A MACHINE LEARNING-BASED INTRUSION DETECTION FOR DETECTING INTERNET OF THINGS NETWORK ATTACKS

Sunil Sharma
Research Scholar (CS)
JRN University, Udaipur

Dr. Bharat Singh Deora
Sr. Assistant Professor ,(CS)
JRN University, Udaipur

Dilip Choudhary
Assistant Professor
JRN University, Udaipur

ABSTRACT

The Internet of Things (IoT) refers to the collection of all those devices that could connect to the Internet to collect and share data. The introduction of varied devices continues to grow tremendously, posing new privacy and security risks—the proliferation of Internet connections and the advent of new technologies such as the IoT. Various and sophisticated intrusions are driving the IoT paradigm into computer networks. Companies are increasing their investment in research to improve the detection of these attacks. By comparing the highest rates of accuracy, institutions are picking intelligent procedures for testing and verification. The adoption of IoT in the different sectors, including health, has also continued to increase in recent times. Where the IoT applications became well known for technology researchers and developers. Unfortunately, the striking challenge of IoT is the privacy and security issues resulting from the energy limitations and scalability of IoT devices. An ad hoc network is a transient network that is self-organizing and does not require any infrastructure. Therefore, the majority of its applications are in the field of military work and disaster assistance. Because of wireless connectivity and the ability to organize itself, ad hoc networks are becoming more common. Susceptible to a greater number of breaches or assaults than the conventional system. Blackhole assault is a significant routing disruption attack that a rogue node promotes itself as being capable of. as a step along the way to the final destination. In this research, we simulated a black hole using computer models. Assault in a setting with ad hoc networking, as well as data collection of important features for the purpose of classifying aggressive behaviour. Then, several different approaches to machine learning have been developed. utilized for the classification of information regarding benign and harmful packets. It seems to imply. a novel method for the selection of certain features, the gathering of crucial information, and the intrusion detection in an ad hoc network with the application of machine learning algorithms.

DOINUMBER:10.48047/NQ.2022.20.19.NQ99433 NEUROQUANTOLOGY2022;20(19):4709-4722

INTRODUCTION

The Internet of Things (IoT) is a joint network of interconnected devices; these devices can decide without any human interventions. The advancement of various technology fields, like automatic identification, sensors, tracking, wireless communications, embedded computing, distributed services, and 5G networks, has increased the possibility of utilizing advanced objects in our daily activities via the Internet [1]. The IoT is defined by the intersection of the Internet and intelligent objects capable of communication and interaction. This new paradigm has been identified as a key player in the ICT business in the coming years [2]. In the IoT, a thing can be anything on the planet: a person with a blood pressure monitor implant, a car equipped with sensors that alert the driver

when the tire pressure is low, a farm animal with a transponder, or any object that can be given an IP address and the ability to transfer data over a network [3]. According to Cisco, it is stated that by 2020, about 50 billion devices will be connected to the Internet [4]. Cisco Systems forecasted that the Internet of Things would generate $ 14.4 trillion in income and cost savings for businesses between 2013 and 2022 [5], [6], [7], [8]. These connected devices – dubbed the IoT holds a lot of promise for improving social and corporate life as well as market development, increased accessibility necessitates the use of stronger security precautions [9]. The main reason for the network's poor performance is that it consumes a lot of energy due to its low battery capacity. As a result, reducing energy consumption is a critical requirement for achieving quality of service (QoS) in the IoT context. IoT devices could be healthcare devices, wearables, industrial robots, smart televisions, smart city infrastructures that can be monitored remotely. There are many interesting applications of IoT. Even if the IoT seems to be a more industrial phrase, about 87 percent of individuals still do not comprehend what it means [10]. Information security is one of the most important parts of the current information process. This is because of the widespread use of computers and the risk of losing information that is stored, processed, and sent across the network. When the Internet came out in the 1990s, it started a new era that would have a big effect on information technology. This was because it made it much easier to use data transfer and communication channels [1]. The first millions of people to use the Internet were able to talk to each other through e-mail because of a network of computers that stayed in one place. Heavy reliance on the Internet and global connections has made it much easier for attacks to come from far away and do a lot of damage through the Internet. Anyone, anywhere in the world, can carry out these attacks. And when you use the internet, there is a chance that your information will be stolen or that you will lose data that you have saved. Intruders plan their attacks so that they can take advantage of any security holes that are already in the system or network [2]. An intrusion is a deliberate act of breaking the law that is done to get information, change information, or make a system untrustworthy or not work.

One of the most important things to think about when using the Internet in our daily lives is how safe our computers and networks are. Network attacks were still one of the most common types of threats in 2019, according to the data Kaspersky reported [3]. Kaspersky's security solutions were able to stop 975,491,360 threats that came from internet resources in 195 different countries. So, there should be ways to protect against this risk. An intrusion detection system, or IDS, is an active process or device that watches the activities of a system or network to look for unapproved and unauthenticated behaviour [4]. Most of the time, this is done by automatically collecting information from a wide range of system and network sources and analyzing it to look for security holes in the system. There is no way to know for sure that any data on a network that is connected to the internet will always be safe. Instead, according to the IEEE x.805 eight security dimensions map to security threats, it is recommended to use a number of different methods to reduce any risk.

