Webology (ISSN: 1735-188X)
Volume 18, Number 4, 2021

An Analysis Of Security Issues, Challenges, And Open Problems In The Internet Of Things

Neeraj Jain[1] , Dr. Manish Shrimali[2]

[1]Research Scholar (CS) , Janardan Rai Nagar Rajasthan Vidyapeeth University , Udaipur.

[2]Associate Professor, Department of Computer Science, Janardan Rai Nagar Rajasthan Vidyapeeth University, Udaipur.

ABSTRACT

A 5G wireless sensor network, also known as a WSN, is a network of independent nodes that is used to keep an eye on the surrounding environment. In the context of WSN, energy competence and secure data transmission are considered to be the most important imperative development goals. Because of the growing complexity of workstation networks, there has been an uptick in the number of attacks that are network-based. This has piqued the interest of academics coming from a variety of disciplines. Since the sensor nodes that make up wireless sensor networks (WSNs) are installed in an area that is open and uncontrolled, they are susceptible to a wide variety of different kinds of attacks. An intrusion detection system is able to identify attacks on the network that nodes are subject to. This thesis proposes a Sybil attack-based intrusion detection model of wireless sensor networks (WSNs), which utilizes a combination of improved particle swarm optimization (PSO) and intrusion detection. In addition, because of the need for the necessary physical protection equipment, the data that is transferred through the wireless sensor network (WSN) is susceptible to multiple forms of malicious attack. Because of this, network clustering can increase the lifetime of a network while simultaneously reducing its overall energy usage.

INTRODUCTION

The fifth generation wireless system or 5G is next production of mobile wireless communications that surpasses present 4G/International Mobile Telecommunications (IMT) superior system .The 5G wireless classification is not only a progress of traditional 4G mobile network, but also a organization with several new service features Research or progress of 5G is aimed at different advanced features such as higher capability than modern 4G, superior mobile broadband user density and support of device-to-device (D2D) communication or large machine type communication. The 5G plan also aims to reduce latency and reduce energy expenditure in order to better implement the Internet of Things (IoT) .More specifically, the 5G wireless systems has eight advanced features, 1-10 Gbps connection with field endpoints, 1 millisecond delay, 1000

times the bandwidth per second. Area unit, 10-100 times the number of related units and 99.999% accessibility, 100% coverage, 90% cutback in system energy consumption, The battery life of low power devices is as long as ten years . To meet these performance requirements, different technologies.

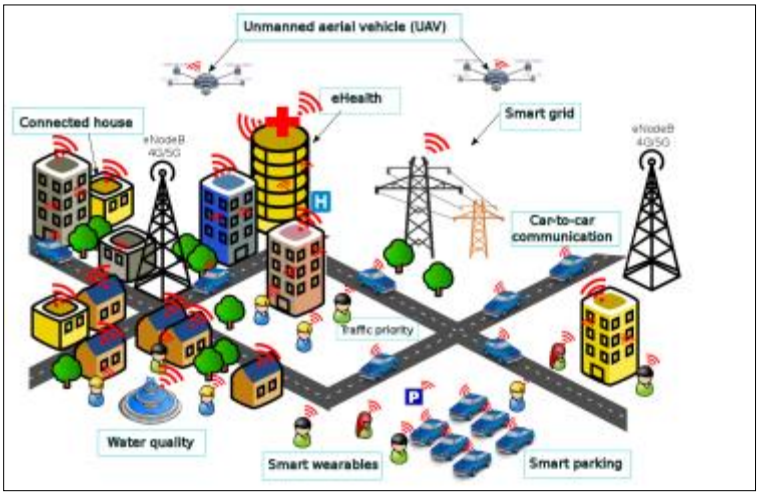

Fig. 1 : 5G wireless networks

The goal of 5G wireless networks is to provide high throughput rates or great coverage by setting up many campsites with more capabilities and better service quality (QoS). And there is not much of a delay. For 5G to be able to offer its core services, it needs new networks, new ways to deploy services, new storage technologies, and more storage space.

Traditional Long Term Evolution (LTE) mobile networks offer users and network operator's high levels of security and reliability [1]. In addition to the user-service authentication that is already in place, a separate authentication can be done between the EU and the base database. A big scale or large key management system [2] also makes sure that LTE access is safe and that traffic is managed. Researchers have also looked into the risks that come with the technology that LTE uses. But for new use cases or ways of thinking to work in new networks, more security measures will need to be put in place.

