ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

EXAMINING THE IMPACT OF SECURITY MEASURES ON QUALITY OF SERVICE VARIATIONS IN IOT NETWORKS

Chetna Prasad
M.Tech Scholar
Sri Aurobindo Institute of
Technology, Indore
chetnaprasad1997@gmail.com

Sunil Parihar
Assistant Professor & Head CSE, Sri
Aurobindo Institute of Technology,
Indore
sunielparihar@gmail.com

Abstract- the Internet of Things (IoT) and other new technologies have made it possible to connect devices all over the world to the internet. The main reason why these devices are often called "smart gadgets" is because they can send, receive, and process data. It is thought to be one of the fastest-growing technologies, and the number of people who use it keeps going up and up every day. The success of the Internet of Things depends on how much data is sent or received over the networks, how well the quality of service (QoS) is maintained, and how the energy limits of battery-powered devices are dealt with (IoT). At the network level, the parameters that are used to measure the quality of service are end-to-end delay, throughput, jitter, and packet delivery ratio. Since there are more Internet of Things devices connected to the network than ever before, it is very important to put a lot of focus on both the safety of the devices and the safety of the data being sent through the connections. In this paper, we tried to look at the algorithms that have been used to keep track of where source and sink nodes are so that they can't be broken into. We have also tried to figure out what effect these AODV protocols have on the quality of service that IoT networks offer. Researchers who study malware, people who work in the industry, and end users all know about them so that better ways to stop them can be used. Because of this, it is very important to make an accurate prediction of the malware early on to stop more damage. The goal of this research is to get rid of malware using K-Nearest Neighbors by predicting how it will act and then getting rid of it (KNN). We found that using these classifiers in the right way can make a big difference in how well predictions are made. MATLAB programme that was used to run the environment.

Keywords - K–Nearest Neighbor, IoT, QoS, Malware detection, Wireless Network, Security

I INTRODUCTION

The Internet of Things (IoT) is a system that lets physical objects be linked together and monitored over the internet. Things like computers, digital machines, electrical or home appliances, and so on, all of which have their own digital identities, are connected to the things around them and can share data with them. This makes it possible for the objects to connect and talk to each other in a smart way. With the help of the Internet of Things (IoT), things can connect without any interaction between people or between people and digital devices. Even though we think of tablets, laptops, computers, and cell phones as ways to connect, in reality, things can connect without us having to do anything. The needs of people who use the Internet of Things have led service providers to make a wide range of apps. The quality of services (QoS) that customers want from an app can vary from person to person. Similarly, the QoS of the many apps that use the internet of things will also be different (IoT)[1]. For each application, the quality

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

metrics should be set in a very clear way, so that a user can tell the service provider what he expects and the service provider can make changes to meet those expectations. So, the researchers should put most of their efforts into finding the QoS (Quality of Service) indicators to find out what IoT service users want. Due to how quickly the internet has grown, the number of cyber risks caused by malware has also gone up. One definition of malware says that it is a type of computer programme that is made to hurt the other user's computer in a number of ways. Malware comes in so many different forms now, and anyone can buy malware on the dark web to increase the number of attacks they launch against our system. This makes it very hard for anti-virus software to fully protect a computer. Malware, also called "malicious software," is a programme that sneaks into a computer system without the user's permission and tries to damage the system or steal private information that is stored on the system. Malicious software, which is also called "malware," is any piece of software that is made to do something bad on purpose by an enemy. Malwares are called things like viruses, worms, Trojan Horses, root-kits, spyware, backdoors, botnets, and adware, among other things, based on how they behave and how they infect computers. [2] Every day, thousands of new malicious software programmes are made, and the structure of already existing malicious software programmes is always changing, making it harder and harder to find them.

Symantec's most recent report on internet threats says that 317 million new types of malicious software have been found. Because more samples of malware are being made every day, automated tools and methods are needed to tell the difference between harmful and harmless code. Signature-based malware classification is used by almost all anti-virus software on the market. This method compares the unknown malware to a database of known malicious programmes to find out if the file in question has malware or is safe to use. A unique identifier that can be added to a binary file is called a signature. Malware's signature can be found through static analysis, dynamic analysis, or a combination of the two. Once the signature is found, it is saved in a database called the signature. The biggest problem with this strategy is that the signature database needs to be updated often because new malware is created so quickly every day. Symantec's latest report on internet threats says that 317 million new types of malware have been found. Because there are more new samples every day, automated tools and methods are needed to tell the difference between malicious and safe code. Most commercial anti-virus software uses a method based on signatures to sort malware. This method compares unknown malware to a database of known malware to figure out if a file is malware or not. The signature is a way to identify a binary file in a unique way. Malware's signature can be found using static analysis, dynamic analysis, or a mix of the two. The signature is then stored in a database called a "signature database." The biggest problem with this method is that the signature database needs to be updated often because new malware comes out every day [3-4].

IoT helps connecting help physical world to connect to computer world. As its application are increasing day by day, privacy issues are also increasing. Different attacks like spoofing, DDoS attack, and jamming, malware and eavesdropping are becoming potential threats. Small IoT devices are restricted to execute computational-intensive and latency sensitive security tasks. Today, the IoT devices are protected using authentication, in which source nodes are identified and identity based attacks are prevented, access control, secure offloading techniques and malware detection to prevent against privacy leakages. These techniques are not applied to small IoT devices like outdoor sensors, so spoofing attack on them is not recognized [5]. Machine learning techniques are applicable on IoT devices whether small or large. These techniques include: Supervised Learning: This includes support vector machine, naïve Bayes, neural network, deep neural network, random forest, K nearest neighbor to track network traffic or app traces of IoT devices to build classification or regression models [6].

IOT Attack Model: IoT systems are vulnerable to network, physical, software attacks and

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

privacy leakage. Following are the security threats to IOT devices: DoS prevent the user to access to services. DDoS attack contains thousands of IP addresses which make it impossible to identify legitimate IoT device traffic from attack traffic [7,8]. Jamming attackers send fake signals to interrupt ongoing radio transmission of IoT devices and further deplete their resources during failed communication attempt [9,10]. Spoofing node gains illegal access to IoT system. Man in the Middle attack sends jamming and spoofing signals to illegally use IoT system. Software attacks, mobile malware like Trojan, worms and viruses result to loss of data, power depletion and privacy leakage [11]

Energy Consumption- Internet of Things networks use sensors that are small and have batteries that are about the same size. Because of the way electrochemistry works, batteries lose their ability to store energy pretty fast. Because of this, it is very important that we come up with algorithms or protocols that use less battery power. To get an accurate picture of how much energy IoT networks use as a whole, it is important to look at how much energy is used at the device, network, and application layers. In terms of how much energy it uses, the Internet of Things is affected by the following: Sensors use some energy when they are sending, receiving, and processing information, as well as when they are picking up the right signals.

The amount of energy used by the sensor nodes is directly related to the distance between the energy source and the energy sink. The amount of energy used will be greater the longer the routing path is. Multi-hop algorithms have a lot of nodes that the data must pass through on its way to the final destination. In the same way, when working with cluster-based algorithms, you should expect both the number of clusters and the number of cluster heads to grow.

