SECURE ROUTING-BASED ENERGY OPTIMIZATION FOR IOT APPLICATION WITH HETEROGENEOUS WIRELESS SENSOR NETWORKS

Bhavya Rathore	Dr. Bharat Singh Deora
Research Scholar CS	Sr. Assistant Professor, CSE
Janardan Rai Nagar Rajasthan Vidhyapeeth, Udaipur	Janardan Rai Nagar Rajasthan Vidhyapeeth, Udaipur

ABSTRACT

The internet of things (IoT) is a complex system that includes multiple technologies and services. However, its heterogeneity can result in quality-of-service (QoS) issues, which may lead to security challenges. Software-defined network (SDN) provides unique solutions to handle heterogeneity issues in large-scale IoT networks. Combining SDN with IoT networks has great potential for addressing extreme heterogeneity issues in IoT networks. Numerous researchers are investigating various techniques to resolve heterogeneity issues in IoT networks by integrating SDN. Our study focuses on the SDN-IoT domain to improve QoS by addressing heterogeneity. Heterogeneity in SDN-IoT networks can increase the response time of controllers. We propose a framework that can alleviate heterogeneity while maintaining QoS in SDN-IoT networks. The framework converts m heterogeneous controllers into n homogeneous groups based on their response time. First, we examine the impact of the controller's bandwidth and find that the system throughput decreases when the controller's bandwidth is lowered. Next, we implement a simple strategy that considers both the bandwidth and service time when selecting the peer controller. Our results show some improvement in the framework, indicating its potential to alleviate heterogeneity while maintaining QoS and other metrics.

Keywords: software-defined networks; internet of things; quality of service; security

DOINUMBER:10.48047/NQ.2022.20.19.NQ99426 NEUROQUANTOLOGY2022;20(19):4634-4644

INTRODUCTION

Recently, sensor networks have emerged as the most promising amalgam of communication and micro-electromechanical systems (MEMS), thanks to the advancements in both of these fields of study. A large number of distributed sensor nodes having networking capabilities working jointly for data gathering are generally termed as wireless sensor network WSN [1] as illustrated in Figure 1. Sensor nodes are dispersed across the study area; each sensor node collects data about its immediate surroundings and relays that information to a sensor coordinator node. The coordinator node further directs the data to the gateway sensor node using an appropriate routing algorithm. The data collected by the multiple coordinators' nodes is sent to a distant computer for additional analysis through the gateway sensor node. The WSNs have brought a paradigm shift in the field of remote sensing and automation by making it feasible to study the places where

human intervention is very difficult like glaciers, dense Forests, etc.