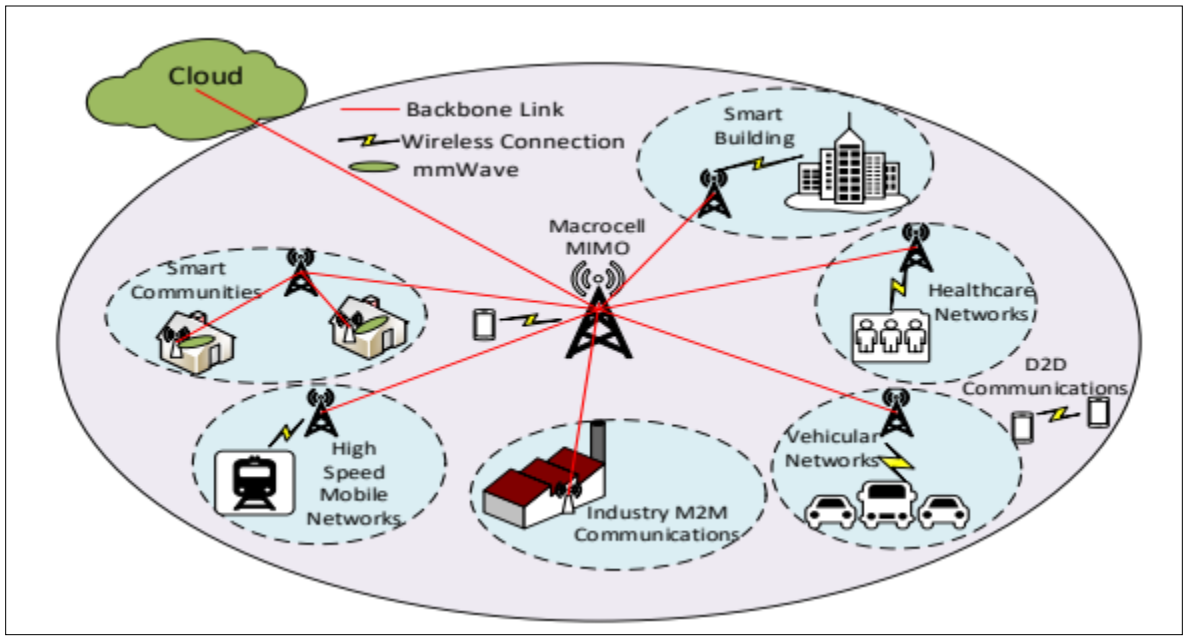

Fig. 2 : A architecture for 5G wireless systems

New usage cases may have special requirements, such as minimum latency for user communication. New knowledge not only produce complex services, but also open doors to loopholes or compel new security measures for 5G [3].In HetNet, different access technologies may have dissimilar security rations[7], or multiple complex environments may require frequent authentication and strict delay limits .Massive MIMO is considered an significant 5G technology to achieve high spectrum efficiency o energy efficiency. It is also considered a precious method to prevent passive control.

RESEARCH METHODOLGY

In this research, a automatic finite deterministic path is proposed to improve the security of 5g wireless sensor networks and energy-saving routing in wireless sensor complex in a secure way. The way research technology is designed can also protect the network from attack[6]. The proposed work combines automatic finite deterministic and particle swarm optimization (PSO) to detect interference or complete data communication in a secure way by influential by the following optimized route in the network[8]. A new automatic finite deterministic pathway is proposed to develop the dynamic character of multipart. In turn, automatic finite deterministic path PSO provides node and data packet, and route inspection information to detect and eliminate unwanted guests from the network and complete data transmission in an effectual energy efficient method through best path. Routing from side to side the best pathway can improve generally management of sensor system and controlled throughout different indicator such as power consumption, capacity, complex life, active nodes and dead nodes. The research method will be to improve the overall system life[5],

Wireless Sensor Networks(WSNs)

Wireless sensor networks (WSNs) are groups of sensors that are spread out across a large area and are made to sense what is going on around them. Usually, a wireless sensor network (WSN) will take readings of the environment's temperature, winds, humidity, sound, pollution levels, and so on, and then store those readings at a central location called the sink or the Base Station (BS) [4].

Network life time

It's a reference to how long the network will be up and running. It is counted from the first time the network was turned on to the last time the last node was shut down.