Different kinds of attacks could happen to the data that is being sent along the routing channel. Because of the attacks, there will be more lost packets, which will cause a lot of extra energy to be used. The main goal of location privacy algorithms is to protect the source or sink nodes from attacks by adversaries. This is done by sending fake packets to the nodes. But because of the fake packets, the length of the path gets longer, which makes the latency from beginning to end get worse. If it takes data longer to get from one end to the other, the nodes will use more energy, which will shorten the life of the network. Congestion in network traffic due to a rise in the number of data packets caused by more end users and Internet of Things (IoT) devices is another important factor that causes networks to use more energy than they should. Both of these things have led to this drop. So, future research should focus on finding a balance between the QoS of the networks, the amount of energy they use, and the level of security.

Intrusion Detection- Intrusion detection works the same way as malware detection. It uses the build to improve its ability to keep an eye on the device across the local IoT network. They also both have the duration feature, which looks for suspiciously long periods of time that could be used maliciously.

Security: Internet of Things devices are more likely to be hacked if they don't have anti-virus or malware security software. Once an attacker has access to the network, they can see both the sensitive data that is being sent over it and where it is going. Internet of Things (IoT) devices can be protected in two main ways: by protecting the data and by protecting the source and sink nodes. The rate at which people start using Internet of Things (IoT) technologies can be slowed down by a lack of data privacy, integrity, and security. Also, since each service provider has its own network for sending and receiving data, it. An Examination of How Location Privacy Algorithms Work Creating security solution that can work with all of the different networks is getting harder and harder. Because IoT devices don't have a lot of resources, it can be hard to deal with security breaches because mainframe security solutions have to meet a lot of requirements. These requirements include being able to do a lot of calculations and having a lot of space to store data. Data authentication can be a very important tool in the fight against data theft. Checking the integrity of the data at intermediate links will make sure that the data is sent or received correctly,

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

but it may slow down the transmission of the data. But because of the delays, more processing power will be needed, which will cause the nodes to use more power. If the integrity of the network is broken, retransmissions will cause the delays. The fact that Internet of Things devices talk to each other wirelessly and have limited space makes it more difficult to make security algorithms.

II LITERATURE SURVEY

The author of [12] says that the main goals of WSNs and IoT are to reduce the amount of power used to make the network last longer and to make sure it is safe. Mamdani An energy efficient secure route adjustment (ESRA) model, which is explained in [9], used fuzzy logic to figure out the most energy-efficient way to communicate. It figures out the best route by adding up the values of a number of quality-of-service criteria. Sink nodes can be moved, but to set up a new route, you need to know where the currently used sink node is. This method uses little power because it chooses the route based on how reliable it is. Cluster-based routing algorithms need a lot more energy to work because there are so many intermediate nodes in the path of communication.

The authors of [13] came up with a double level unequal clustering algorithm (DLUC) to solve the problem of clustering techniques using more power than they used to. This algorithm tells each cluster how much traffic it needs to handle. Since the cluster heads don't have to be present for information to flow between nodes, the number of clusters and nodes along the transmission line can be cut. Networks can use less energy if the bandwidth is optimized, the values of interference between control packets are lowered by using framing periods to avoid congestion, and the values of data loss are lowered. This method doesn't take into account how people move around and how different clusters are sized, which are two major factors that cause networks to use more power.

This section will try to list a few ways that have been made to keep track of the positions of source nodes, sink nodes, or sometimes both source and sink nodes, while an Internet of Things application is running. We also looked into how security algorithms affect how efficiently they use energy and how they affect quality of service measures like throughput, end-to-end delay, and packet delivery ratio. A. Where the source node is the idea of source location privacy (SLP) has become a difficult problem for research institutions to solve if they want to keep their networks safe. If SLP is not present, it will be easier to figure out where the source nodes are and get to the data before it is sent along the communication route [14]. Most of the time, a route made by the sensors will have a source node, a sink node, and a few nodes in between. In order to move data packets, these intermediate nodes will use hopping techniques. Some of the research shows that it is easy for the source's enemies to figure out where the source is, even if they know where some of the nodes are along the route that is currently being taken [15]. Because of this, it is very important to make SLP algorithms to protect IoT networks from security attacks.

In [16], a technique called SDR-m was described. SDR-m is a stochastic and diffuse routing method that uses many virtual nodes to improve SLP without having a big effect on the lifetime of the networks. Escape angle and the difference in potential components have been used to find out how things are routed. Because this method only uses the nodes that have a lot of energy available, there is no chance that the transmission will fail because there isn't enough energy. Even though the algorithm provides enough protection, there is still room for improvement to make the system even less likely to fail. Even though the number of data packets provided is good and the algorithm uses a reasonable amount of energy, it doesn't take into account how mobile the sensor nodes are, which is an important factor that must be taken into account when figuring out how much energy an algorithm used.

A second SLP called the sector-based random routing scheme (SRR), which is described in [17], helps source nodes keep their privacy by switching to new routes at regular intervals. When high

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

threshold approaches are used, the amount of energy that is used goes down. The method can protect against backtracking and direction attacks while also trying to find a balance between the level of security and the amount of power each node uses. Even though the algorithm has reduced the amount of energy used, more needs to be done to deal with the fact that the source and sink nodes are always moving around. An algorithm called SLP that is based on ring loop routing (SLPRR) to offer SLP has suggested that IoT networks could use less power and be safer. This change was written up in [18].

Sink Node Location- Sink nodes are the nodes at the end of networks that receive data. To keep sink nodes safe from attackers, you need algorithms that keep sinks' locations secret. In the absence of sink location privacy techniques, attackers can easily figure out where the sink is. This gives them access to the data packets that are being sent to the receiving end. Because sink nodes get all the data packets and, as a result, have a lot of information, privacy methods for sink nodes in networks are becoming an interesting area of study. This is because sink nodes collect all of the information. In this section, we'll talk about sink location privacy algorithms and try to name a few of them.

[19] Is a way to hide the location of sink nodes that uses a semi-random walk strategy to keep track of where sink nodes are. This algorithm is called "Semi Random Circle Routing." Because the locations of the sink nodes move around in a circular pattern, it is hard for an attacker to figure out where the target node is in the network. The QoS metrics, the PDR, and the end-to-end delay all have good values. However, the lifetime of the network is getting shorter because the energy consumption is going up as the radius grows and the sink node moves around. In [20-25], a method has been shown that uses fake sink nodes and fake data packets to reduce the risk of attacks on sink nodes. This algorithm is called a privacy-preserving strategy for sink node location in telemedicine networks (PSNL-TNs).

III PROPOSED METHODOLOGY

Figure 1 shows a block diagram of the proposed method. By looking at the proposed system's diagram in Figure 2, we can tell that no integrated algorithm has yet been found that can both improve the quality of service of the network as a whole and make the network safer as a whole. Because of this, our research is focused on a lot of different things. This means working on security issues like anonymity, route security, data security, and so on. It also means working on improving quality of service by doing things like choosing routes, making nodes run better, and so on. Most of the time, it's hard to get algorithms to work together because there are so many different domains to choose from. So, this research needs to be done to meet another need, which is to create a single algorithm that can take care of both quality of service and security, which are the two most important parts of a wireless network. Because of this research, we will be able to show that the machine learning KNN Algorithm can be used to improve QoS and security at the same time, which will make wireless networks work better overall. In general, the KNN Algorithm for machine learning can also be used to find and stop malware.