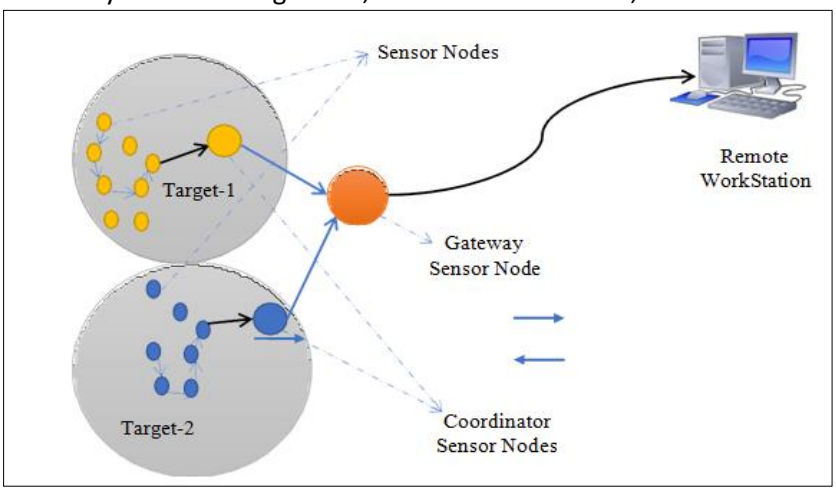

Figure 1: Illustration of Wireless Sensor Network

The sensor nodes (also called motes) in WSN are tiny battery-operated devices [2] that can perceive the natural signals using transducers, convert the analog physiological data to the digital format using an analog to digital converter (ADC), process using microcontroller, and communicate the data to a remote server using radio frequency (RF) module as shown in Figure 2 [3]. These motes are positioned in the desired fashion at the place of analysis within a WSN [4].Wireless Body Area Network (WBAN) [5], the leading application of WSN [6] [7], is used for human body vital parameters monitoring like body temperature, electrocardiogram (ECG), electroencephalogram (EEG).

WSNs have been used for a wide range of things, such as monitoring health, keeping an eye on the environment, keeping an eye on structures, keeping an eye on habitats, and helping with disaster management. Wireless sensor networks (WSNs) will have to connect to the internet in the future because there are so many important WSN applications. The integration makes it easy to connect to devices that don't need human supervision and gives high-resolution information about what's going on. In fact, connecting WSNs to cloud storage and the internet is one of the most important technologies for making the Internet of Things (IoT) a reality.

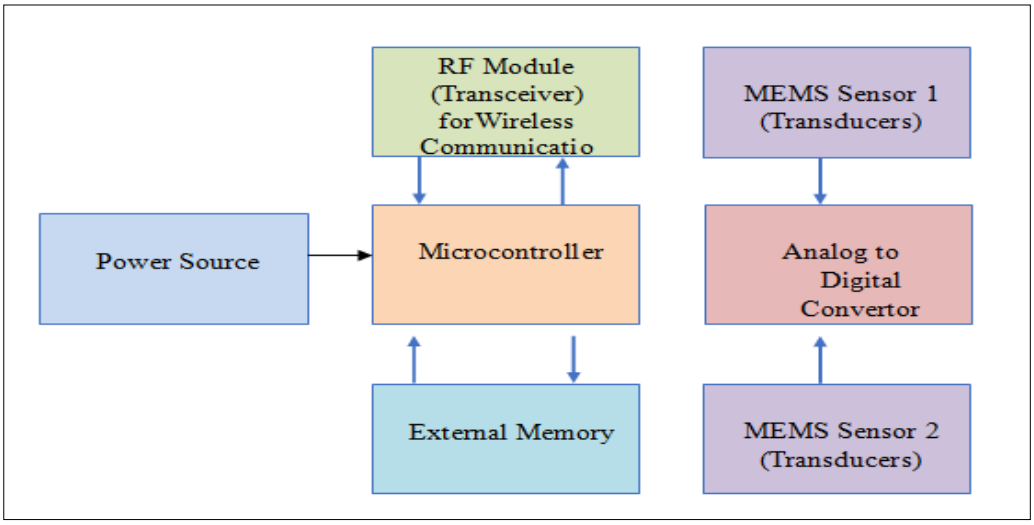

Figure 2 : Architecture of Wireless Sensor Node (Mote)

Low-power multi-function sensor devices can now detect and react to changes in their surroundings because to the fast development of wireless communication systems, small-scale energy sources, microprocessors, low power digital circuits, and low power radio technologies. Small microprocessors, batteries, and transducers are the brains of these sensor devices, which are placed in their environments to monitor changes and relay that data. Then, with this information, decisions can be made about how to respond to the changes. As a direct result of this, low-power and tiny wireless sensor devices have made it easier to build wireless sensor networks (WSNs).

PEGASIS

PEGASIS is a different way to choose which CH nodes to use. Figure 3 shows how the PEGASIS routing protocol [82] is set up and how the sensor nodes work together to make a chain for transmissions. Each node gets information from a neighbouringhub and sends it to the following hub in the organization. The two end hubs send the data down the chain that makes up the routing structure to the leader node. The leader node then sends the data to the BS. The data is sent to the BS by a leader node that is chosen at random. PEGASIS focuses on shortening the distance data has to travel between nodes to cut down on the amount of power each one needs to run. But only one node in each round is chosen to be a CH node. It could become a bottleneck, causing some packets to take longer to send and lose data. It also quickly uses up the energy of the node chosen as the leader by making it send packets more quickly.

