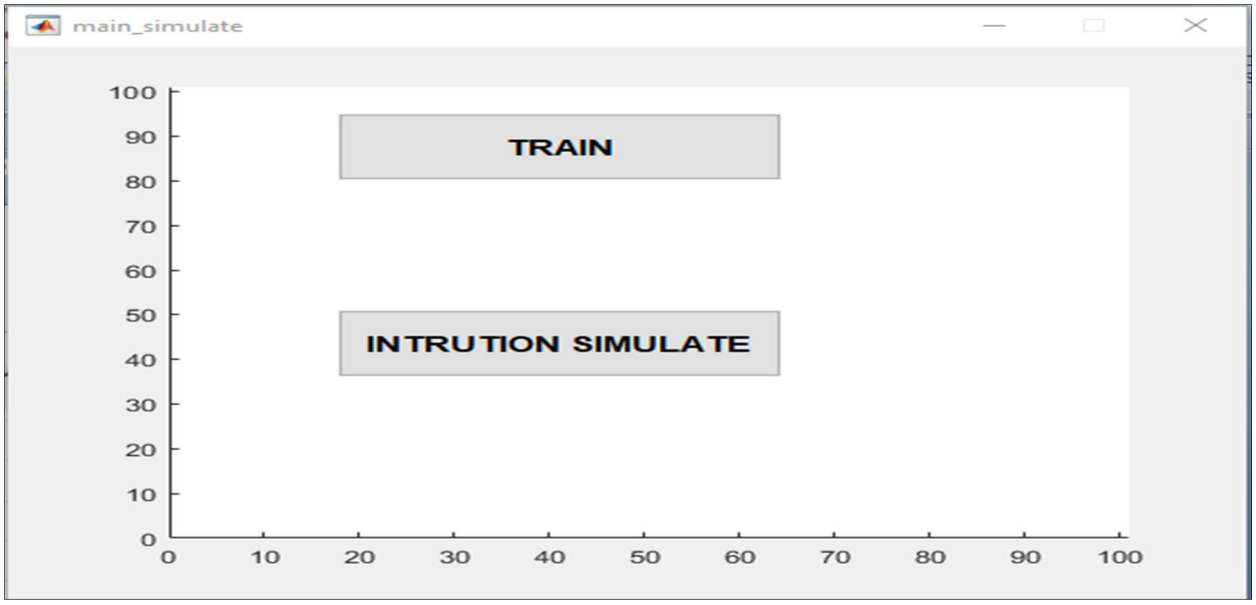



Fig.1 Training and Simulation Window

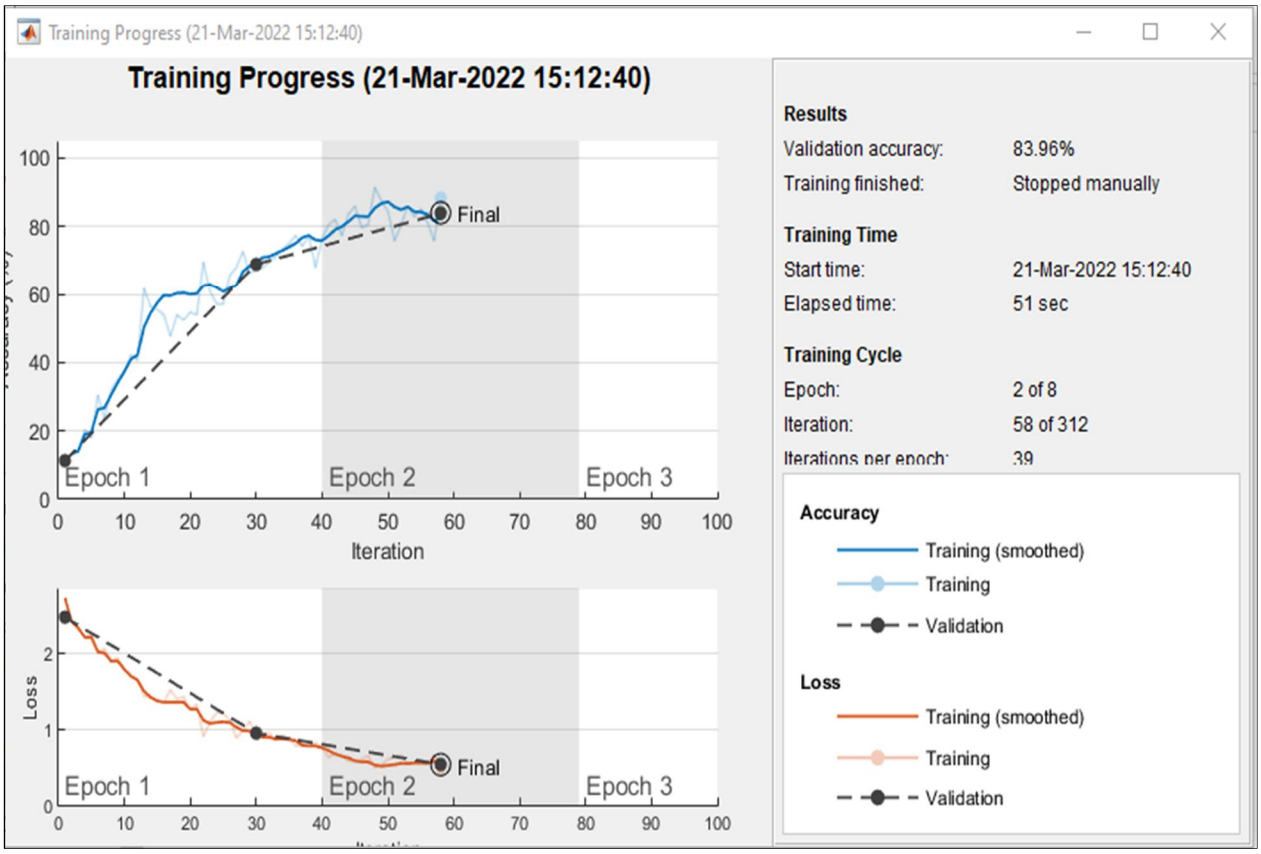



Fig.2 Training Process Window