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].

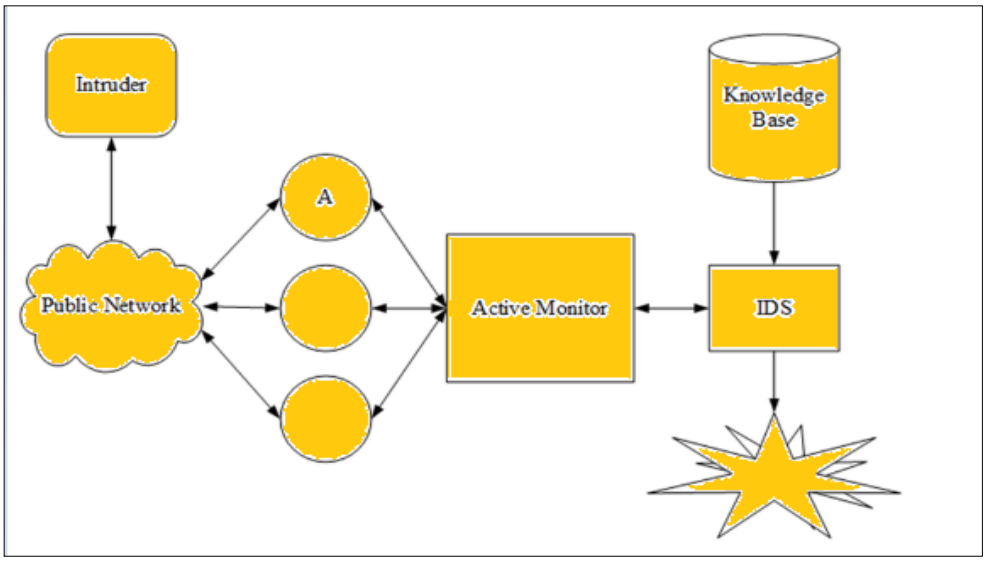

Figure 1 : Intrusion Detection AODV (IDAODV)

NETWORK –BASED IDS

(NIDS) is to keep an eye on data about network traffic by using sensors that are connected to the network to record any actions that seem strange. Threats to the security of a network can show up in many different ways and can affect more than one part of network security, such as authentication, integrity, authorization, and availability. Most network-based IDSs are OS-agnostic, which means they work on any system that supports the target OS [4]. IDSs that are based on a network can also find some types of protocol and network attacks. One of the benefits of NIDS is that its monitors don't use any of the host computer's resources when they read each packet as it moves over a network segment. Also, they don't need a specific operating system to work and are easy to set up on a small part of the network. On the other hand, there are some bad things about NIDS. They have trouble keeping up with systems, especially busy ones, because they have to check every packet that goes through the segment. In the next section, we'll talk more about how anomaly detection works with network-based intrusion detection, which is the main topic of this research. An Intrusion Detection System (IDS) can keep an eye on the traffic on a network and send out alerts if it sees anything suspicious.

OVERVIEW OF MANETS

MANET (Mobile AdHoc Network) is a self-configuring non-infrastructure network of mobile devices connected via a wireless environment. Adhoc is a Latin word that means "for this purpose." Each node in MANET is dynamic and therefore frequently changes its connections with other devices. The Ad Hoc Routing Protocol is a standard that defines how nodes route packets between a source and destination on an ad hoc mobile network. In an adhoc cellular network, the nodes are not static and do not have a specific topology, but must discover it.

AdHoc Mobile networks are standalone and decentralized wireless systems. MANETs consist of mobile nodes that move freely in the network and outside it. Nodes are systems or devices, such as a mobile phone, laptop, personal digital assistant, and personal computer that participate in the network. These nodes can act as host / router or both. They can create any topologies depending on their interconnection in the network. These nodes are self-adjusting and, thanks to their self-configuration capability, can be deployed as a matter of urgency without the need for any infrastructure.

ADHOC Networks

Nodes can freely join and leave ad hoc networks because there is no infrastructure to support them. A wireless link, like the one shown in figure 3.1, is what makes it possible for the nodes to talk to each other. A node can act as a router and send data to the nodes in the network that are close to it.

Figure 2 : Simple Adhoc Network.

This kind of network is sometimes called "infrastructure-less" networks because there is no one place where decisions about how the network works are made. Ad hoc networks are set up to be able to handle any problems with the nodes or any changes that might happen if the network's topology changes. When a network node stops working or leaves the network, the other network nodes that are affected by this simply ask for new routes, and an ad hoc network sets up new links between them. It can be split into mobile ad hoc networks and static ad hoc networks, which are also called SANET (MANET).

Static Adhoc Networks-In static Adhoc networks the geographic location of the nodes or the stations are fixed. There is no mobility in the nodes of the networks.

ADHOC Network Routing Protocol

The study of routing protocols is one of the most difficult and interesting fields of study. For MANETs, a lot of routing protocols have been made, like AODV (Adhoc on Demand Distance Vector). There are a lot of different kinds of routing protocols that can be used in Ad hoc networks. These protocols can be put into four main groups.