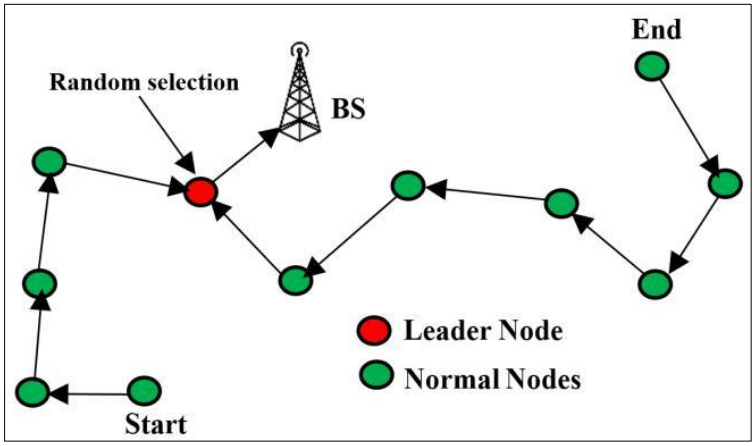

Figure 3 PEGASIS protocol architecture.

Optimal Path Selection

Researchers have thought a lot about how to find the best paths through WSNs to use the least amount of energy. In the many-to-one WSN [97], routing trees are often made using the shortest path strategy. The potential benefits of taking the briefest way are less time squandered and less energy utilized. Bannered et al. thought of a multi-bounce heuristic strategy for topographical steering. This convention picks a course with the least number of jumps and the most limited in general distance.By using the proposed method, the delay from one node to the next is cut down. The first networks that used the shortest route from a source node to a destination node were made in [99]. The result is a method that extends the life of a network while keeping link costs as low as possible.

PROPOSED METHODOLOGY

The proposed method can be shown using the block diagram in Figure 4.1. From this diagram, we can see that no integrated algorithm has yet been found that can improve both the nature of administration and the security of the organization in general. Because of this, our research is focused on a lot of different things. This implies chipping away at security issues like namelessness, course security, information security, etc. 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 significant pieces of a remote organization. Due to this examination, we will actually want to show that the AI KNN Calculation can be utilized toimprove 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.

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 doesn't have any predecessors. Because of this, the RSU needs to find a new way to get to the vehicle that is its target. In a vehicle network with a limited number of wireless connections, this is a hard and time-consuming task.