IV ANALYSIS AND DISCUSSIONS

Studying the papers in the review showed that routing algorithms can keep some of the QoS parameters, such as end-to-end delay, throughput, and packet delivery ratio, but many of the location privacy algorithms can't keep a balance between energy use and security. This was found out by looking at the papers that were included in the review. Most of the articles we've read have been successful at improving the security of source or sink nodes. However, because fraudulent packets are added along the route, the amount of energy used goes up. There is a direct and inverse link between how much energy a network uses and how long it lasts. When the amount of energy needed to run privacy algorithms goes up, the amount of time a network can last goes down. Because of this, it is very hard to put in place security and privacy algorithms for Internet of Things devices that have limited energy. We can reduce the number of times a route needs to be

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

recovered by setting up a backup route mechanism in the coverage area of the RSU that just passed by. This will cut down on how often a route needs to be found again. The right way to do it is to create a backup route from a serving RSU that has already passed by.

Case -1- The number of nodes in a VANET has nothing to do with the network's ability to grow or expand without limits. V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) are the two types of communication in VANET (Vehicle to Infrastructure). Nodes in both types of communications get information from other nodes or from RSU, so the information must be accurate. VANETs have different security requirements for how vehicles should talk to each other. VANETs are a type of network that is made for nodes that need to send time-sensitive information in a safe way but also need to be able to move around easily and have a network structure with no boundaries. The two parts of the routing protocol that are being talked about in this conversation are proactive and reactive communication. The AODV protocol provides reactive routing based on what users want. AODV won't figure out the route unless it's clear that it's needed. It has a route request-response system that lets it send a request to figure out the route and then get a response. Based on the response, it figures out the best route. Because vehicles move around in a V2I communication environment, the passed-by serving RSU may notice that the link to the 1-hop vehicle on the way to the destination vehicle disconnects often. In this case, AODV is able to fix the broken link by forcing the RSU to send a route error (RERR) message to the predecessors. But from the point of view of the vehicle network, the RSU has no predecessors. This means that the RSU needs to find a new way to get to the vehicle it is supposed to follow. In a vehicle network with a limited number of wireless connections, this is a hard and time-consuming task.

So that a route doesn't have to be fixed as often, we're going to set up a backup route mechanism within the coverage area of the RSU that has just gone by. Setting up a backup route from a serving RSU that has passed by is the method that must be used.

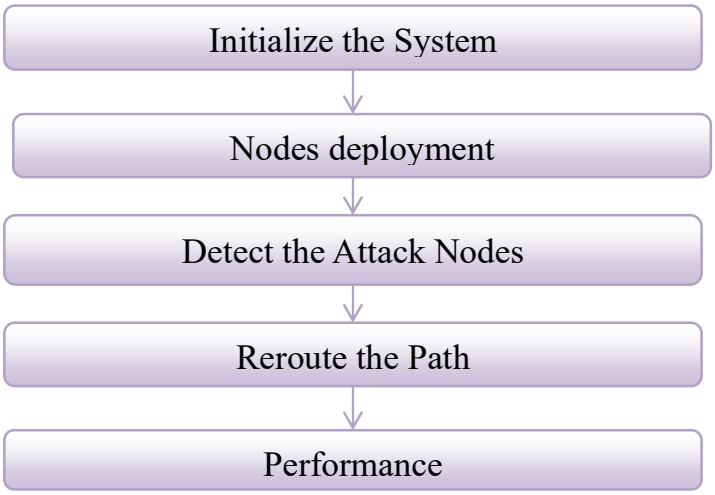

Fig.1 Simulation Flow Diagram

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

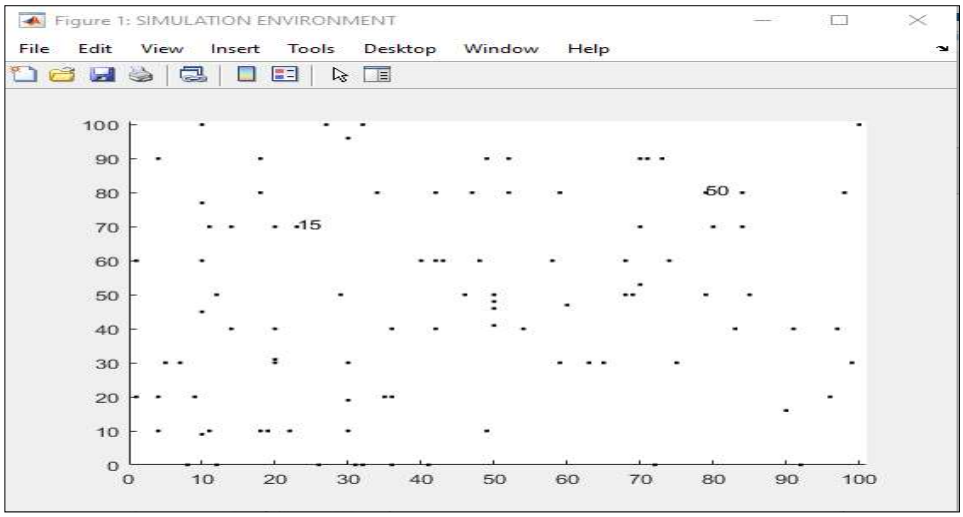

Fig.2 Initialization Network

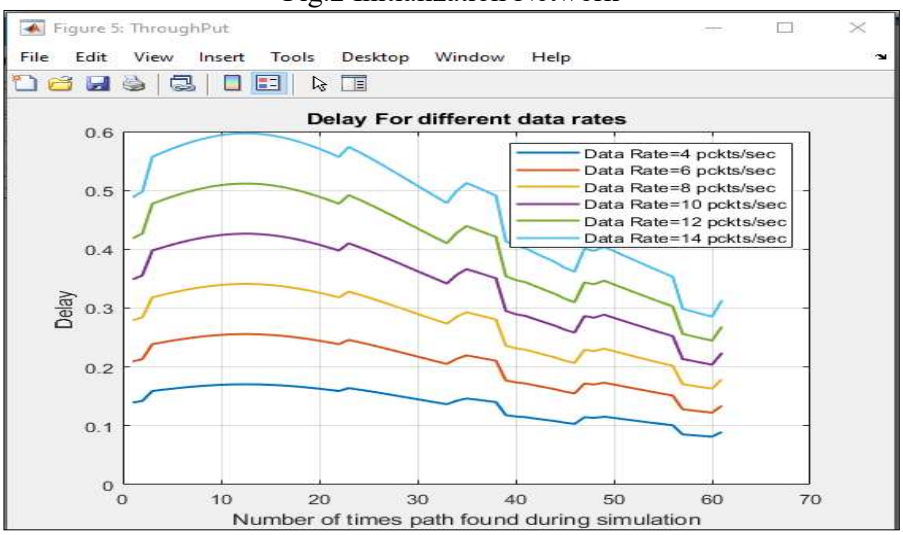

Fig.3 Delay for Different Data Rates

Source node -> path node-> destination node

Path node, we have 100 nodes the data transmit from source to destination through nearest available nodes the data delay transmission through path showing in the fig. 3