Type1: Information Update Mechanism

Type 2: Use of temporal information for routing

Type 3: Routing topology

Type 4: Utilization of specific resources

Routing information Update mechanism

Adhoc network routing protocols can be classified into three categories.

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. 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 attempts to determine whether there is anything strange going on in the check nodes by using the information provided by the module that came before it as well as the threshold value. 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.

Deep Learning (ML) has recently come to the forefront as an approach that is not only desirable but also possible to make available practical efficiency across a variety of contexts. 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 WSN between its vehicle nodes and/otherwise its communications, 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.

Network Model

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

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

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

Initial Parameters

- Number of Nodes =100
- Number of Source node = 10
- Number of Destination node = 20
- data rate = 8 packets/sec
- city size=100
- intrusion node=14

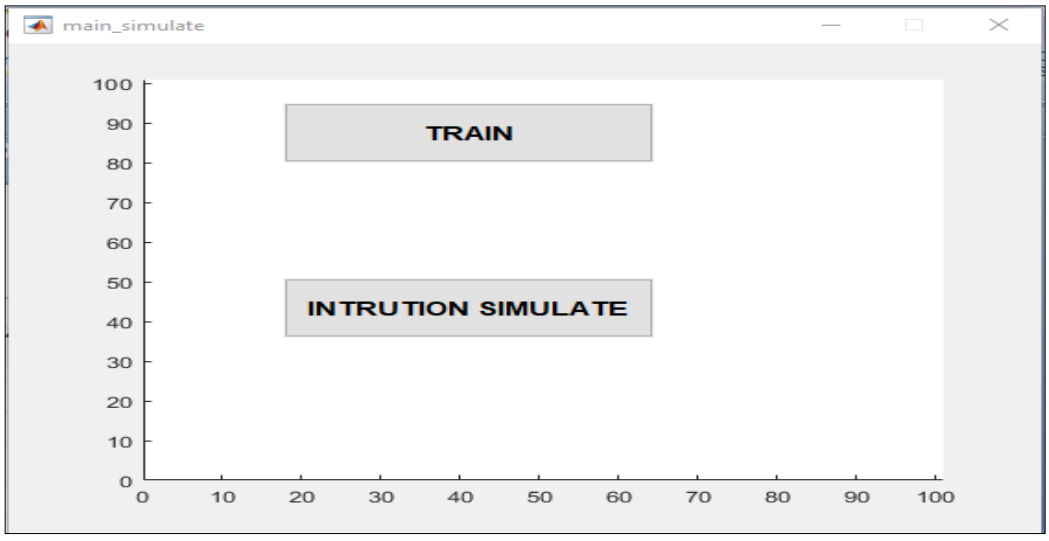

Figure 3 : Training and Simulation Window

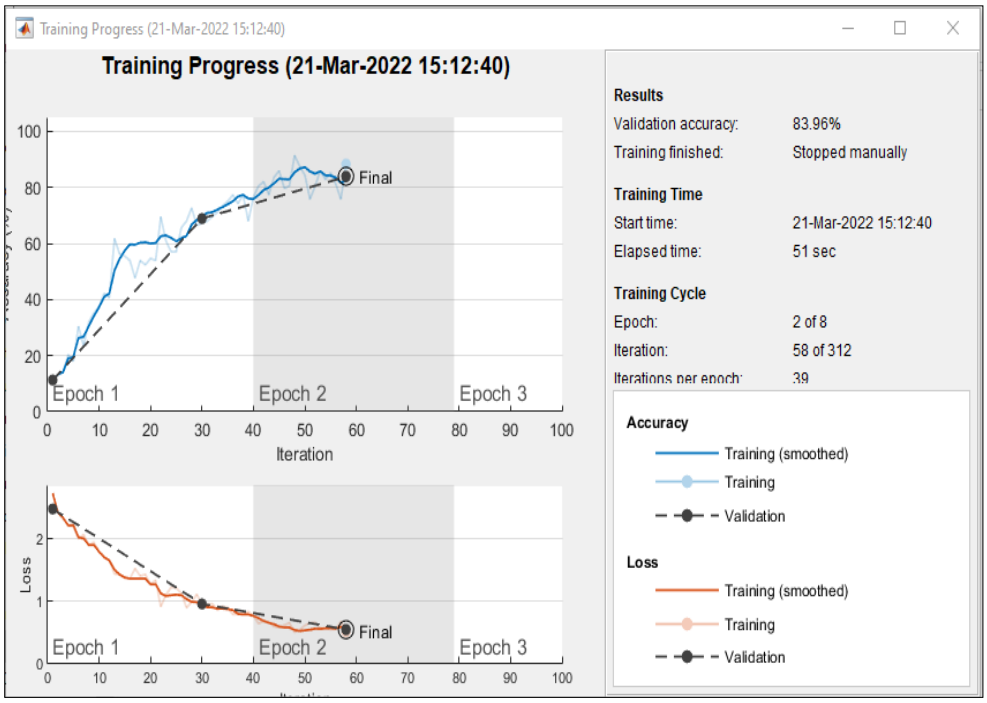

Figure 4 : Training Process Window

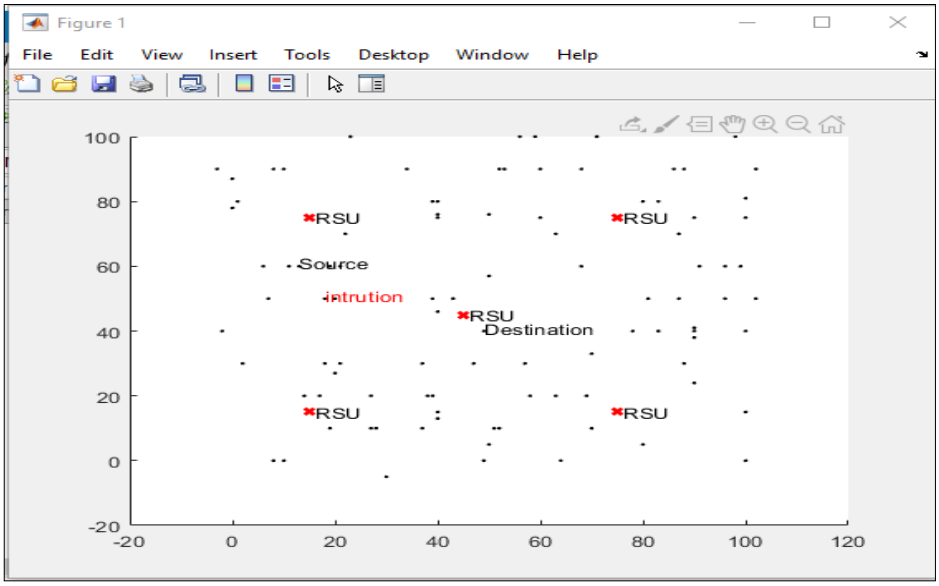

Figure 5 : Network Architecture

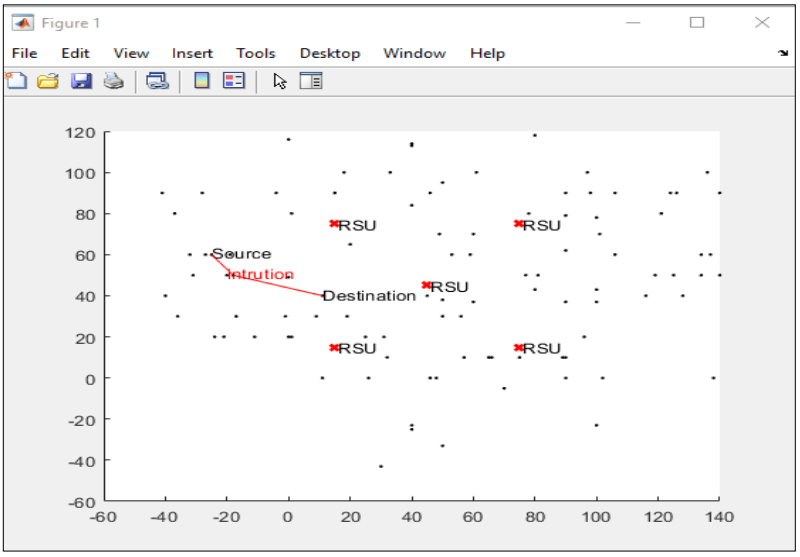

Figure 6 : Network Architecture

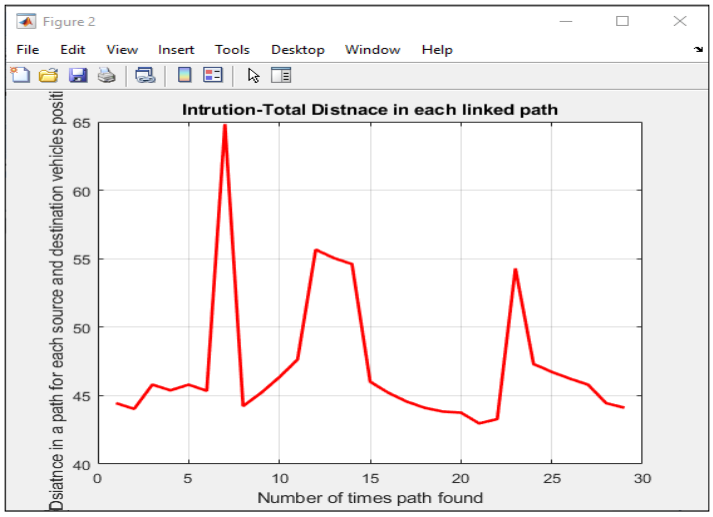

Figure 7 : Total Number of Linked Path

Table 1 : Comparison result with the existing system

	Approaches	Accuracy performance (%)
Implementation work	Deep learning ResNet50	0.99
Previous Work	Machine learning -LSTM	0.97
	Machine learning -KNN	0.92

Results Discussion

We send the packets through the SOM once they've been collected, vectored, and trained. Figure 8 depicts the end product. the categorization of input vectors, which represents user behaviour, and its mapping to specific neurons, which comprise single potential user behaviour states. Intrusion is indicated by the form, but is it really an intrusion, or is it only a possibility. Based on the results of the tests, the SOM network seems to be an appropriate core for IDS systems.