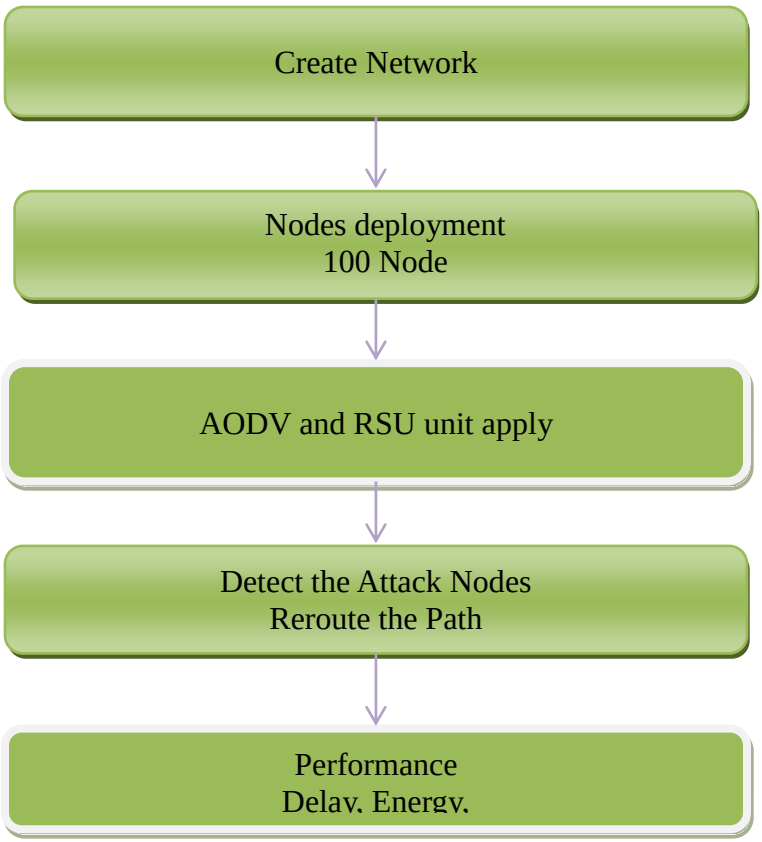

Figure 4 : Proposed Flow Diagram

The field of study called "vehicular ad-hoc networks" (VANETs) is both powerful and active, and it has led to a number of problems with routing protocols and communication with other vehicles or "roadside units," which are fixed infrastructure (RSU). In VANET environments, where the topology is always changing and there are many obstacles, routing data and talking between vehicles is hard because of the obstacles and the way the topology is set up. This is especially true for applications in vehicles that need reliable communication and a good level of service (QoS).