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

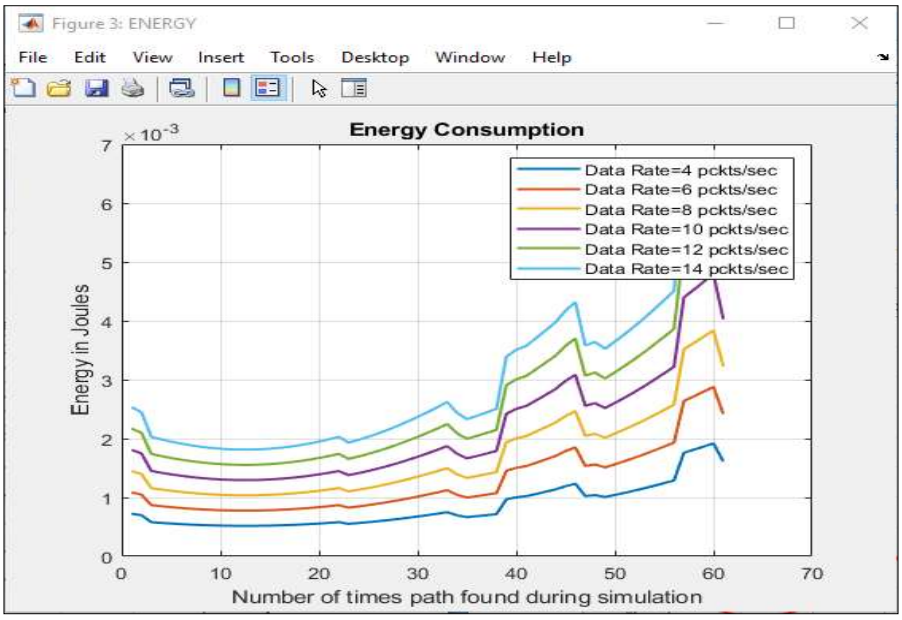

Fig.4 Energy Consumption for Different Data Rates

The data transmit from source to destination through nearest available nodes the data energy consumption for different data rates transmission through path showing in the fig. 4

Fig.5 Number of Path Found During Simulation

The data transmit from source to destination number of path found during simulation showing in the fig.5

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

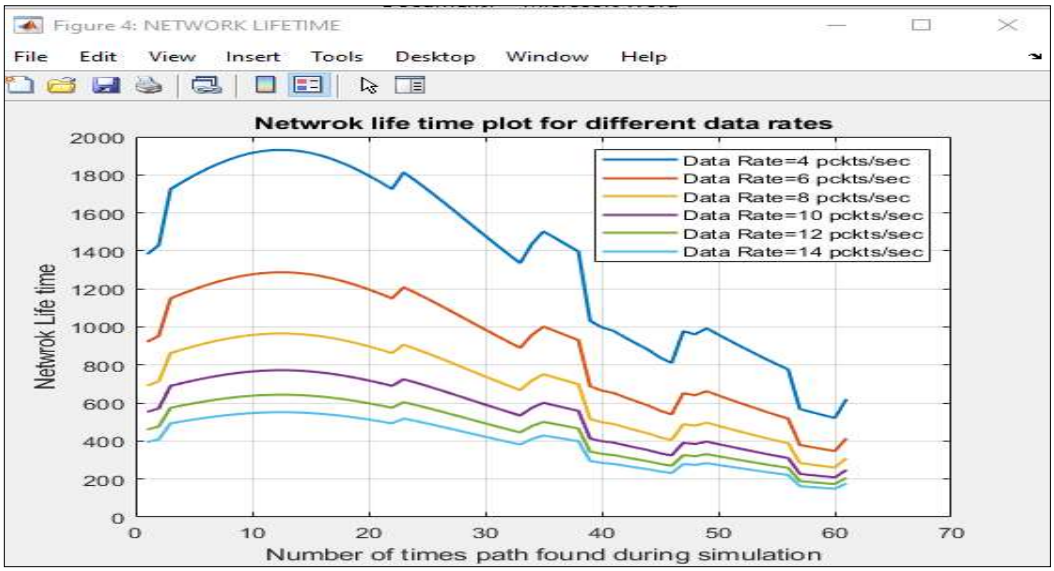

Fig.8 Network Life Time for Different Data Rates

The data transmit from source to destination through nearest available network life time for different data rates while data transmission through path showing in the fig. 8

Case-2

Malware Detection -As the picture shows, the system will start by setting up a normal wireless network. This network will use standard algorithms to improve service quality and make sure the network is safe. When one of the performance evaluation metrics is not met, both this security performance and the QoS performance will be fine-tuned. As a direct result of the proposed work, the following things are likely to happen: showing in the fig. 9

- Improved QoS for any kind of wireless network
- Adaptive security for wireless networks
- A KNN algorithm will be used for performing Malware detection
- Flexibility in terms of security and QoS of the network

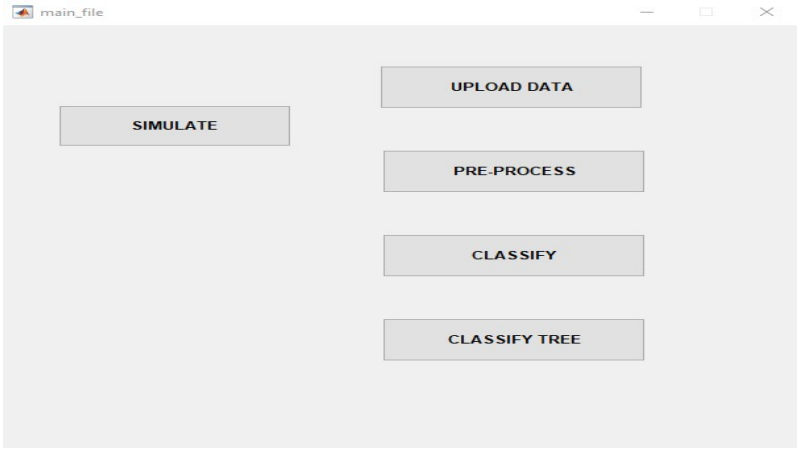

Fig.9 Flow Diagram for Malware Detection

Using machine learning will help with the ongoing configuration of the network. This means that the network will always have the latest security and quality of service features. The quality of service (QoS) will go up, which will speed up how quickly security attacks are dealt with.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

Sink Node Location- Sink nodes are the nodes at the end of networks that receive data. To keep sink nodes safe from attackers, you need algorithms that keep sinks' locations secret. In the absence of sink location privacy techniques, attackers can easily figure out where the sink is. This gives them access to the data packets that are being sent to the receiving end.
Source and Sink Location- The authors of [10] used a K-means cluster-based method to keep track of the locations of both source and destination nodes in WSNs used in the Internet of Things. This was done to make sure that no data would be lost. The real source and sink nodes are kept safe by a large number of fake nodes that are used both as source nodes and as sink nodes. With the help of a clustering mechanism, data packets can be sent to multiple sink nodes. This algorithm helps to keep the routing path the same length while protecting the flow of data in both directions. The latency has been cut down because the real packets are now sent through the shortest route. The proposed solution gets better results in terms of safety time, but it can't prove that it's an energy-efficient protocol because it increases the number of false sink nodes.
Learning-Based IoT Malware Detection: IoT devices can use supervised learning methods to look for malware by analyzing how applications behave while running. The K-NN method of finding malware puts network traffic into the category that has the most items out of its K nearest neighbors.
Data Collection For this project, we have a malware dataset that is derived using the open source software tools. The pe header analysis tools were used to extract the required features from the malware file which is then used for the further steps of the proposed system as in Figure 1. Ten malware categories used in this research are: virus, trojan, adware, backdoor, muldrop, sdbot, spam, rbot, ransom ware and unknown.
Pre Processing-In this phase of proposed work, data pre-process has been done for the dataset which we have visualized in the previous section. This step is done to make data more appropriately fit into proposed model for training purpose. In this step, we closely looked on the features and tried to make possible changes in the dataset for getting more efficient results. Generally pre- processing step consist Cleaning, transformation, and Reduction of three sub steps which are to be followed for preparing the dataset to train: In the cleaning phase, all the garbage entries present within the dataset that are not suitable for modeling are removed. Let’s say our dataset doesn’t contain any relevant data in some particular cell then we have to assign some integer value to these non-relevant entries. This assigning of integer values has many approaches to achieve that. In the transformation phase, all the non-integer values are converted into integer values because integers are suitable for computation work as compared to strings or characters that is non-integer values make it difficult for the model to train over it. In the last phase of data cleaning or pre- processing, reduction plays a vital role since our data may contain many irrelevant features which don’t accounts in the prediction of the malware category. Therefore removal of those irrelevant features from the dataset is done in this phase of our proposed work.
K-NN is a way to classify data that doesn't need to know anything about it ahead of time. It works on the idea that the new sample label is chosen only by the label of the samples nearest neighbour [2, 3]. The k-nearest neighbour (k-NN) method is not only easy to understand, but it is also easy to put into practise in a short amount of time. It is both one of the easiest and most popular machine learning algorithms**.** [4] In KNN-CV, we have seen that training data set is divides as three parts as Training data, Cross validation data and Testing data. When we use this method for algorithm, we are unable to use the training data set as much as possible. So K-Fold KNN is the way to utilize the data we have as much as possible