Clustering inWSNs

In wireless sensor networks (WSNs), "clustering" is the process of dividing the whole network into many smaller sub-networks, each of which has a CH in addition to its individual member nodes. In WSNs, CHs work like the repeaters you see in traditional computer networks. A member node will collect information,[9] which it will then send to its CH. The CH will then send that information to the BS. Clustering the wireless sensor networks (WSNs) may help them last longer by making sure that each cluster uses the same amount of energy.

Implementation Approach

In the proposed architecture, the base station is a trusted part that is supposed to send safe data by setting up a secure link between different types of nodes. In the end, this leads to data that is safe. The nodes that are closest to the base station are in charge of giving it the most respect. Nodes that are farther away from the security hierarchy, which is the beginning of a base station, which is a set of routing choices at startup and during reconfiguration, are easy to spot. Base stations are the first step in making a network safe[10]. The security architecture can send the parts of the relationship between the different types of nodes that are connected to the command/message data, etc. Hierarchical routing and the parts of a base station take care of any kind of authentication. After it has been found, the re-node clustering unfavorable event is triggered when the node is ready to do several things to set up an energy-efficient sensor network. These include:

- rejoining the cluster;
- re-establishing dynamic routing; and
- Restarting the service.
- Changed the sensor's job to work with the safety features.

Some WSN anomalies are called Node anomalies, Network anomalies, Data anomalies, and other anomalies. This is because WSN anomalies can take many different forms. Most problems with WSN networks are caused by connection problems, and there are both increases and decreases in how well signals connect. This is what shows if there is any loss in the network or not. "Node anomalies" refers to any problems with software or hardware that show up in the sensors. The

main reasons for this are problems with the solar panels and the power supply. A lot of the time, data anomalies is caused by data sets that aren't put together well or by inconsistencies caused by problems with sensors or the environment. Other anomalies explain why it doesn't match any of the other kinds of oddities[11]. A new Automatic path search-PSO has been suggested for the framework that has been put forward. This Automatic path search -PSO learns how the network changes over time and controls nodes, data packets, and routes to find the best way. Because of this, unwanted visitors can no longer get in, and data can be sent more efficiently.

Figure 3 shows the proposed system, which makes routing in wireless sensor networks safe and energy-efficient (WSN). Build and run a network with a number of nodes in an area with no obstacles. After all of the nodes have been set up, the cluster will be made.