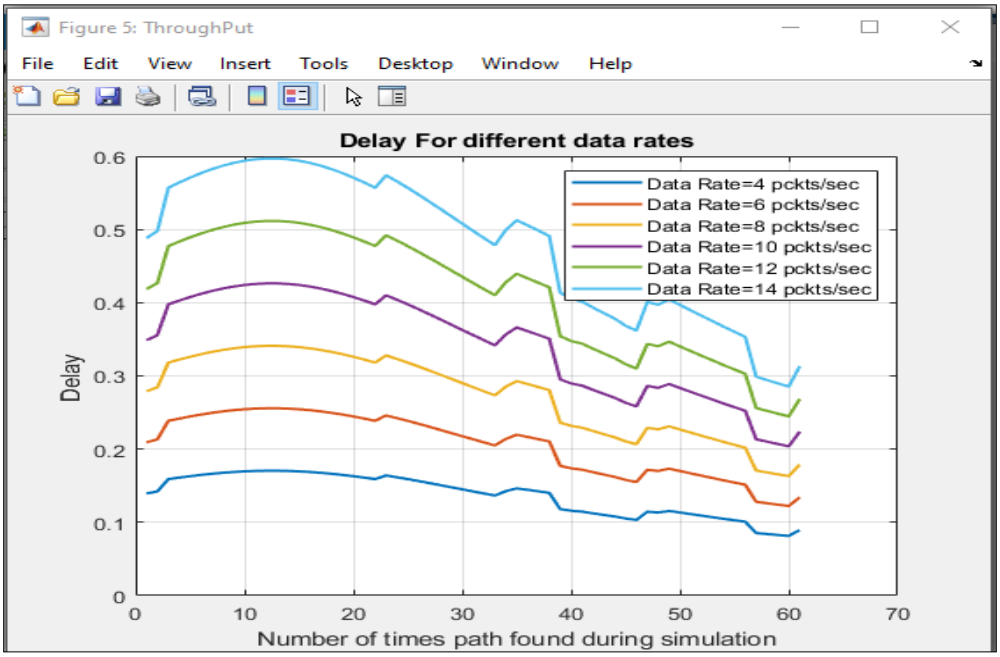

Figure 5 : Delay for Different Data Rates

Source node -> path node-> destination node

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

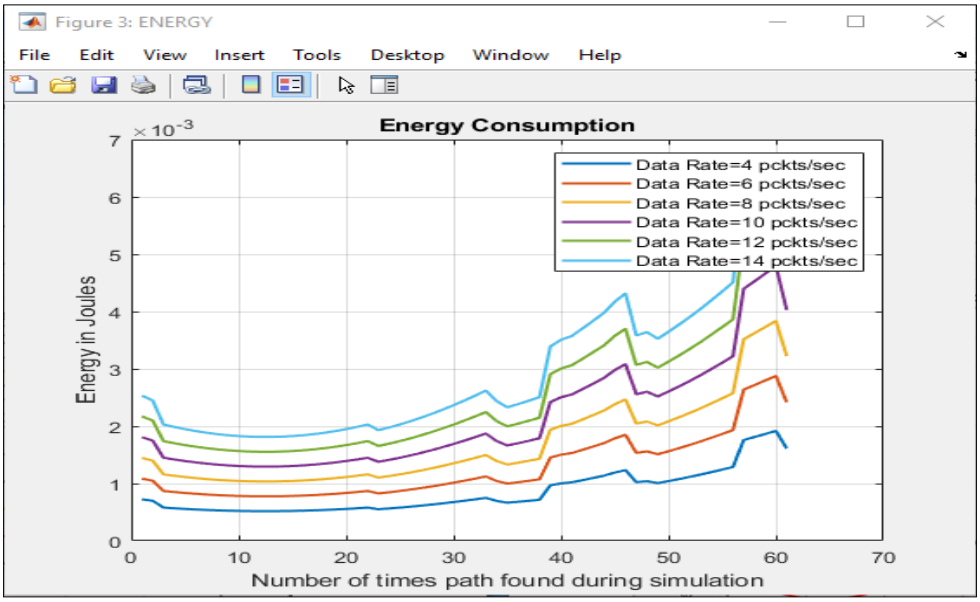

Figure 6 : Energy Consumption for Different Data Rates

The data transmit from source to destination through nearest available nodes the data energy consumption for different data rates transmission through path