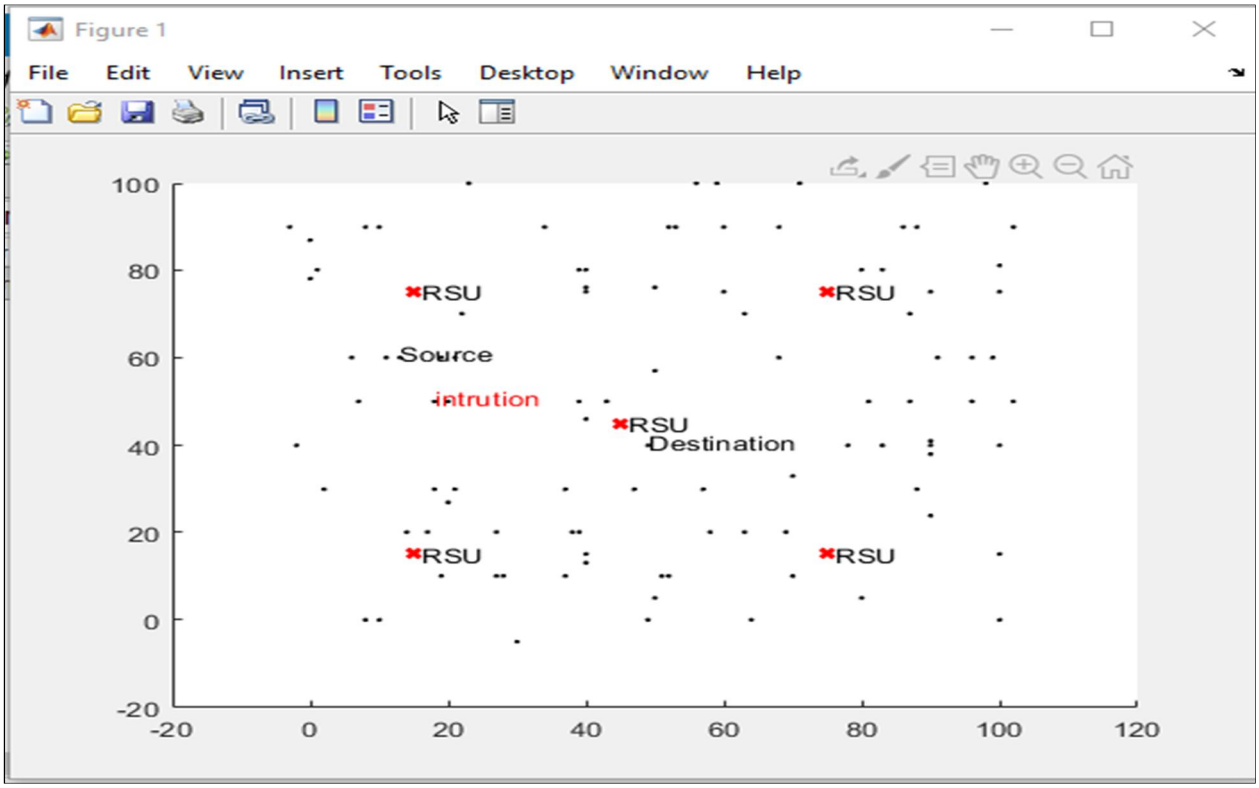



Fig.3 Network Architecture

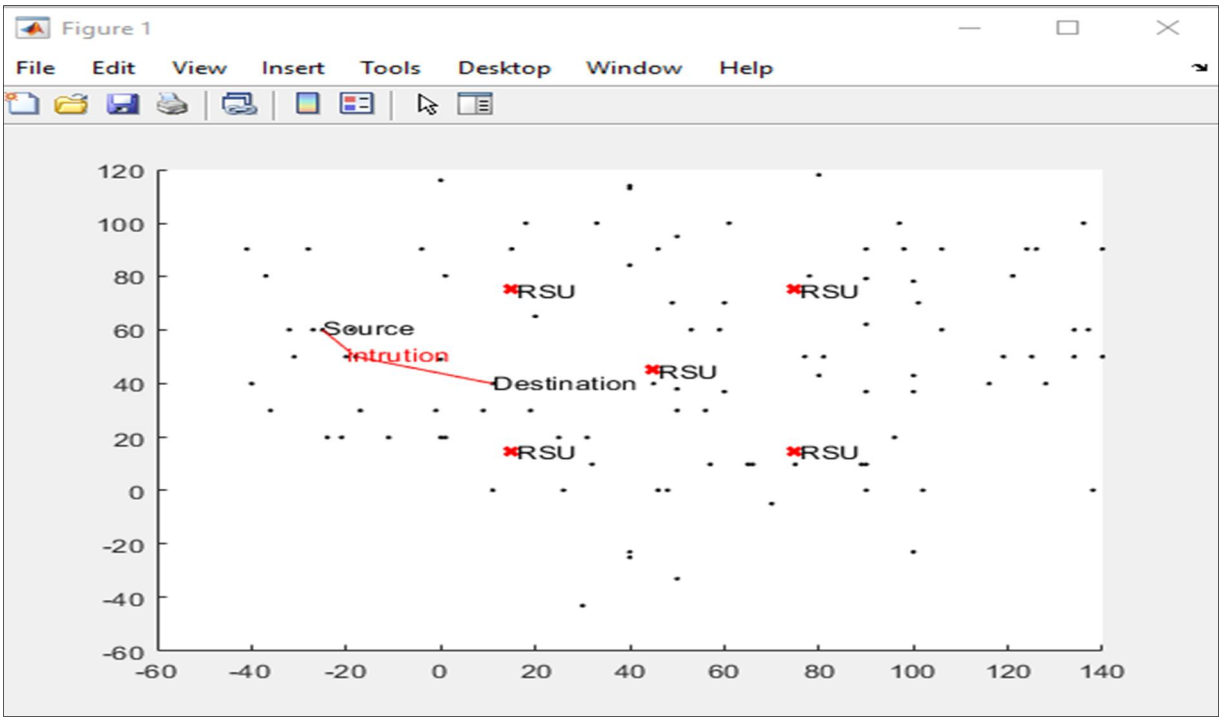



Fig.4 Network Architecture

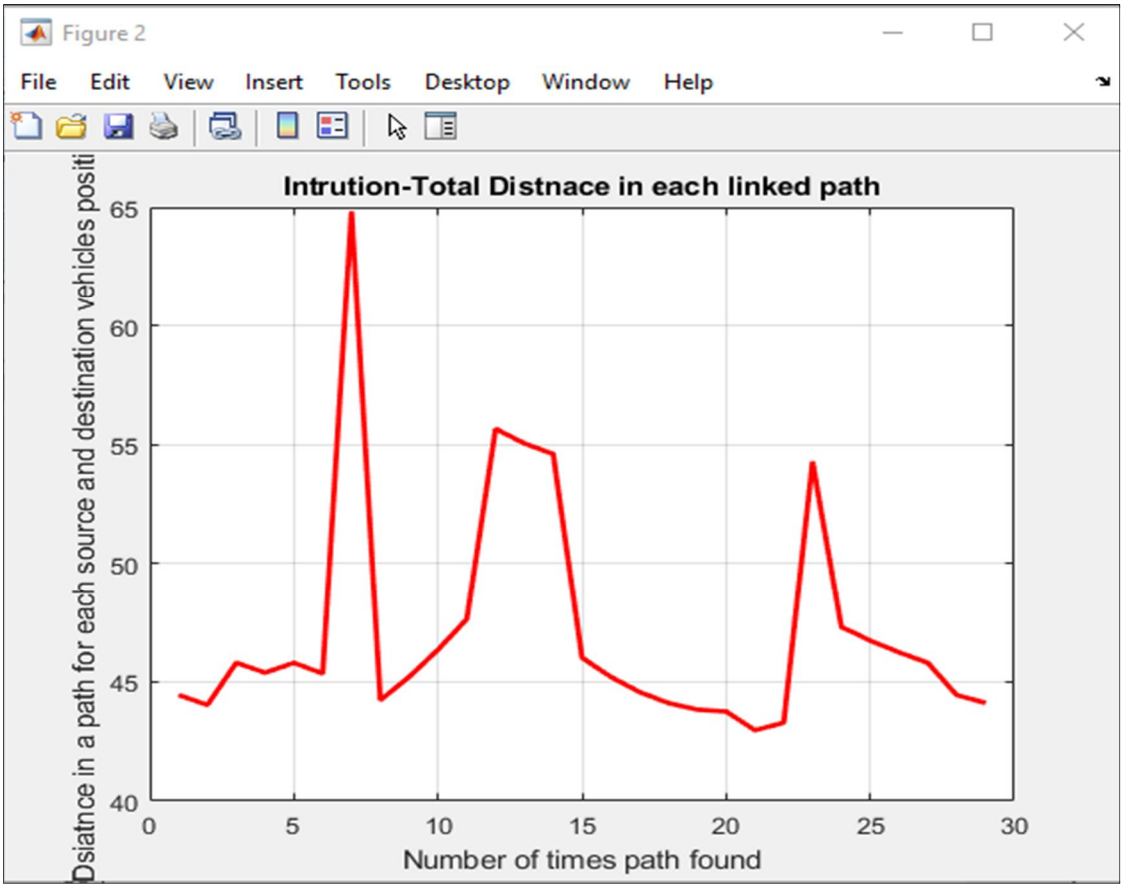