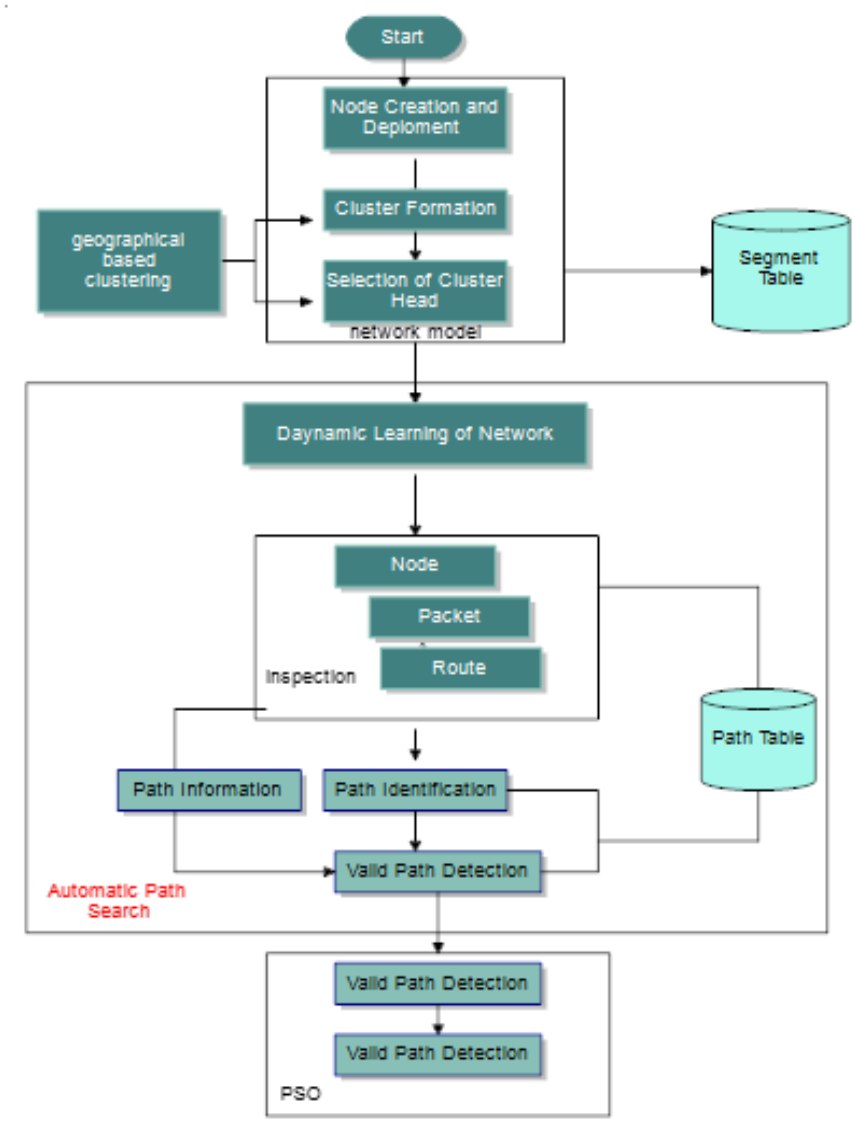

Fig 3: Block Diagram

Network Model

The complex consists of N points spread over an infinite world. Each node has its own characteristics, such as original energy, greatest packet size, message size or threshold, which are allocated as showing in Table 1. The system consists of a network- a base line in which nodes are organized into small assembly called clusters[12]. A key indicator in evaluating the effectiveness of a sensor network is the network life .The full operation of the network creation model is shown in Figure3.

Table1 Simulation parameters of network

Parameters	Value
Sensing region length(meter)	200
Sensing region width (meter)	200
cluster radius(meter)	30
Sensing range (meter)	36
No nodes number of nodes (meter)	100
Packet size in (Bytes)	512
Initial Energy (Eo)	200

Modules:

- System model
- Cluster head selection
- Automatic Path Search and PSO
- Performance analysis

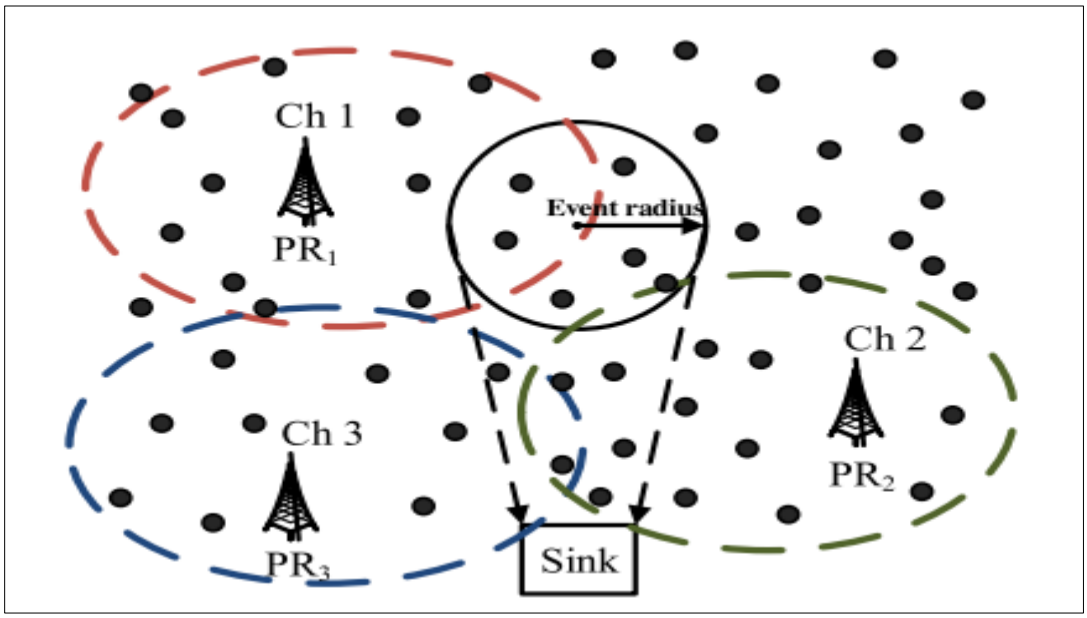

Fig 4 : System model

Simulation and Performance Analysis

The efficiency of the protocol with respect to the interchange of control and data packets, the needs of cluster processes, the communication between clusters, the amount of energy required by clusters, and the rate at which clusters develop as a result of the fact that they are mobile. The results of the simulations indicate that the algorithm has a high degree of efficiency in terms of communication, the amount of energy it uses, and the level of safety it provides.