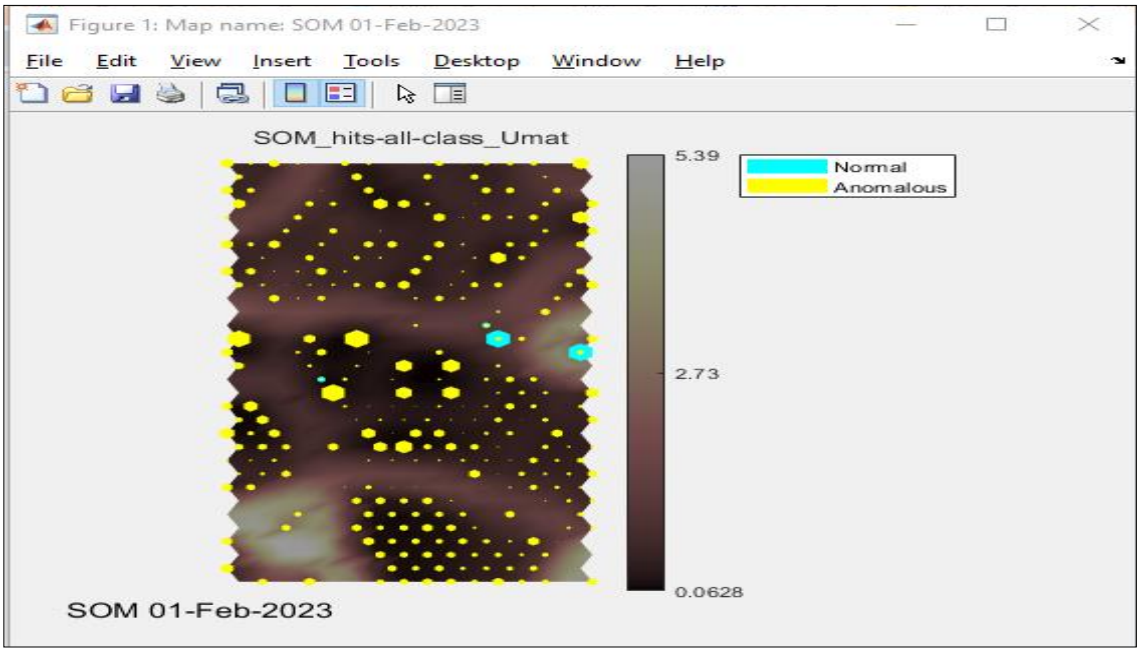

Figure 8: Normal and abnormal activity in the network

As part of our research, we sent an attack flow into the network that had been trained. As a result, the attacks spread to two classes and to both normal and weird activities.

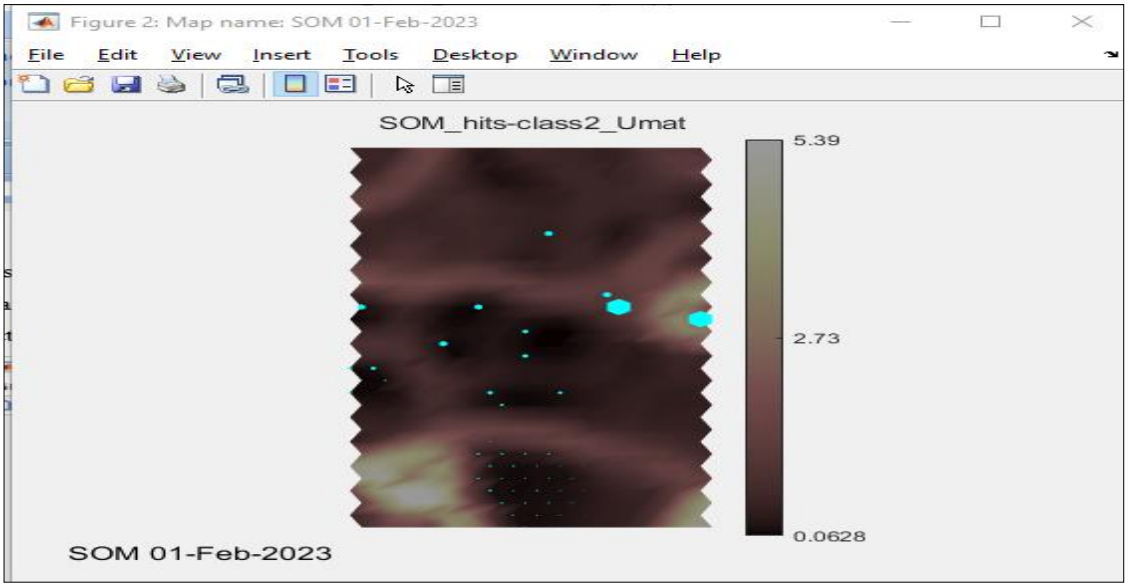

Figure 9: Normal activity in the network

During this experiment, we will use attack flow to train the network. We will not use the regular flow. For this reason, we thought it would be easier to tell attack patterns from normal flow if we trained

with attack flow. This suggests that we are not looking for unusual things, but rather looking for signs of abuse or signatures.