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

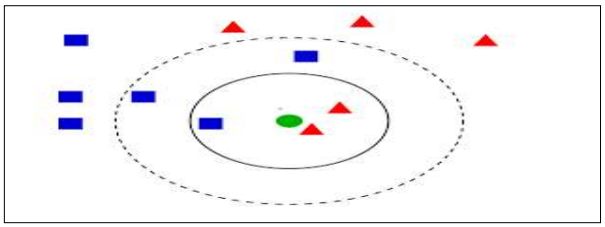

Fig 10 : An abstract of KNN

- Split the training data set we have as Training and Testing. We will only use testing data for finding accuracy for our KNN model.
- Now split again the Training data as K" fold times.
- Now consider three parts for training and one part for testing. And change this combination for possible times for Every K values to find the Best K.

Data evaluation k-Fold Cross Validation is the type of evaluation data that was used for this investigation. In the process of cross validation, the dataset is split into k different folds. The process is repeated until all of the data have been looked at. During each iteration, the data from each fold are used as test data once, and then the data from the remaining folds are used as training data.

Classification of the information After collecting the distribution of training data and test data from the evaluation of the model using k-Fold Cross Validation, the data is then put into groups using k-NN to figure out how well the model is working. This process is repeated until the k-Fold value reaches 10, or until the highest level of precision is reached. After the last step, which consisted of evaluating the k-FCV algorithm to figure out the training data and test data, is done, the next step is to start classifying the data using the k-NN method.

The following are the research stages in the k-NN method.

- Determine the value of k.
- Calculate the Euclidean distance of the test data with the training data in the dataset.
- Display the Euclidean distance ascending.
- Take the smallest distance of k.

The results of data classification using the k-NN method

This is the most crucial part in whole work since in this module only trained our model to predict the malware type as discussed in the dataset module. We have used two most famous modelling techniques for training on our model on the given dataset which contains various features to predict the type of malicious content and compared the results extracted from both of the models after training it on the particular dataset by using KNN Classifier. KNN model implements the technique of clustering in which the whole dataset is divided into some specific number of clusters whose cluster head is the centroid of the cluster nodes. In each of the iteration, the centroid for a particular cluster updates as a new node joins the cluster. For calculating the distance between instances, various distance algorithms are used such as: i. Euclidean Distance: This algorithm is mainly used for real valued input-variables and is given by the following mathematical formula:

Euclidean Distance(x, xi) = sqrt(sum((xj – xij)^2))

Hamming Distance: It is helpful in calculating distance between binary valued input- variables.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