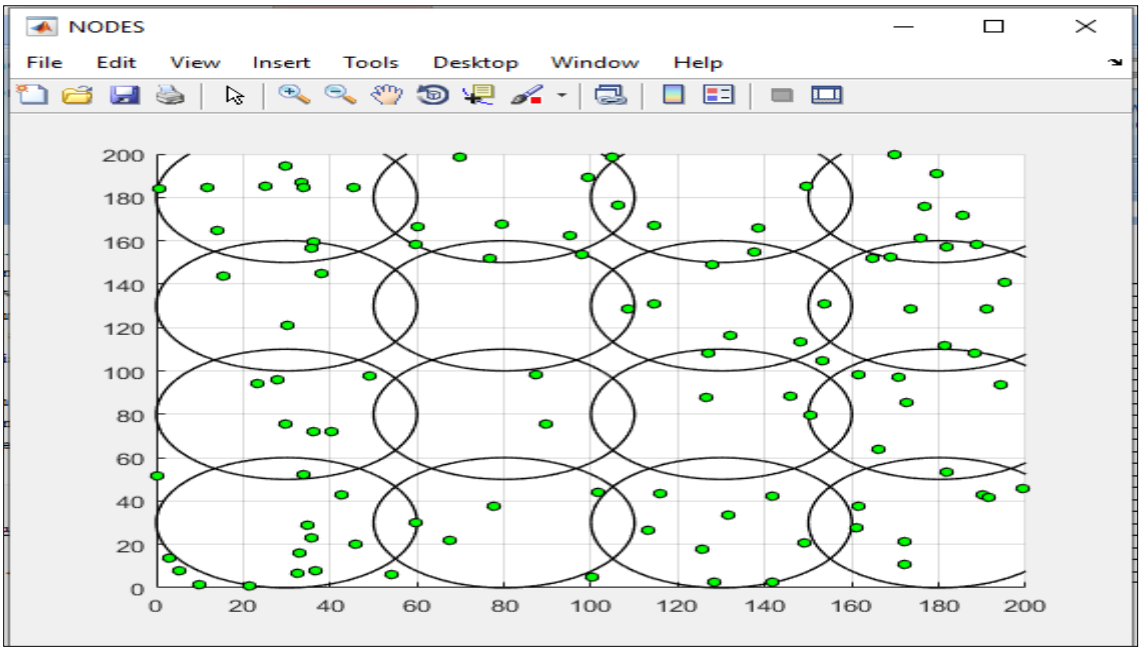

Fig 5: Initial network

First, set up the network that's already there. Then, copy the whole number of nodes. Figure 6 shows the main parts of the network[13]. The length of its area is 200 meters, the width of its sensing area is 200 meters (clusters), its radius is 30 meters, and the distance between feelings is 36 meters.