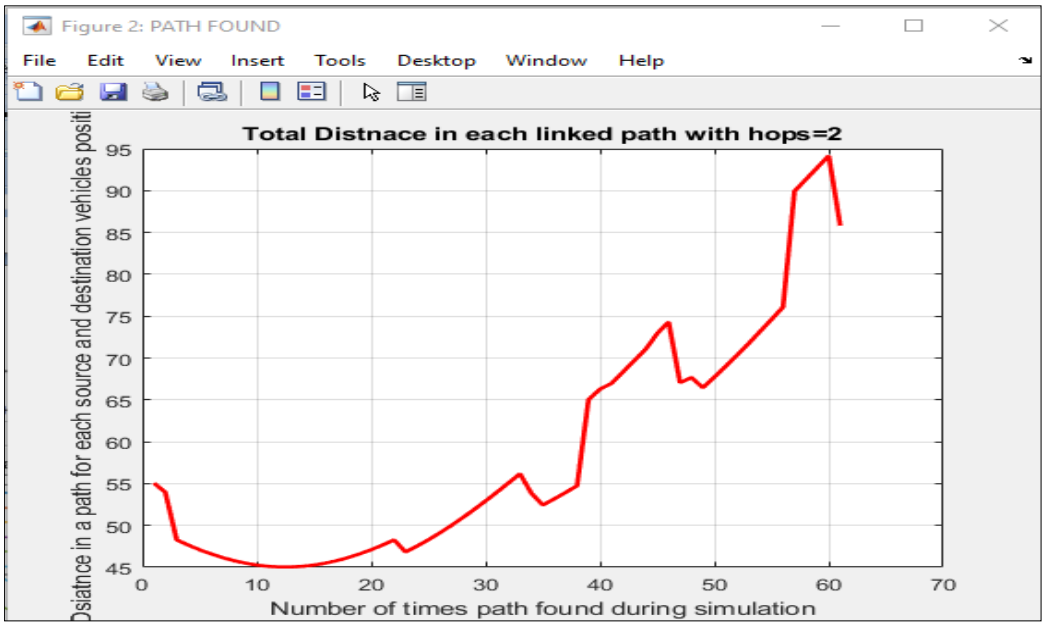

Figure 7 : Number of Path Found During Simulation

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

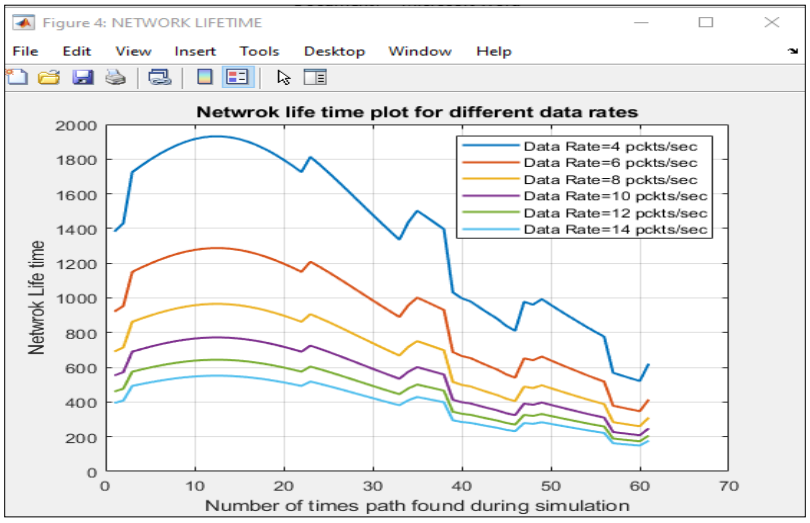

Figure 8 : Network Life Time for Different Data Rates

K-Fold Cross Validation

In this method, the data set is broken up into a certain number of smaller groups, called "folds." After that, each of the subsets is used to prepare the model, however the last subset is utilized to test the modelthat has been trained (k-1). With this method, we will do k iterations, setting aside a different part of the data each time for use in testing. At the point when the K-crease cross-approval strategy is utilized, the dataset is parted into K gatherings of tests that are overall a similar size. Folds is what these examples are called. The expectation capability involves k short one folds for each learning set, saving the other folds for the test set. This is one of the most well-known ways of composing a CV since it is straightforward and delivers less slanted results than different strategies.

The means for k-overlap cross-approval are:

- Part the information dataset into K gatherings
- For each gathering:
- Accept one gathering as the save or test informational collection.
- Utilize remaining gatherings as the

preparation dataset

- Fit the model on the preparation set and assess the exhibition of the model utilizing the test set.

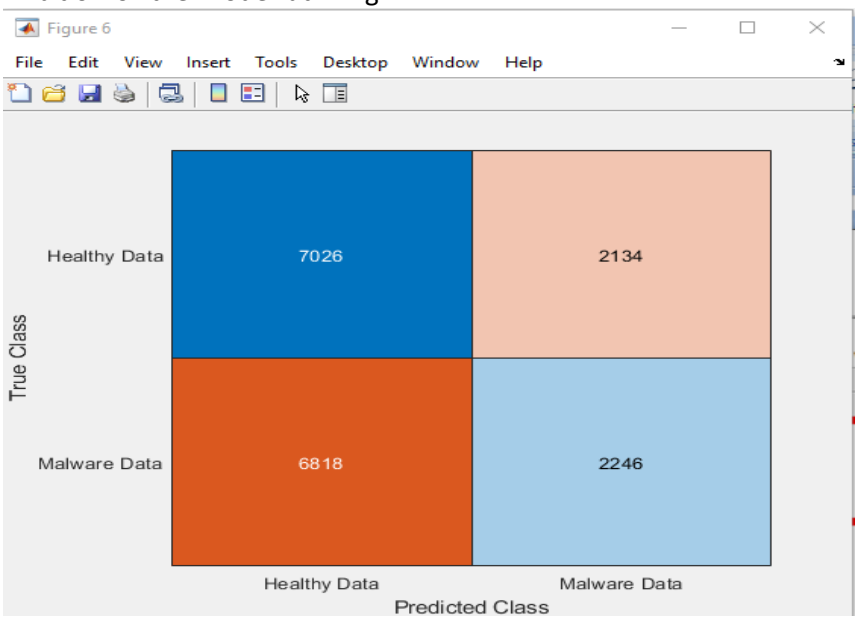

Figure 9 : Test Result Dataset

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 executes the procedure of grouping wherein the entire dataset is partitioned into some particular number of bunches whose bunch head is the centroid of the group hubs. In every one of the cycle, the centroid for a specific bunch refreshes as another hub joins the group. 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.