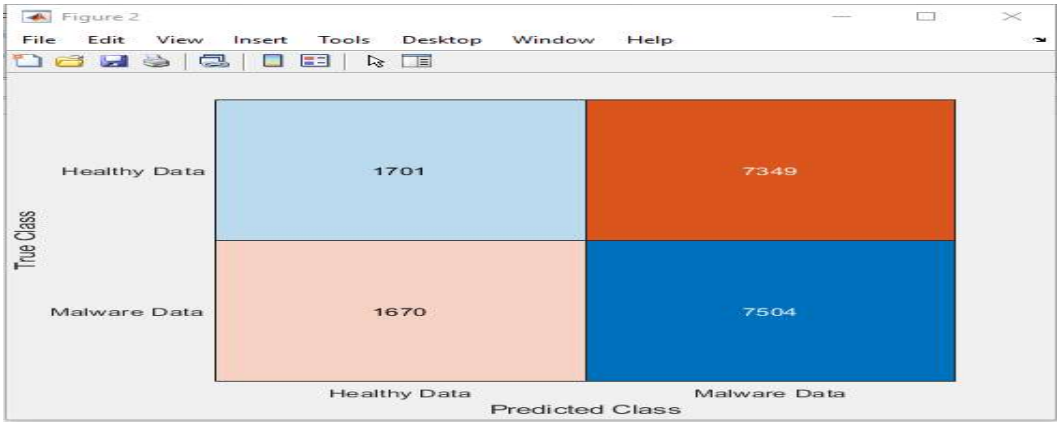

Fig.11 Test Result Dataset

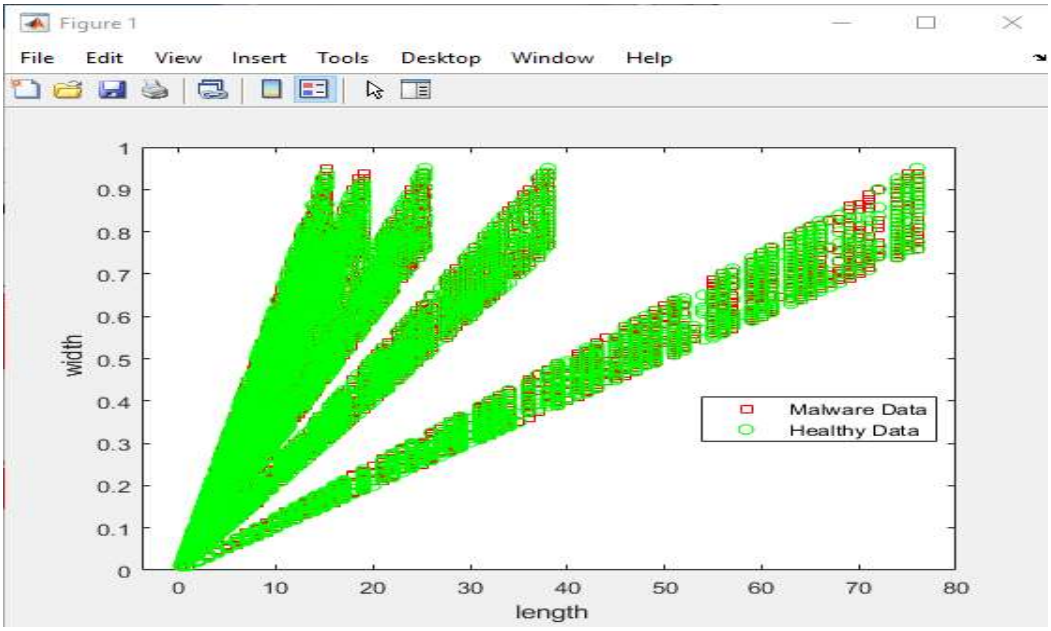

Fig.12 traning of malware and heathy data

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

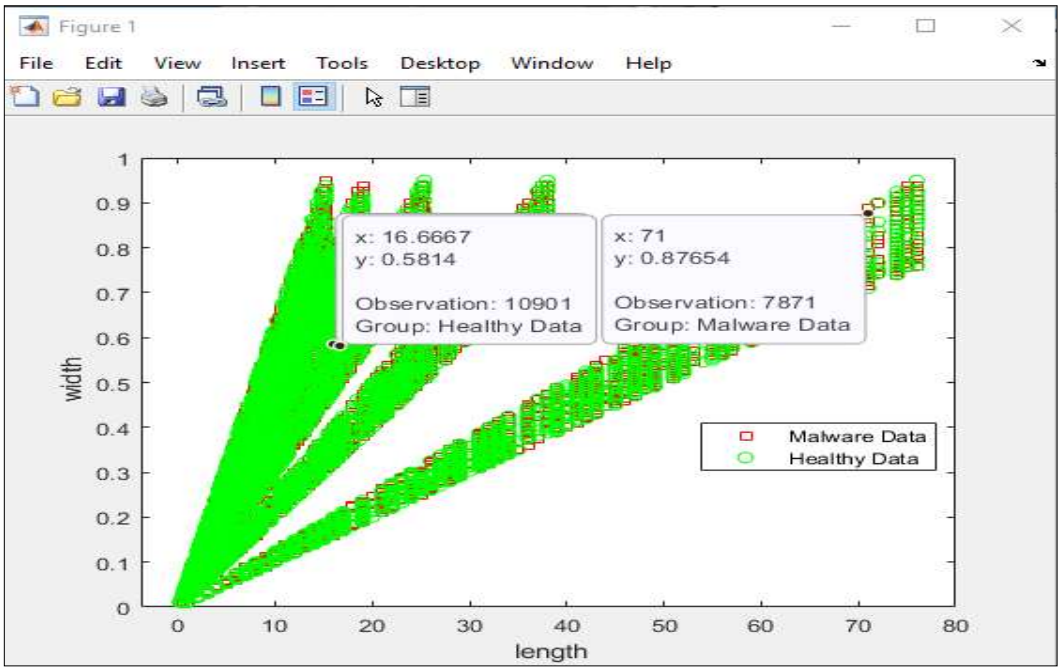

Fig.13 Obesrvation Of Healthy Data And Malware Data

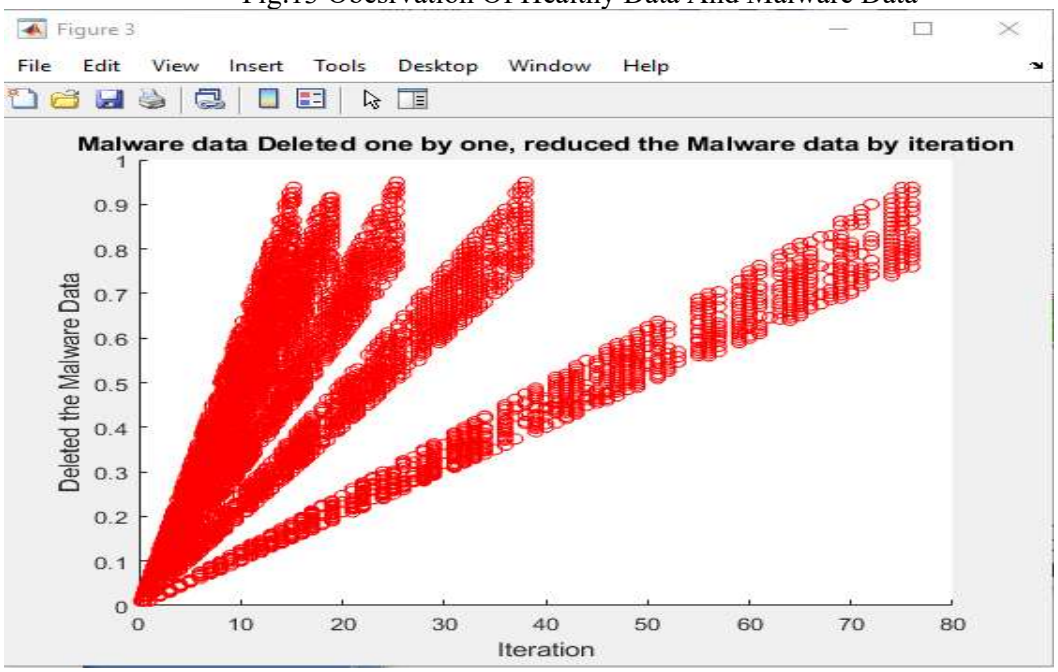

Fig.14 malware data delation

In the fig.14 x axis showing the iteration and Y axis showing the different category set of datas