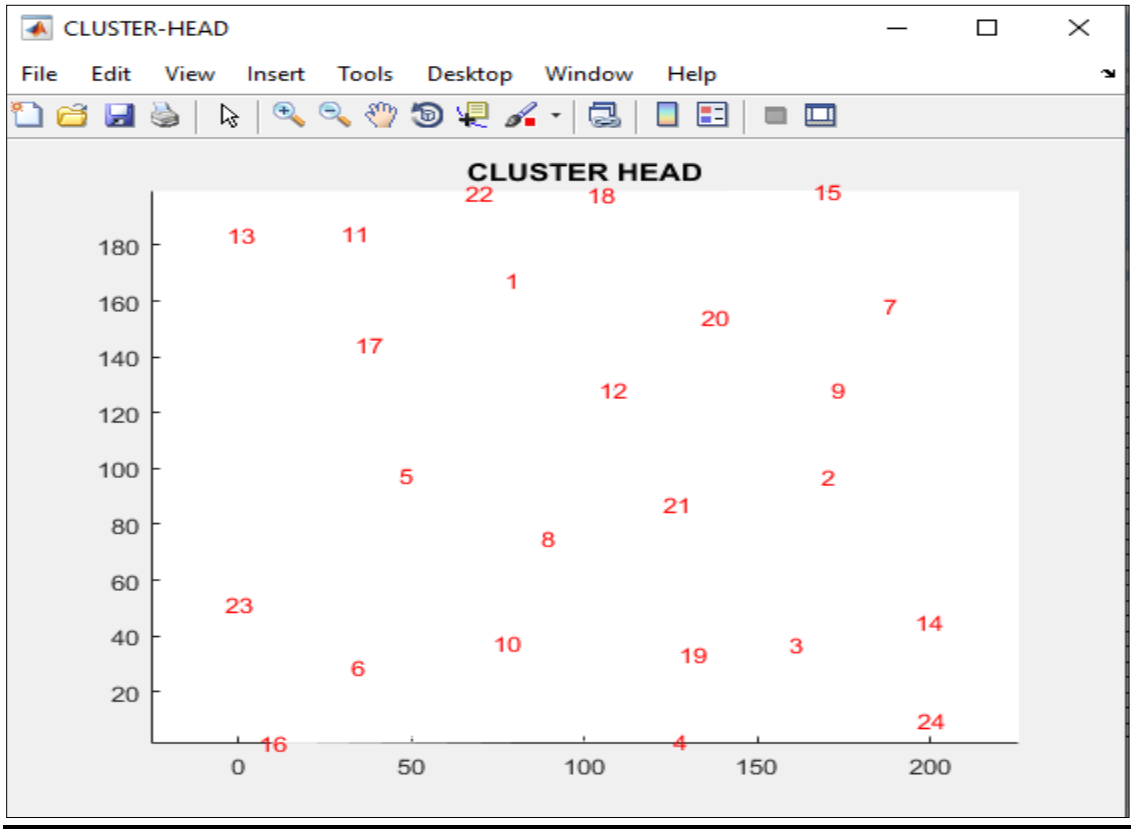

Fig 6 : Number of cluster head

Figure 6 Clustering is one of the most important methods that may be used to increase the lifetime of wireless sensor networks. This can be accomplished in a number of different ways (WSNs). The process involves assembling clusters out of individual sensor nodes and choosing cluster heads, also known as CHs, for each of the assembled clusters[14].

A connecting point inside a communications network is referred to as a network node. Every node in the network functions as an endpoint for the transmission or redistribution of data. The transmission of data from one node in a network to the subsequent node is known as node-to-node data transfer.