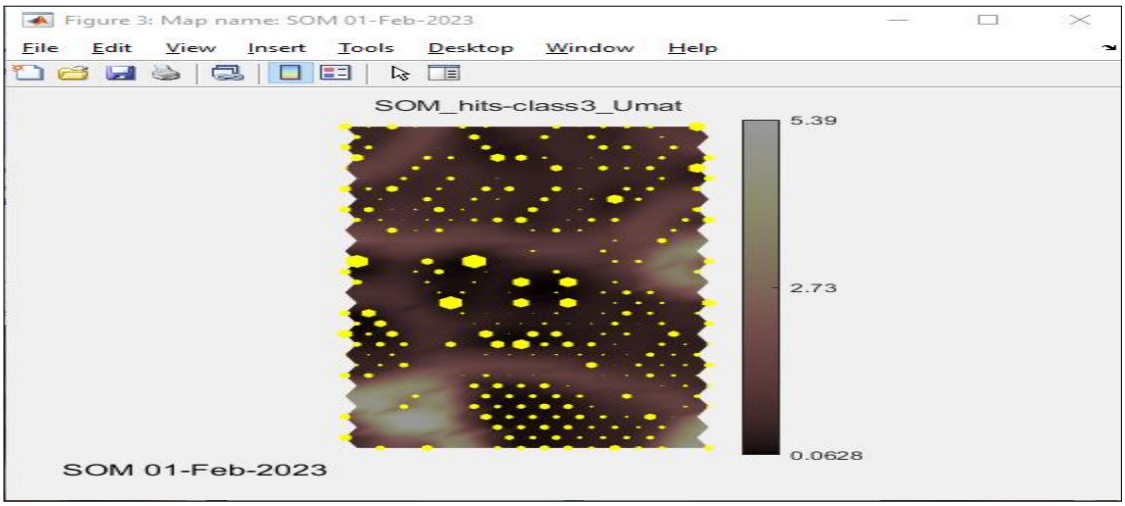

Figure 10: self organization map distribution network with normal activity

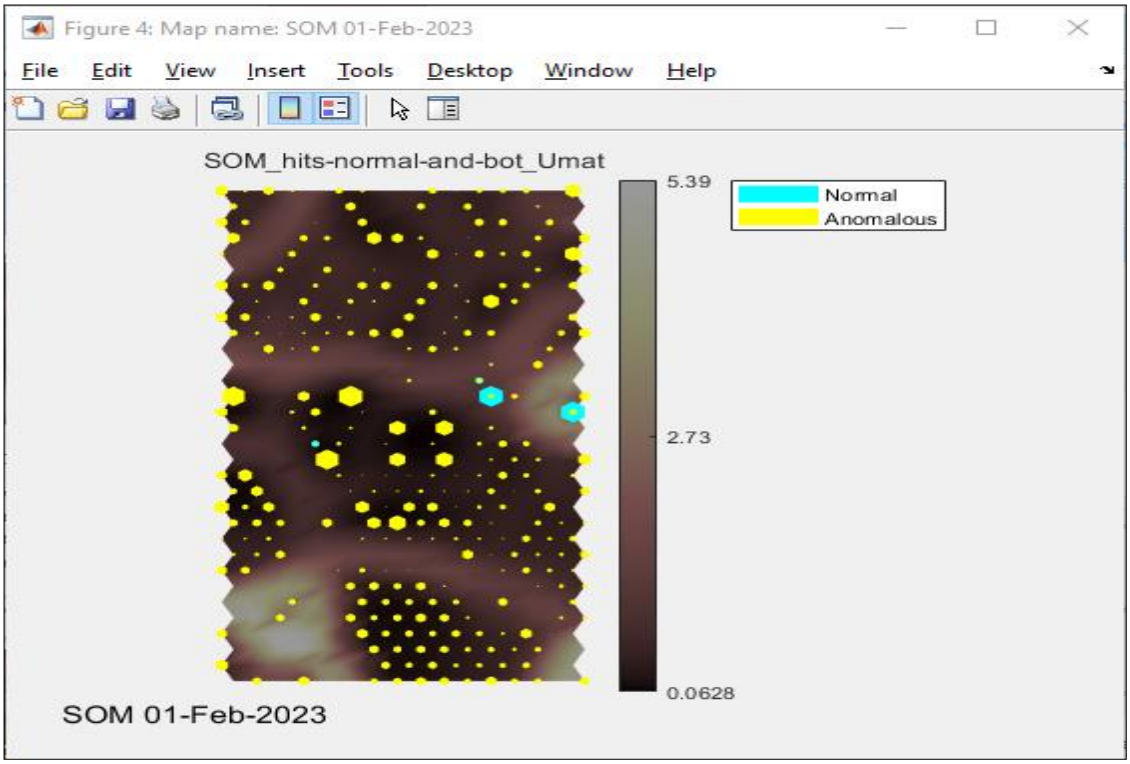

Figure 11: self organization map distribution network with normal activity and abnormal activity