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

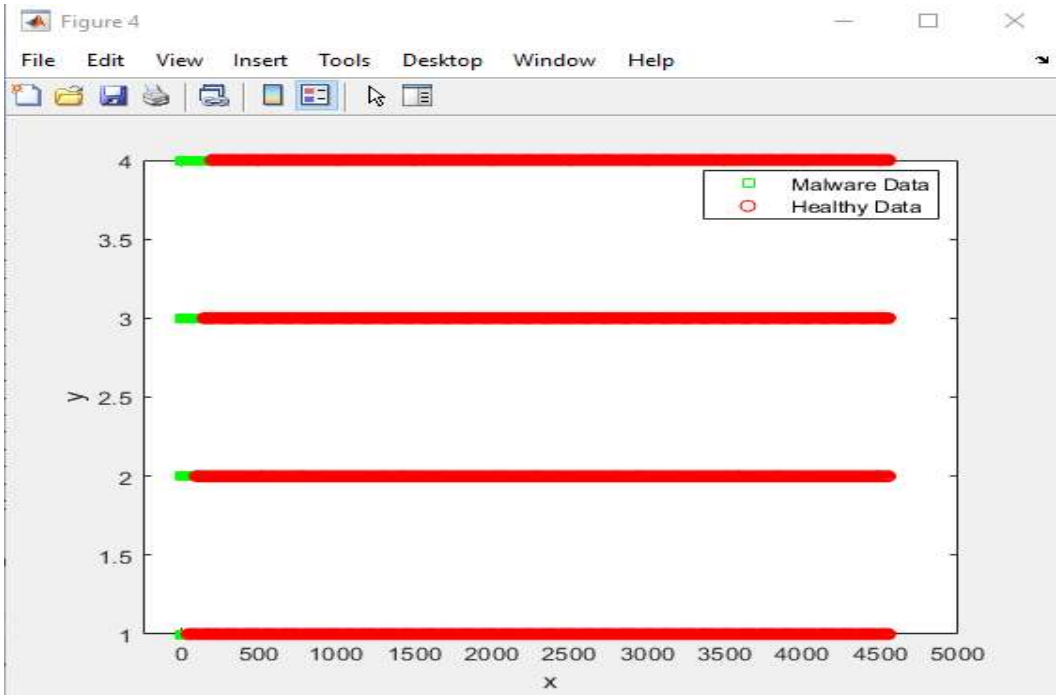

Fig.15 seprate the malware and healthy data

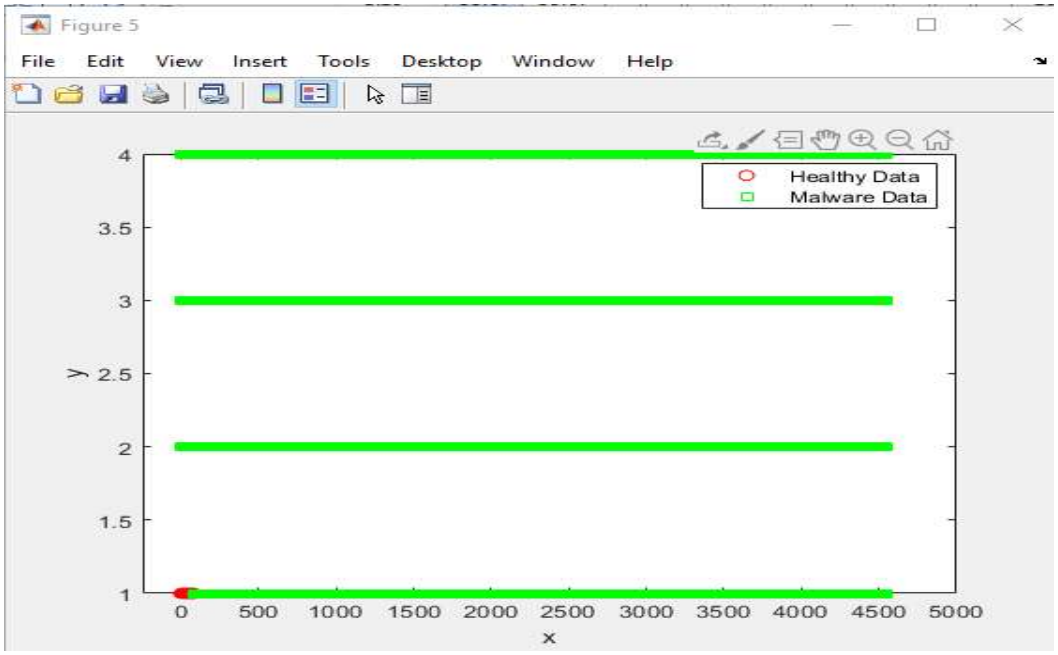

Fig.16 malware data deletion

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

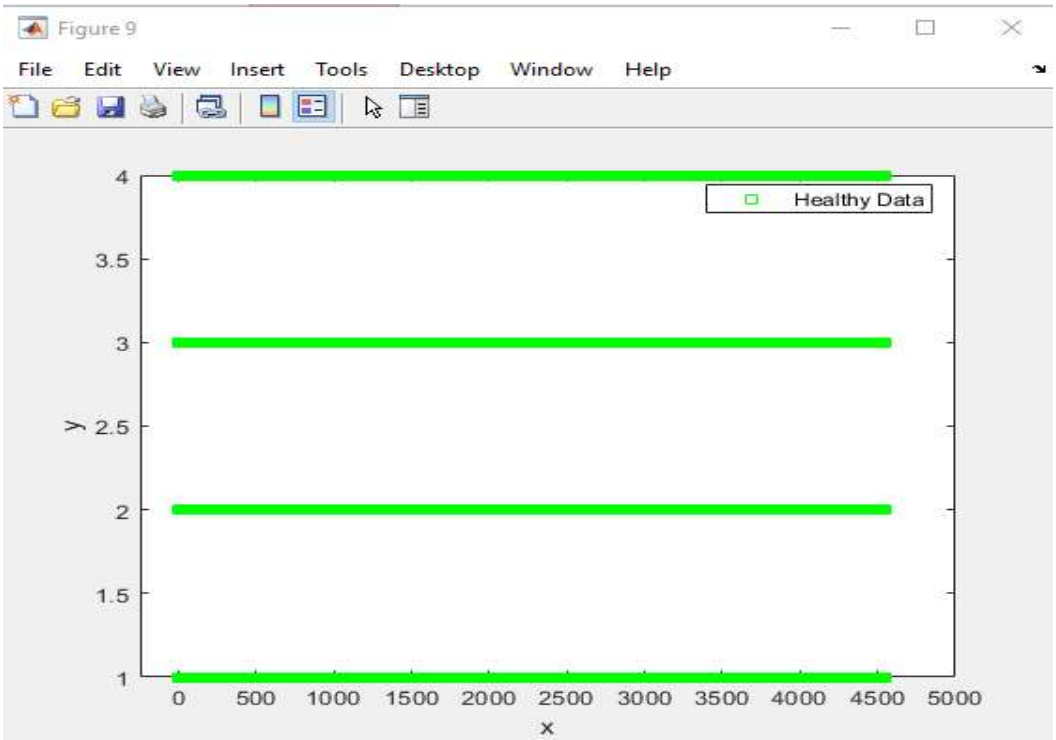

Fig.17 Heathy data after malware deletion

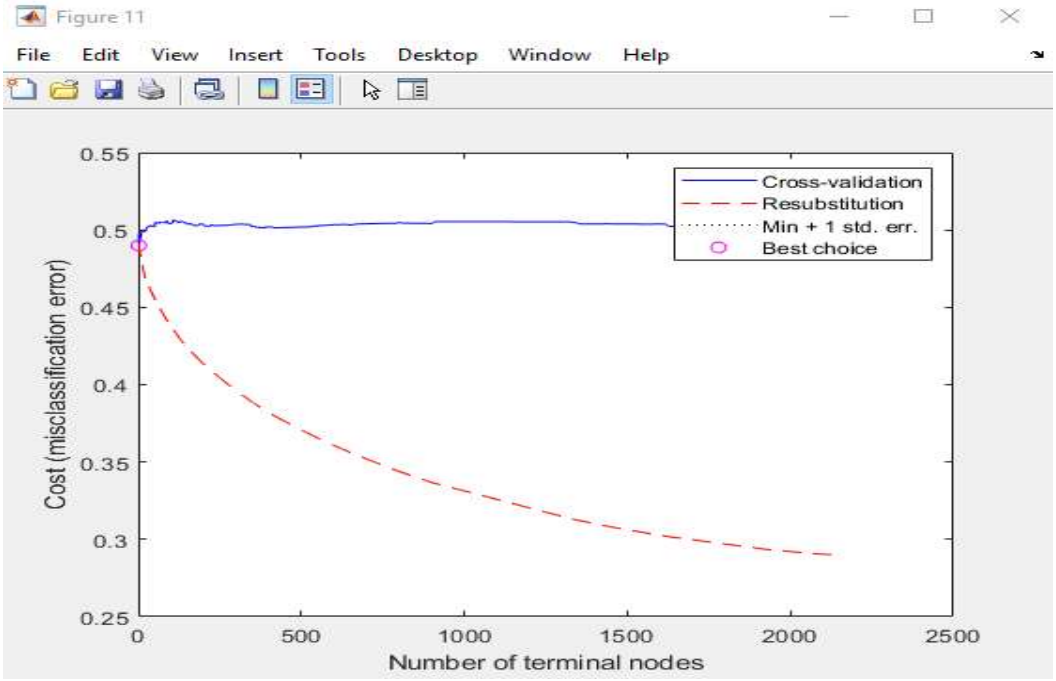

Fig.18 cross validation

It lets us make better use of our data and gives us a lot more information about how well our algorithm is working. Cross-validation is a resembling method that is used to test machine learning models with a small set of the available data. a single parameter called "k" that tells how many groups should be made from the data sample given. For the k-fold cross-validation, all that is needed is to use the cross-validation method more than once and then give the average result from all folds and runs. The standard error gives us an idea of how accurate this mean result will

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

be as a measure of the model's true underlying mean performance on the dataset, which we don't know.