Fig.5 Total Number Of Linked Path

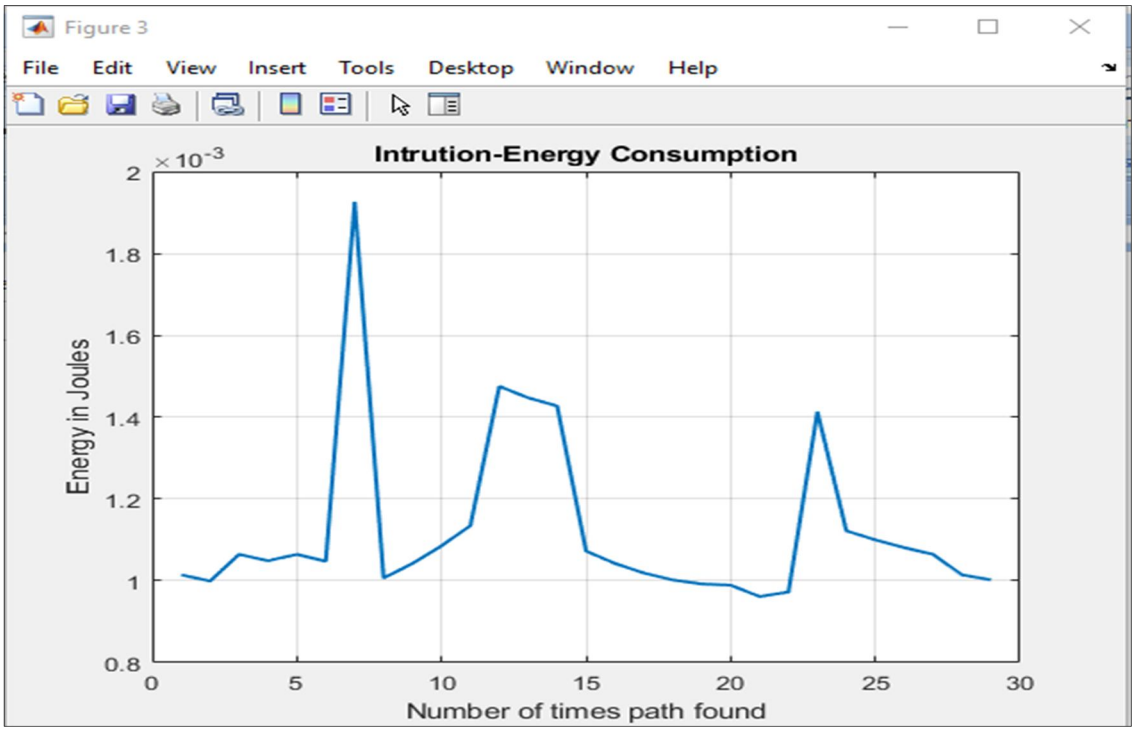



Fig.6 Intrusion Energy Consumption

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