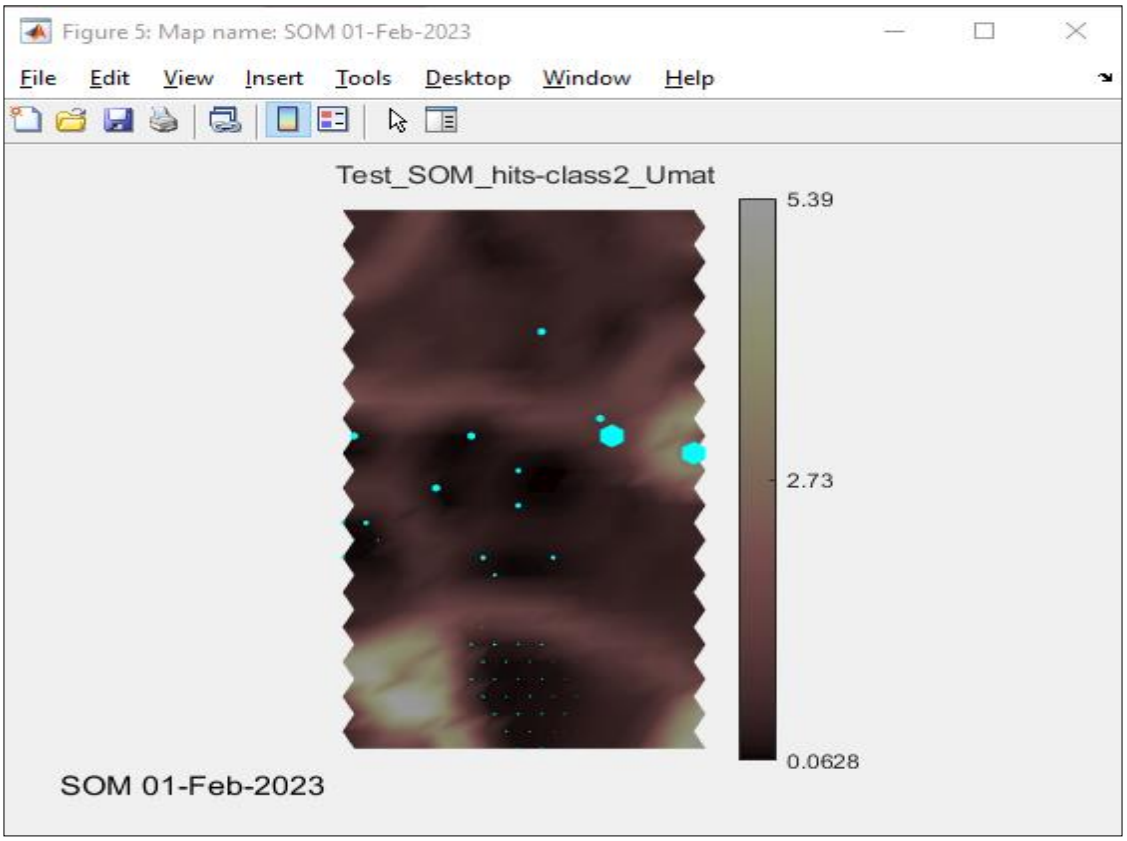

Figure 12: self organizing map with abnormal activity

As you train on the same set of data, the UMAT shows how far apart the neurons are from each other. Training data colour codes show how many neurons are close together and far apart. Brighter colours in the training data show how close together and far apart neurons are.

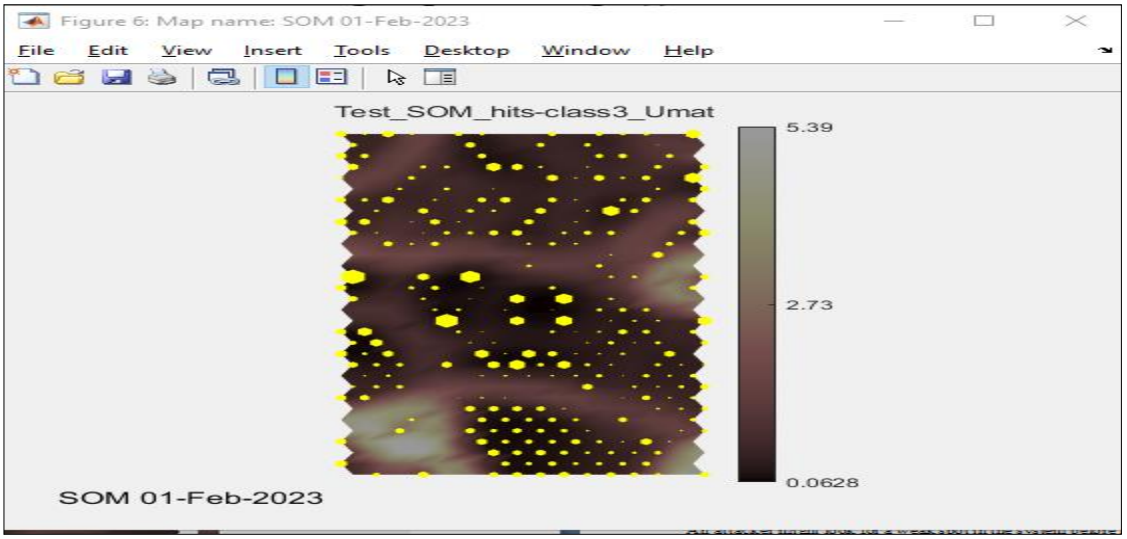

Figure 13: releasing a number of packets

An attacker might look for a weak spot in the system before he or she starts a fight. In order to find a vulnerability, many packets are sent to a lot of different hosts until they find one that is.