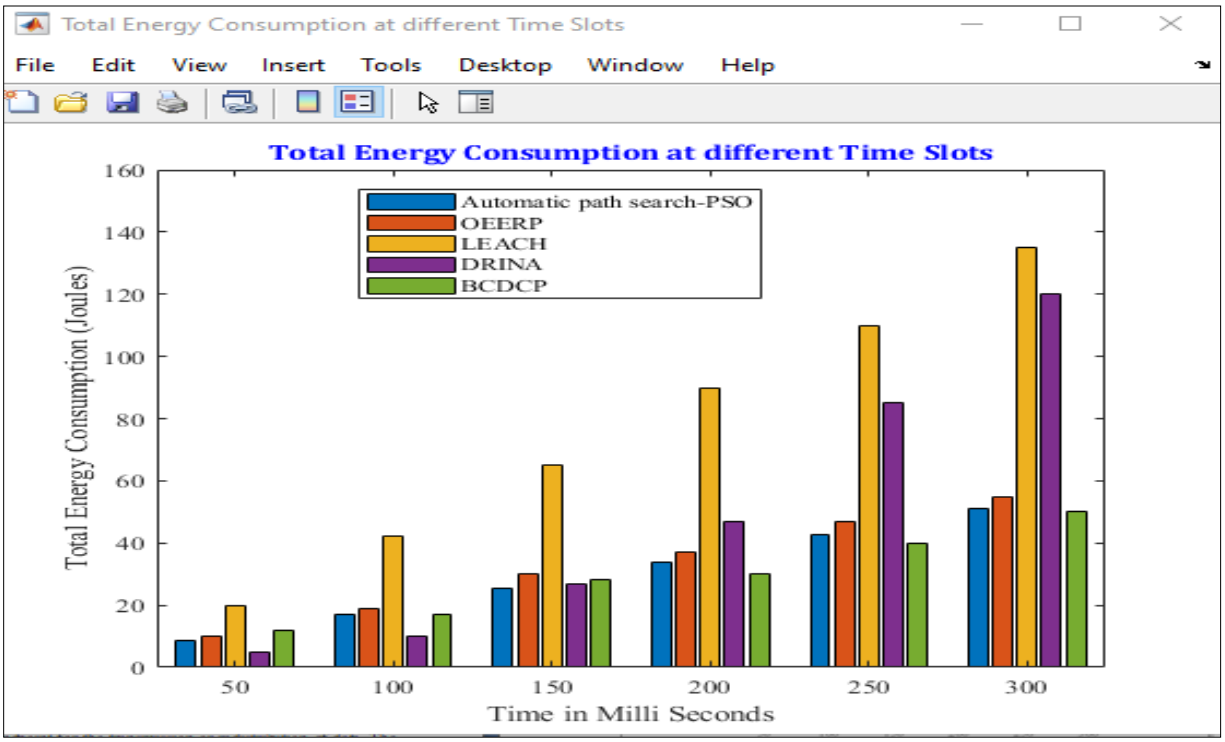

Fig 7: Total energy consumption at different time slot

Conclusion

WSNs are being used in every part of human life, and this has led to the creation of a lot of new protocols. These protocols try to cut down on the amount of energy used while also making the network work better. The performance of the network takes into account many things, such as the maximum PDR, the least amount of energy used, and the least amount of delay. To do this task, autonomous path search methods will need to be made to find the cluster head and the best secure path. As a way to find the best route for secure routing[15], a PSO technique for optimal cluster head selection was put forward. The suggested automatic path search simulation results are compared with OEERP, DRINA, and LEACH, BCDCP.

the plan being thought up Cluster head selection is one of the things that need to be thought about because it is so important for keeping the energy needs of the network's nodes in a healthy balance. Because choosing cluster heads often causes an energy imbalance and shortens the life of a network, this is another problem that needs a lot of attention. The work that has been proposed solves these problems by using two algorithms, automated path and PSO, for energy-efficient selection of cluster heads and optimal selection of paths, respectively.

REFERENCES

1. N. Panwar, S. Sharma and A. K. Singh, “A Suvery on 5G: The Next Generation of Mobile Communication”, Physical Communication, vol. 18, no. 2, pp. 64-84, 2016.
2. “5G Vision”, 5G PPP, February, 2015.
3. “NGMN 5G WHITE PAPER”, NGMN Alliance, February, 2015.
4. G. Andrews et al., “What Will 5G Be?”, IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1065-1082, 2014.
5. “Understanding 5G: Perspectives on future technological advancements in mobile”, GSMA Intelligence, December, 2014.
6. M. Agiwal, A. Roy and N. Saxena, “Next Generation 5G Wireless Networks: A Comprehensive Survey”, IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617-1655, 2016.
7. Qiao, X. S. Shen, J. W. Mark, Q. Shen, Y. He, and L. Lei, “Enabling Device-to-Device Communications in Millimeter-Wave 5G Cellular Networks”, IEEE Communications Magazine, vol. 53, no. 1, pp. 209-215, 2015.
8. Wei, R. Q. Hu, Y. Qian, and G. Wu, “Energy Efficiency and Spectrum Efficiency of Multihop Device-to-Device Communications Underlaying Cellular Networks”, IEEE Transactions on Vehicular Technology, vol. 65, no. 1, pp. 367-380, 2016.
9. Dabbagn, B. Hu, M. Guizani, and A. Rayes, “Software-Defined Networking Security: Pros and Cons”, IEEE Communications, vol. 53, no. 6, pp. 73-79, 2015.
10. J. Zhang, W. Xie, and F. Yang, “An Architecture for 5G Mobile Network based on SDN and NFV”, 6th International Conference on Wireless, Mobile and Multi-Media (ICWMMN2015), 2015, pp. 87-92.
11. “5G security recommendations package #2: network slicing”, NGMN Alliance, April, 2016.
12. “5G SECURITY”, ERICSSON WHITE PAPER, June, 2015.
13. “The Road to 5G: Drivers, Applications, Requirements and Technical Development”, GSA, November, 2015.
14. Shailesh Pramod Bendale;Jayashree Rajesh Prasad Security Threats and Challenges in Future Mobile Wireless Networks 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN) Year: 2018 DOI: 10.1109/ IEEE Lonavala, India
15. Mehmet Alp Ilgaz;Bostjan Batagelj Application of an Opto-Electronic Oscillator in 5G Mobile and Wireless Networks with a Low Frequency Drift, a High Side-Modes-Suppression Ratio and without a Power Penalty due to Chromatic Dispersion 2018 European Conference on Networks and Communications (EuCNC) Year: 2018