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

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

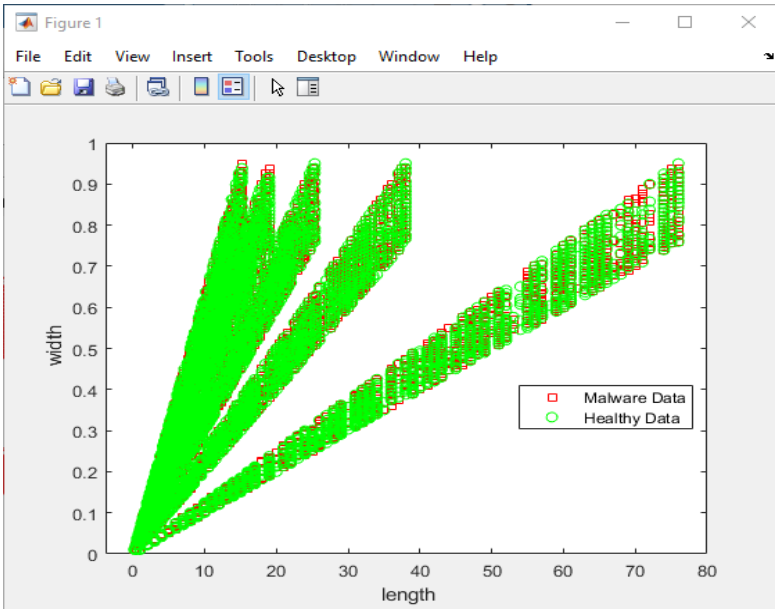

Figure 10 : Traning of Malware and Heathy Data

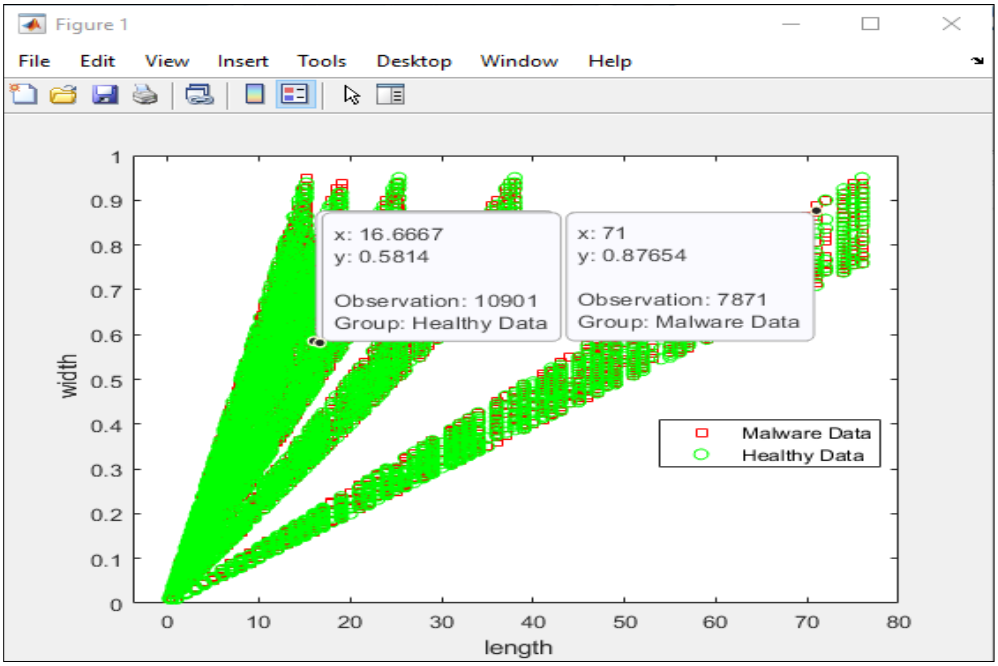

Figure 11 : Obesrvation of Healthy Data and Malware Data

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 be as a proportion of the model's actual fundamental mean exhibition on the dataset, which we don't know.