Table 2 IoTQOS Result

Parameters values	**Parameters values**
Avg Delay	206.118855
Avg Energy	84.594327
Avg PDR	274.825140
Avg Through	206.118855

The Internet of Things (IoT) is a technology that is growing quickly and is going through a lot of changes right now so that people can get better services. In this survey report, the architecture explains what each layer of the Internet of Things does, and the taxonomy explains the factors that determine the quality of the services. Also, the metrics that need to be worked on to improve the quality of the services as a whole were given. In the future, this can be expanded by suggesting new ways to deal with problems like unstable links, traffic, node failure, packet loss, lifetime of node, congestion, and other similar problems in order to improve Quality of Service in the Internet of Things (IoT). Only a few different metrics were looked at in this work. In the future, the metrics can be explained in greater detail.

Table 3 Compare the Proposed Results with Existing Work

Parameters	Proposed Work	Existing Work[1]
	AODV-KNN	RL-QRP
Avg Delay	290.65	351
Avg Energy	173.05	196.3
Avg PDR	144.15	136.7
Avg Through	108.11	136.7

Table 4 Network Simulation Result at Different Data Rates

Data Rates	Delay	Energy Consumption	Network Life Time
Data Rate 4	0.11	0.9	1399
Data Rate 6	0.21	1.1	950
Data Rate 8	0.29	1.5	750
Data Rate 10	0.35	1.9	590
Data Rate 12	0.43	2.1	490
Data Rate 14	0.49	2.5	400

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

Table 5 KNN classification results

Classification technique	Accuracy (%)	Malware node remaining
KNN	96.50	349

V CONCLUSION

The proposed method increases security from source to destination without hurting the network's lifespan. However, there is still room for improvement in terms of cutting energy use along both the transmission and reception paths. The study of algorithms that are used to keep track of where the source and sink nodes are shows that quality of service, energy efficiency, and security are the factors that determine how well IoT applications can be used by end users and how likely they are to be adopted by them. To meet the Internet of Things (IoT) requirements for network security, both data security and protecting the locations of nodes that send and receive data are needed. Internet of Things devices that run on batteries have energy limits that have a big effect on how security algorithms are put into place. We've talked about some of the things that can affect how long IoT networks last and how safe they are. Concerns about the Internet of Things' quality of service (QoS) and security can be addressed with technologies like cognitive radio networks, fog computing, and machine learning. After figuring out what the end customers want, service providers can use these technologies to build real-time applications. Even though the level of security provided by different apps can be very different, any breach in security or attempt by bad actors to get through it can cost the end users a lot of money. When it comes to health care applications, a lack of security can put a person's life in danger. When it comes to military applications, a lack of security can be a threat to the security of the whole country. In the future, we will try to use techniques like machine learning to protect IoT networks and improve service quality.

References

1. Manisha Bhatnagar Dolly Thankachan Identifying the Effects of Security Measures on QoS Variations for IoT Network: An Application Perspective Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021). IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4
2. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. “Internet of Things security: A survey”. In: Journal of Network and Computer Applications 88 (2017),
3. pp. 10–28.
4. C. Alcaraz, P. Najera, J. Lopez, and R. Roman. “Wireless sensor networks and the internet of things: Do we need a complete integration?” In: 1st International Workshop on the Security of the Internet of Things (SecIoT’10). 2010.
5. J. Arkko, D. Thaler, and D. McPherson. “IETF RC 7452: architectural considerations in smart object networking”. In: IETF, Fremont, US (2015).
6. M. A. Bhabad and S. T. Bagade. “Internet of things: architecture, security issue and countermeasures”. In: International Journal of Computer Applications 125.14 (2015).
7. G. Breed. “Wireless ad hoc networks: basic concepts”. In: High frequency electronics 1 (2007), pp. 44–47.
8. L.-H. Chang, T.-H. Lee, S.-J. Chen, and C.-Y. Liao. “Energy-efficient oriented routing algorithm in wireless sensor networks”. In: 2013 IEEE International Conference on Systems, Man, and Cybernetics. IEEE. 2013, pp. 3813–3818.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

9. M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally. “Internet of things (iot): Research, simulators, and testbeds”. In: IEEE Internet of Things Journal 5.3 (2017), pp. 1637–1647.
10. A. Chhabra, V. Vashishth, A. Khanna, D. K. Sharma, and J. Singh. “An energy efficient routing protocol for wireless internet-of-things sensor networks”. In: arXiv preprint arXiv:1808.01039 (2018)
11. HamidiĞ Alaoui, Z, El Belrhiti El Alaoui, A. FMĞ MAC: A fastĞ mobility adaptive MAC protocol for wireless sensor networks. Trans Emerging Tel Tech. 2020; 31:e3782. https://doi.org/10.1002/ett.3782
12. Kumar, S, Sharma, B, Singh, AK. An efficient algorithm for backbone construction in cognitiveradionetworks.IntJCommunSyst.2020;33:e4345. https://doi.org/10.1002/dac.4345
13. DadashiGavaber, Morteza, Rajabzadeh, Amir, “BADEP: Bandwidth and delay efficient application placement in fog-based IoT systems”, Transactions on Emerging Telecommunications Technologies, 2020
14. Gomes, PH, Krishnamachari, B. TAMUĞ RPL: Thompson sampling based multichannel RPL. Trans Emerging Tel Tech. 2020; 31:e3806.
15. H. Liang, S. Yang, L. Li, and J. Gao. “Research on routing optimization of WSNs based on improved LEACH protocol”. In: EURASIP Journal on Wireless Communications and Networking 2019.1 (2019), p. 194.
16. K. L. Lueth. IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year. https://iot-analytics.com/iot-2019-in-review/. Accessed: 2020-3-13.
17. K. L. Lueth. IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally. https://iot- analytics.com/iot- platform- companies- landscape2020/. Accessed: 2020-04-09
18. K. L. Lueth. The Effect of the Internet of Things on Sustainability. https://iotanalytics.com/effect-iot-sustainability/. Accessed: 2020-04-09.
19. K. L. Lueth. Why the Internet of Things is called Internet of Things: Definition, history, disambiguation. https : //iot analytics.com / internet -of - things -definition/. Accessed: 2020-3-13.
20. Z. Magubane, P. Tarwireyi, and M. O. Adigun. “Evaluating the Energy Efficiency of IoT Routing Protocols”. In: 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC). IEEE. 2019, pp. 1–7.
21. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. “Internet of things (IoT) security: Current status, challenges and prospective measures”. In: 2015 1 International Conference for Internet Technology and Secured Transactions (ICITST) IEEE. 2015, pp. 336–341.
22. M. A. Mahmud, A. Abdelgawad, and K. Yelamarthi. “Energy efficient routing for Internet of Things (IoT) applications”. In: 2017 IEEE international conference on electro information technology (EIT). IEEE. 2017, pp. 442–446.
23. R. Minerva, A. Biru, and D. Rotondi. “Towards a definition of the Internet of Things (IoT)”. In: IEEE Internet Initiative 1.1 (2015), pp. 1–86.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

24. F. Muhammad, W. Anjum, and K. S. Mazhar. “A critical analysis on the security concerns of internet of things (IoT)”. In: International Journal of Computer Applications (0975 8887) 111.7 (2015).
25. A.-S. K. Pathan and C. S. Hong. “A secure energy-efficient routing protocol forWSN”. In: International symposium on parallel and distributed processing and applications. Springer. 2007, pp. 407–418