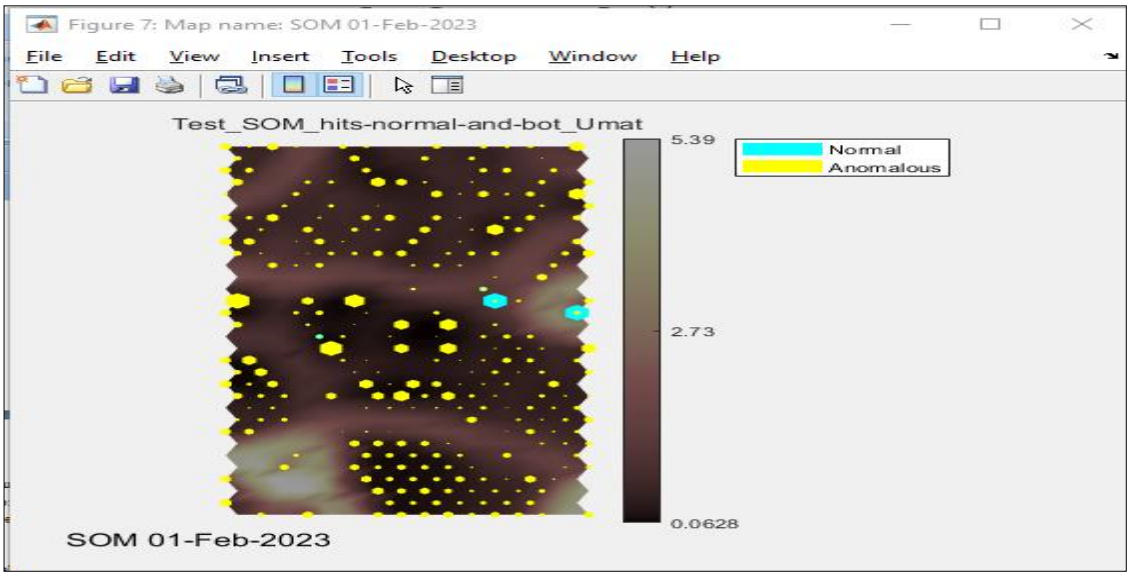

Figure 14: classification of normal and abnormal activity of network

This method was made to look for any problems with the way a machine does its job. It makes a profile for each host or network connection and records everything that happens in the system. If your profile suddenly changes, you'll be seen as suspicious. Regular users who usually log in to their accounts twice a day will make the system think that 20 logins in a single day is unusual. If the user logs on more than twice a day, it will be seen as an attack.

Accuracy is the percentage of time slots that are correctly identified to the total number of time slots. This is called the accuracy rate.

Accuracy = $\frac{T_{P+T_N}}{N}$

Table 2. Result comparison

Parameters	Accuracy (%)	True positive ratio (%)
Value	99.9	93.5

Figure 15 : Result graph

CONCLUSION

In the world we live in now, more and more gadgets and services are connected to each other through networks. This has made communication more complicated and hard to predict. In addition to making it easier for people to talk to each other and for systems and services to work together, computer networks are dynamic, always growing, and always changing. Hackers and other intruders have been changing this connected environment by causing problems or stealing information to help themselves personally or professionally. As the level of complexity goes up, the results of methods and metrics for monitoring networks, recognising malicious or unusual events, and classifying traffic become harder to explain to people who make decisions. The information that security analysts' analytical systems give them needs to be paired with tools that help them understand what it all means and come to the right conclusions. In the data-driven world of today, using deep learning algorithms as a back-end engine makes it easier to automatically tell the difference between dangerous and normal network traffic. This is done with the goal of helping people who work in security. An Intrusion Detection System has been built to protect the AODV protocol. This system uses a method that is based on the specification. We have suggested that AODV use an intrusion system tool to protect itself from some of its own threats.

REFERENCE

1. 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
2. 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
3. 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

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. Mohammad Baqer;Axel Krings Reliability of VANET Bicycle Safety Applications in Malicious Environments 2019 27th Telecommunications Forum (TELFOR) Year: 2019
11. 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
12. 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
13. 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
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. 42. Jan Lastinec;Mario Keszeli Analysis of Realistic Attack Scenarios in Vehicle Ad-hoc Networks 2019 7th International Symposium on Digital Forensics and Security (ISDFS) Year: 2019
    Yi Zeng;Meikang Qiu;Jingqi Niu;Yanxin Long;Jian Xiong;Meiqin Liu V-PSC: A Perturbation-Based Causative Attack Against DL Classifiers' Supply Chain in VANET 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) Year: 2019
17. Mevlut Turker Garip;Peter Reiher;Mario Gerla BOTVEILLANCE: A Vehicular Botnet Surveillance Attack against Pseudonymous Systems in VANETs 2018 11th IFIP Wireless and Mobile Networking Conference (WMNC) Year: 2018
18. Chunhua Zhang;Kangqiang Chen;Xin Zeng;Xiaoping Xue Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in

VANETs IEEE Access Year: 2018