Table 1 : IoT QOS 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.

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) necessities for network security, the two information security and safeguarding the areas of hubs that send and get information are required.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 mental radio organizations, haze processing, and AI. In the wake of sorting out what the end clients need, specialist organizations can utilize these advances to assemble constant 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. S. Ezdiani and A. Al-Anbuky, "Modelling the integrated QoS for wireless sensor networks with heterogeneous data traffic," Open Journal of Internet of Things (OJIOT), vol. 1, 2015.
2. S. E. S. N. Azlan and A. Al-Anbuky, "Quality of Service Modelling for Federated Wireless Sensor Network Testbed Gateways," in Proc. of 5th Int. Conf. on Commun., Theory, Reliability, and Quality of Service (CTRQ 2012), Chamonix/ Mont Blanc, France, 2012, pp. 14-18.
3. S. Ezdiani, I. S. Acharyya, S. Sivakumar, and A. Al-Anbuky, "An IoT environment for WSN adaptive QoS," in Proc. of IEEE Int. Conf. on Data Science and Data Intensive Systems, 2015, pp. 586-593.
4. S. E. Syed Nor Azlan, I. S. Acharyya, S. Sivakumar, and A. Al-Anbuky, "An architectural concept for sensor cloud QoSaaS testbed," in 6th Workshop on Real World Wireless Sensor Networks (RealWSN 2015), Seoul, Republic of Korea, 2015.
5. S. Ezdiani and A. Al-Anbuky, "Integrating WSN with the Internet: QoS Analysis and modeling for heterogeneous data traffic," presented at the Wireless Telecommunication Symposium (WTS 2014), Washington DC, 2014.

6. S. Ezdiani, A. Indrajit S, S. Sivakumar, and A. Al-Anbuky, "Wireless Sensor Network Softwarization: Towards WSN Adaptive QoS," IEEE Internet of Things Journal, vol. 4, pp. 1517 - 1527, 2017.
7. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey,"Computer Networks, vol. 54, pp. 2787-2805, 2010.
8. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, pp. 1645-1660, 2013.
9. N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, "Combining cloud and sensors in a smart city environment," EURASIP Journal on Wireless Commun. and Networking, vol. 2012, pp. 1-10, 2012.
10. L. Wu, J. Riihijarvi, and P. Mahonen, "A modular wireless sensor network gateway design," in Proc. of Int. Conf. on Commun. and Networking in China (ChinaCom 2007), Shanghai, China, 2007.
11. L. Shu, X. Wu, H. Xu, J. Yang, C. Jinsung, and L. Sungyoung, "Connecting heterogeneous sensor networks with IP based wire/wireless networks," in Proc. of the 4th IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems, 2006 and the 2006 2nd Int. Workshop on Collaborative Computing, Integration, and Assurance (SEUS 2006/WCCIA 2006) p. 6 pp.
12. K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," in Proc. of 2003 Conf. on Applications, Technologies, Architectures and Protocols for Comput. Commun. (SIGCOMM 2003), Karlsruhe, Germany, 2003, pp. 27- 34.
13. P. A. C. d. S. Neves and J. J. P. C. Rodrigues, "Internet Protocol over Wireless Sensor Networks, from Myth to Reality," Journal of Communications, vol. 5, pp. 189-196, March 2010.
14. L. Shu, X. Hui, X. Wu, L. Zhang, C. Jinsung, and L. Sungyoung, "VIP Bridge: Integrating several sensor networks into one virtual sensor network," in Proc. of Int. Conf. on Internet Surveillance and Protection (ICISP '06), Côte d'Azur, France, 2006, pp. 2-2.