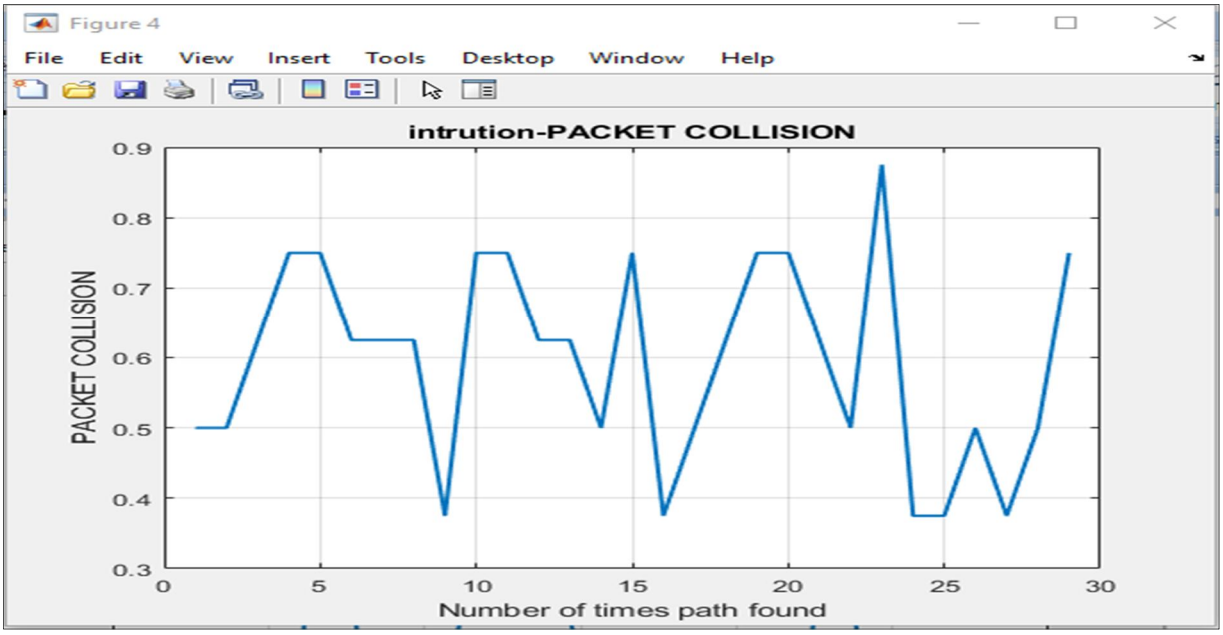



Fig.7 Packet Collision

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

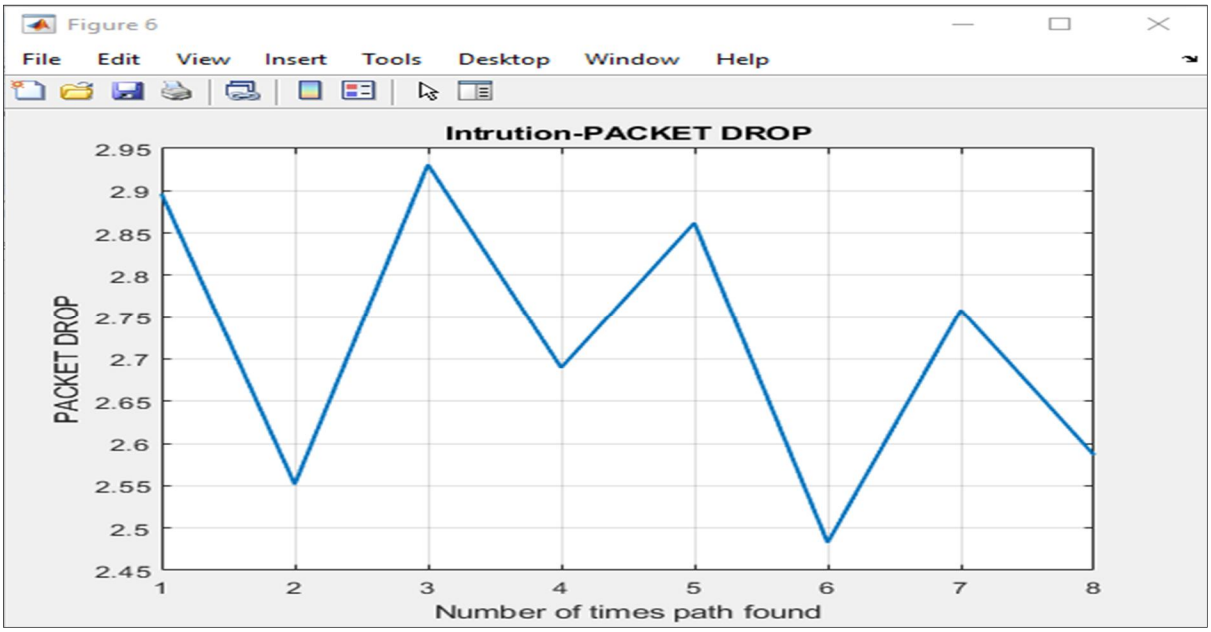



Fig.9 Intrusion Packet Drop

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,

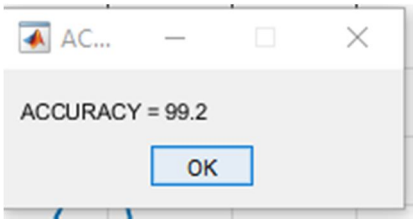



Fig.10 Accuracy of the System

Table 1 Comparison result with the exixsting system

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

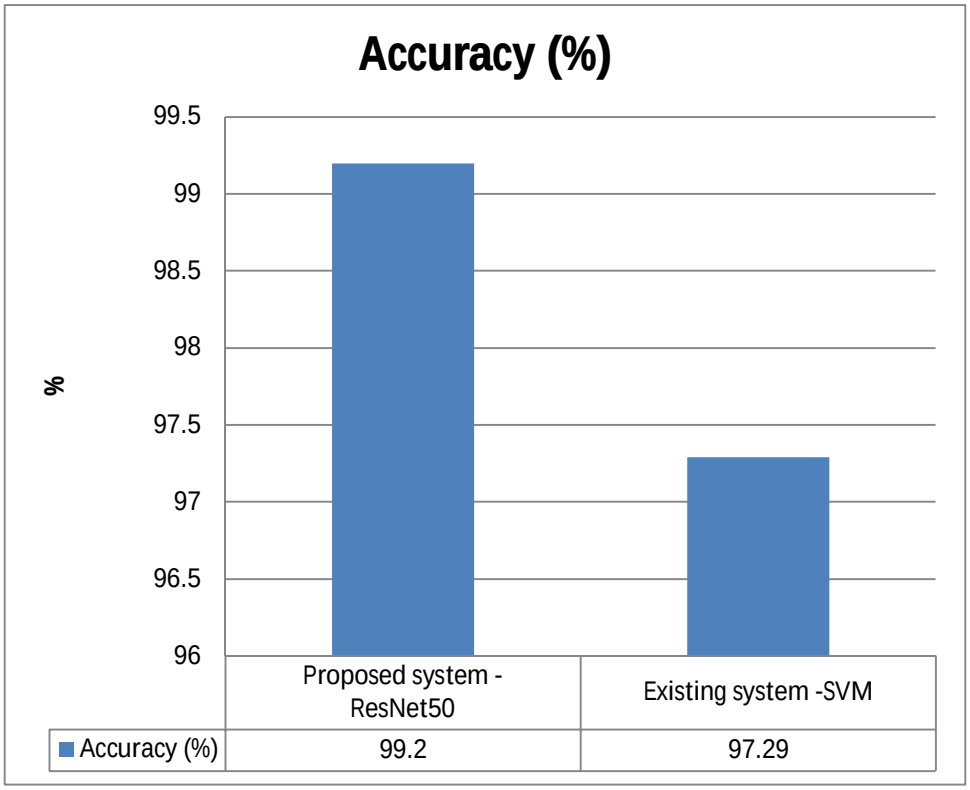


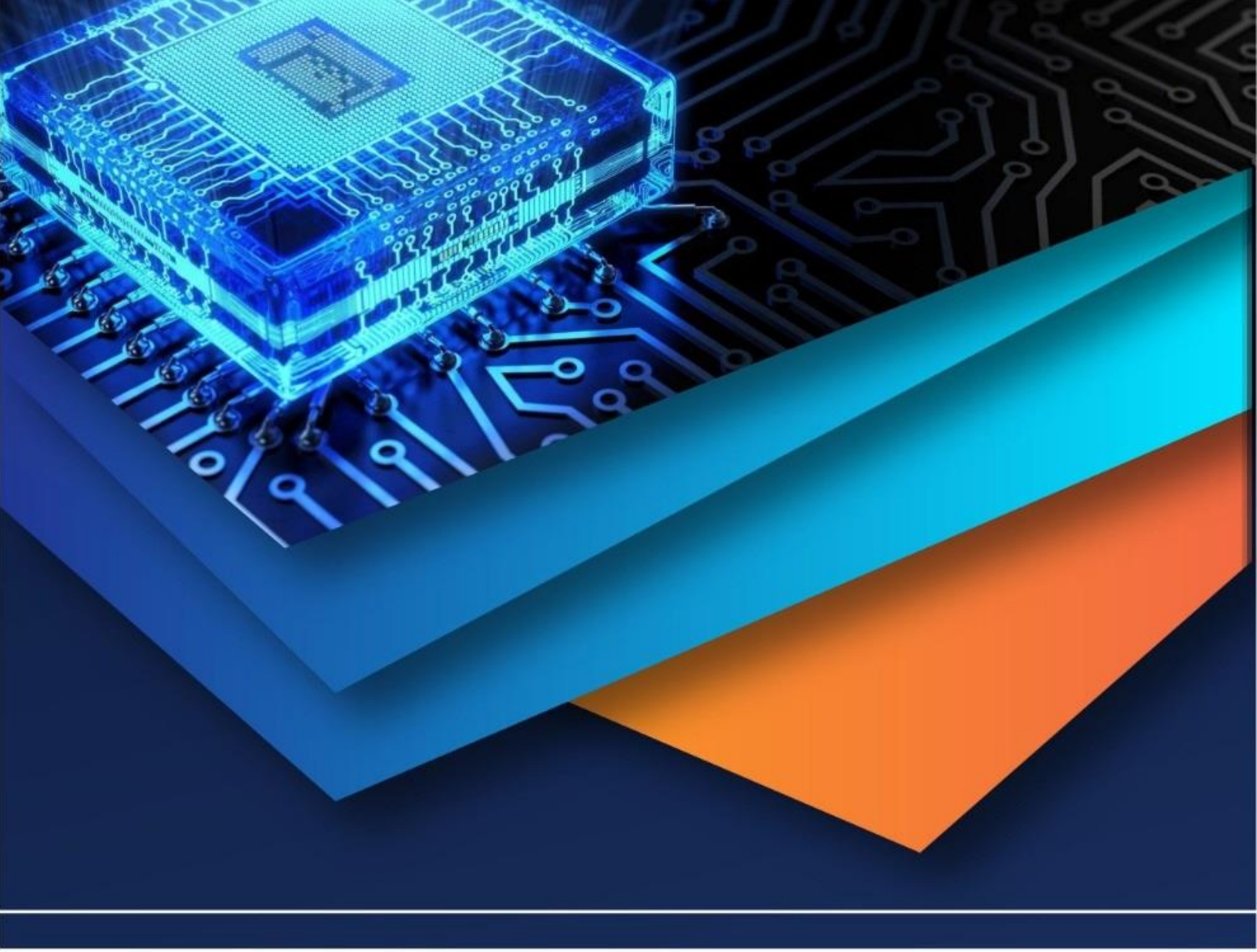

Fig. 11 comparison result with the existing system

## 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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY