International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 4, July-Aug-2021, ISSN (Online): 2395-566X

PSO and Automatic Finite Deterministic Algorithm for Secured Energy Efficient Routing in Wireless Sensor Network

M.Tech. Scholar Diksha Jharbade, Prof. Amit Shrivastav
Dept. Electronics and Communication Engineering,
VNS College of Engineering,
Bhopal (M.P.)
Diksha11.04.1994@gmail.com, vnsit.amit@gmail.com

***Abstract*- 5G wireless sensor network (WSN) is a network of autonomous nodes used to monitor the environment. Energy competence or secure data transmission are measured as mainly imperative devise goals for WSN. With the increase in difficulty of workstation networks, the increase in network-based attacks has attracted consideration of different researchers from several fields. Therefore, many intrusion detection systems (IDS) have been implemented to address various aspects of complex safety, such as DoS, worms, viruses, malware, etc. IDS automation has been planned to recover realization of energy resourceful routing in wireless sensor networks in a secure manner. Automatic finite deterministic and particle swarm optimization (PSO) solutions for intrusion detection and data transmission performed in a secure manner by determining and following an optimized path Routing through the best path can recover overall presentation of sensor network in wireless technology and has been controlled through various indicators (such as power expenditure, capacity, network life, active nodes and dead nodes). In this work, threat model and safety objectives for secure routing in wireless network. This simulation executed in MATLAB simulation platform.**

***Keywords*- PSO, wireless sensor network (WSN), intrusion detection systems, Sybil attack, Automatic Intrusion Detection AFD.**

I. INTRODUCTION

The vision of 5G wireless networks is to provide high throughput rates and high coverage by setting up multiple campsites, with increased capabilities, quality of service (QoS).and the latency is low.

In order to provide the essential services of 5G, new networks, service deployments, storage technologies and storage are needed. Cloud computing provides an efficient way for businesses to maintain data, services and applications without needing to have infrastructure for that purpose. Therefore, the mobile cloud using this concept will also bring a unique technology system into a platform to deploy multiple services, thereby reaching higher with less cost (CapEx) and Operating Expenses (OpEx) Compatibility and efficiency. Simplifying network performance will make communication and service system capabilities easier and more flexible.

Software -defined networks (SDNs) realize the flexibility of network operations by separating the control plane and the data forwarding plane. SDN brings network innovation through abstraction on the one hand and simplifies network management on the other. Network virtualization (NFV) provides the basis for deploying various network functions on different network perimeters as needed, and eliminates the need for specific equipment or services specific to the service [1].

SDN and NFV complement each other, improving network capabilities, simplifying network monitoring and management and breaking down barriers to vendor-specific managed solutions. However, with these new technologies and concepts, network security and user privacy remain major challenges facing future networks. From the very beginning, wireless communication systems have been vulnerable to security.

In wireless (1G) networks, the purpose of mobile phones and wireless channels is to colonize and hide illegally. In non -second -generation (2G) networks, spam is not only a common attack, but it has also become common to insert false information or spread unnecessary marketing information.

In third-generation wireless (3G) networks, IP-based communication supports the migration of Internet vulnerabilities and challenges to wireless platforms. As the need for IP-based connectivity continues to grow, fourth-generation (4G) telecommunications networks will enable smart devices, multimedia traffic and new services to evolve rapidly in the mobile sector. This development has led to a more complex and dynamic threat. With the availability of the fifth group's wireless (5G) network, the security risk area will be larger than before, and more privacy will be provided.

Due to the nature of transmission and unlimited communication channels, it can be difficult to provide security features such as authentication, authenticity and confidentiality. In today's mobile networks, there are various security issues in the areas of media access control (MAC) and physical layer (PHY), within that is the potential for attacks, vulnerabilities, and privacy issues. Voice and data protection is provided based on traditional security architecture, with security functions such as user data management, network authentication and user devices (EU) and the protection of the communication channel. In traditional Long Term Evolution (LTE) mobile networks it provides high levels of security and reliability for users and network operators.

In addition to user -service authentication, different authentication can also be applied between the EU and the base database. In addition, the protection of LTE access and traffic management is ensured by a large scale and a large key management system. The safety associated with the technology applied to LTE has also been examined however, new security measures are needed to support new use cases and paradigms in new networks [2-5].

1. Sybil Attack:

The Sybil attack was first proposed by John R. Douceur when examining the security of the neighbors' networks [6], and later Karlof and Wagner showed that this type of attack posed a threat to navigation method in the WSN [7]. Sybil is a chemical attack in which a malicious node pretends to be a group of nodes by claiming false information or creating a new signal in the worst case scenario.

Such an attack can be easily carried out in a WSN environment because the node will always be deployed in an unorganized and distributed environment and can communicate via radio transmission. They are particularly damaging to applications such as data collection, polling systems, reputation assessment and geographic processes. By using Sybil's attack by going to detect a location, multiple locations can be found at one time.

II. LITERATURE SURVEY

The advanced features of the 5G mobile wireless networking system pose new security requirements and challenges. Compared to the traditional mobile network, this article conducts a comprehensive study of the security of the 5G wireless networking system. This research work first reviews the characteristics of 5G wireless networks and the new requirements and motives for 5G wireless securities. It then summarizes potential attacks and security services considering new service requirements and new use cases in 5G wireless networks. Based on similar security services, including identity verification, availability, data confidentiality, key management and confidentiality, the latest developments and existing solutions for 5G wireless securities are introduced. This article further discusses new security features related to various technologies used for 5G, such as heterogeneous networks, device-to-device communications, large scale multiple input multiple output, software defined network and the Internet of Things. Motivated by these security research and development activities,

Wang Haiming et al. (2019) millimeter wave communication (mm Wave) will be used in fifth generation (5G) mobile communication systems, but they suffer from severe course loss and high sensitivity to physical objects, resulting in smaller cell radius and complexity network architecture. A coverage expansion plan using a large-scale antenna array (LSAA) has been proposed, and the combination with an ultra-dense small cellular network has theoretically been shown to be cost effective.

To analyze and optimize network implementation based on LSAA, the latest developments in statistical millimeter-wave channel modeling are examined first for channel parameter estimation, large-scale loss model and small cluster model. Then, the measurement and modeling of two 5G candidate millimeter wave bands (e.g., 28 GHz and 39 GHz) in several interesting outdoor scenes are reviewed and compared and compared. In these scenes, proliferation characteristics have an impact on wireless Network design has made an important contribution. Finally, the coverage behavior of a system is discussed using a large number of antenna arrays and some influences on the design of future mm Wave cellular networks [8].

Xi Zhang et.al (2018) As an important step towards the next generation of ultra-high speed wireless networks, fifth generation (5G) mobile wireless networks have recently received a lot of research attention and efforts from academia and industry. It is expected that 5G mobile wireless networks will provide unparalleled delay limited quality of service (QoS) guarantees for various multimedia services, applications and users with very different requirements.

However, how to effectively support multimedia services on 5G wireless networks has brought many new challenging issues that are unprecedented in fourth generation wireless networks. To overcome these new challenges, we propose a new network function-based virtualization and software-defined network architecture (SDN) based on mobile traffic reading for heterogeneous statistical QoS settings through 5G multimedia wireless networks. Specifically, we have developed a new SDN architecture that scalable virtualizes wireless resources and physical infrastructure to three types of virtual wireless networks according to user location and request: virtual network without load, virtual network with WiFi load Network and device-to-device virtual network device reading.

We derive the best transmission power allocation plan to maximize the total efficient capacity, the total spectrum efficiency and other related performance for these three types of virtual wireless networks. We also deduced scalability improvements from the three integrated virtual networks we proposed. Finally, we verify and evaluate the solution we developed through numerical analysis, which shows a significant performance improvement compared to other existing solutions [9].

Joonyoung Kim et al. (2020) we demonstrated that 4 × 4 Multiple Input Multiple Output (MIMO) based on Distributed Antenna System (DAS) supports mmWave-based indoor 5G mobile network which has a wireless interface to receive remote control from mobile front band wireless signal from the radio head (RRH). To achieve a cost-effective/ bandwidth-efficient indoor 5G DAS network with low latency, we have developed a radio-over-optical fiber (RoF) system based on IFoF (medium frequency optical fiber) technology.

More specifically, we use both wavelength multiplexing and frequency division multiplexing in the IFoF link to transmit 4 × 4 MIMO 5G signals with a bandwidth efficiently 3.2 GHz (= 4 × 800 MHz, where each antenna 800 MHz 5G signal). The error vector size performance (EVM) of the IFoF link supporting 4 × 4 MIMO is <; on all channels in downlink and uplink the maximum transmission speed of 2 km is 4.5%.

The entire RoF system uses IFoF links, mmWave frequency conversion modules and control / management plans to prove that it can meet the EVM requirements defined by 3GPP (ie 8%) on all channels. Based on the RoF system, we combined KT's 5G mobile network (ie 5G baseband device and RRH) to demonstrate the indoor 5G DAS network and studied the throughput of downlink and uplink. We have achieved a total throughput of approx. 4 Gb / s for the end user, where the extra latency caused by the DAS network is only a few hundred nanoseconds in addition to the transmission delay of the single-mode fiber [10].

III. PROPOSED WORK

In the proposed framework, a new AFD-PSO is proposed, which learns the dynamic properties of the network and achieves the best way by controlling nodes, data packets and routes, thereby eliminating uninvited guests and efficiently transmitting data. The proposed framework is illustrated in Figure 1, which provides secure energy efficient routing in WSN. Create and implement a network of a set of nodes in an unobstructed environment. Once the nodes are implemented, the cluster is formed. The cluster is formed geographically.

Geographically based cluster formation is based on equal distribution of spatial regions. In the proposed method, a cluster is formed in three levels, i.e. the regional space is divided into three equal parts. All sensor nodes in the cluster may only communicate with the cluster head. The cluster head information and path information are updated in the segment table along with the energy in each node and the distance between each node.

Automata Finite Deterministic AFD dynamically learns all nodes, routing and packet information and regularly updates the information on each node in the stack table. When a data packet is to be sent from the source node to the destination node, AFD gets the available path from the source node to the destination node. AFD verifies these paths and updates the valid paths in the pin table.

The AFD-PSO algorithm analyzes the pin table and checks nodes, data packets and routing information, thereby eliminating unwanted attacks or uninvited guests, such as selective forwarding and Sybil attacks available on the network. AFD and PSO combine to achieve the best path. Once the best route is achieved, the data packet is transferred from the source to the destination in a safe and efficient manner.

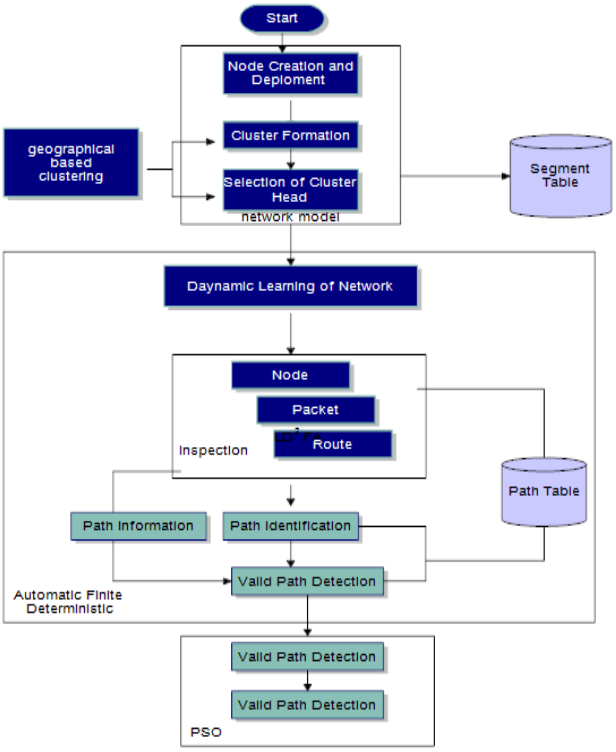


Fig 1. Proposed Framework.

IV. SIMULATION RESULTS

The effectiveness of the protocol in terms of control and data packet exchange, cluster process requirements, cluster communication, cluster energy consumption, and clustering rate Because of mobility. The simulations show that the algorithm has good efficiency in terms of communication and energy consumption and security.

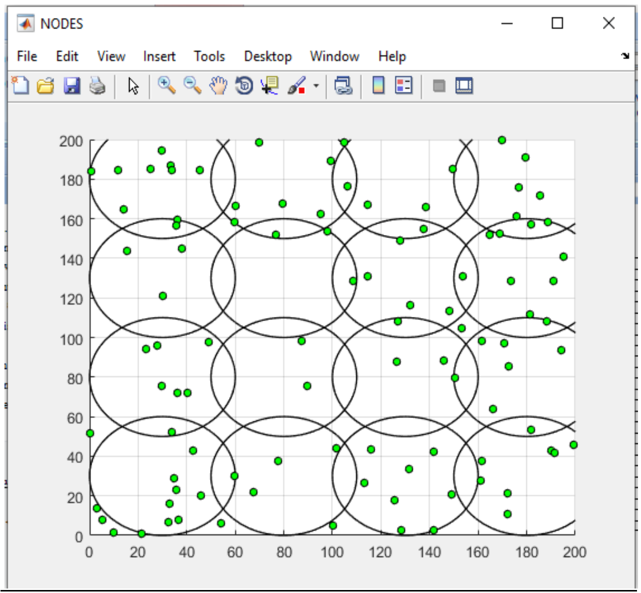


Fig 2. Initial Network.

Configure the original network and paste the number of nodes Figure 3.1 shows the initial network, the length of its area = 200 (meters), the Sensing_region_width = 200 meters (clusters), the radius = 30 (meters), and the distance of sensation = 36

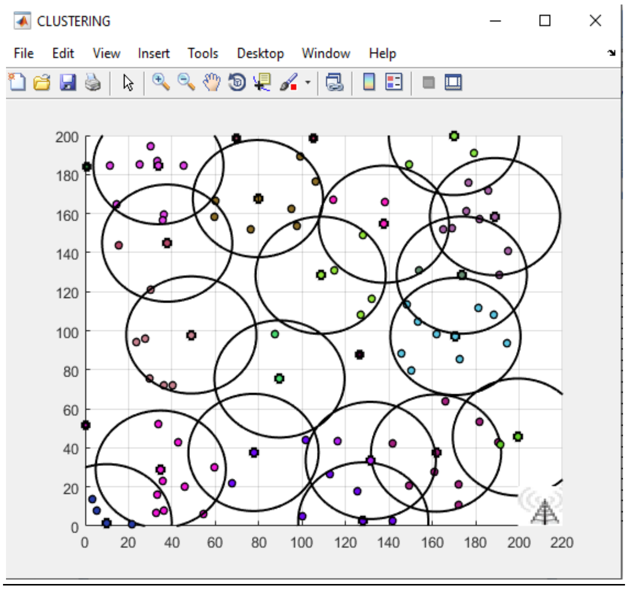


Fig 3. Cluster Head.

The WSN divides each cluster, and each cluster has an administrator (cluster head), who is responsible for collecting data from the node and sending it to the receiver (base station).

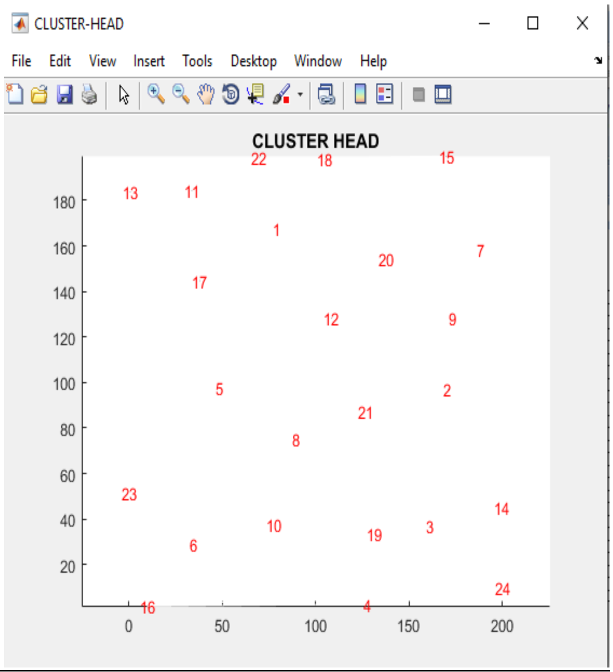


Fig 4 Number of Cluster Head.

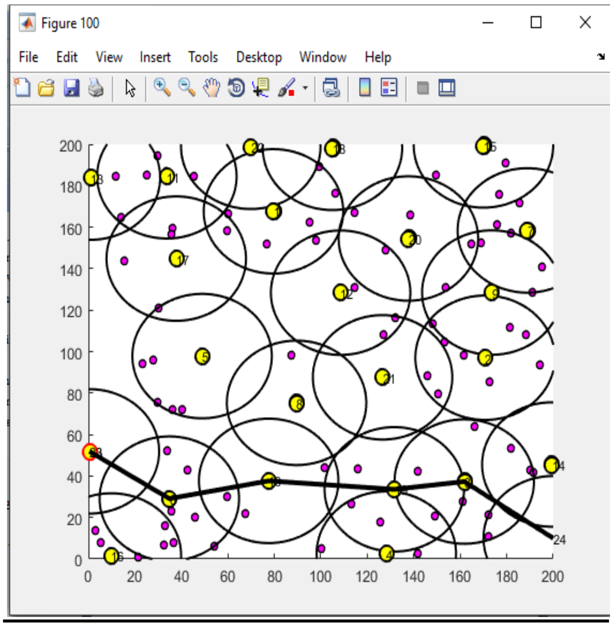


Fig 5. Node Finds The Optimum Path In The Network.

The sensors are usually deployed to meet coverage requirements, which allow certain points to enter sleep mode, thus storing a large amount of energy. The cluster head can be selected randomly or depending on one or more criteria. The choice of the cluster head affects the lifespan of the WSN in a large way. The most suitable cluster head is the cluster head with the highest power, the number of neighboring nodes and the minimum distance from the base station.

Figure 3.2 shows the head numbers of the various clusters in the network. The WSN divides each cluster, and each cluster has an administrator (cluster head) responsible for collecting data from the node and sending it to the receiver (base station).

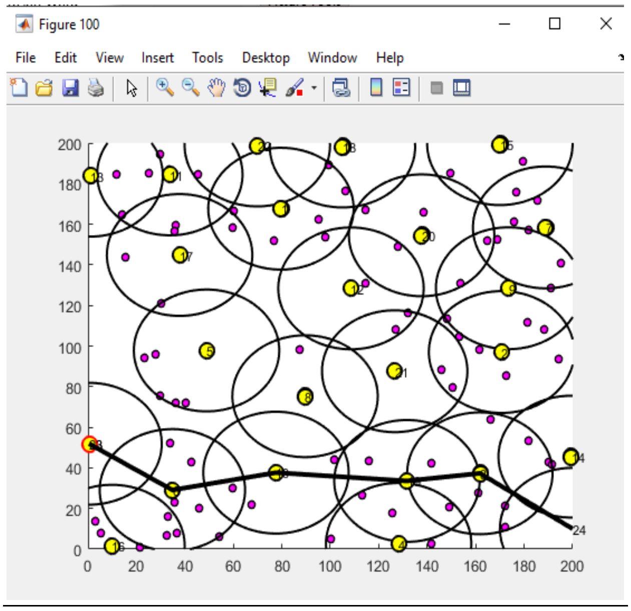


Fig 6. Node Searching Path in the Network to Secure Communication.

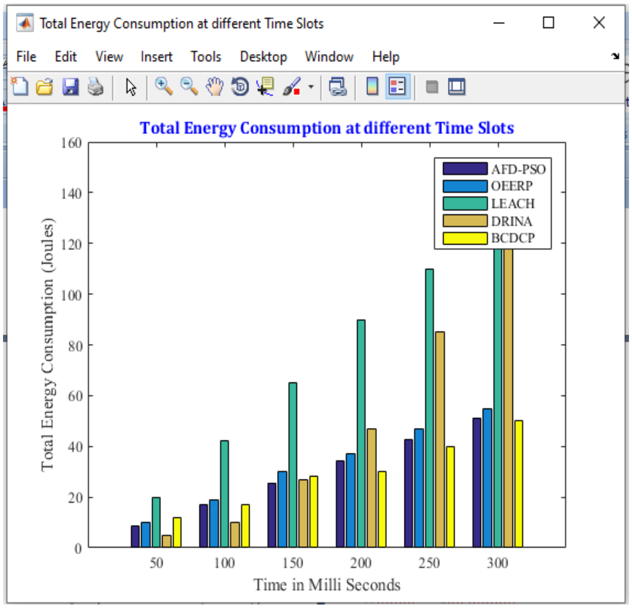


Fig 7 Total Energy Consumption at different time slot.

The proposed AFD-PSO consumes more energy than the existing system. This is because the sensor nodes do not consume energy when they are assigned to a cluster close to them, while the AFD-PSO detects malicious nodes, the energy consumed by malicious nodes.

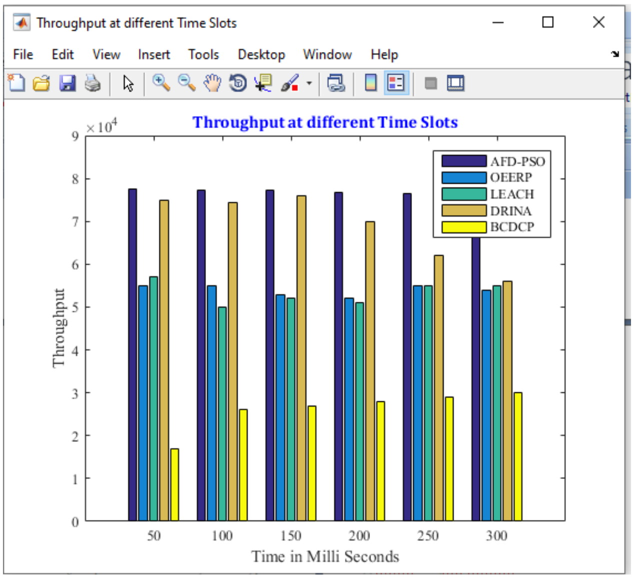


Fig 8. Throughput at different time slot.

Compared to other methods such as OEERP, LEACH, DRINA,BCDCP the AFD-PSO proposed method show higher accuracy as compare to other compared to other techniques

.

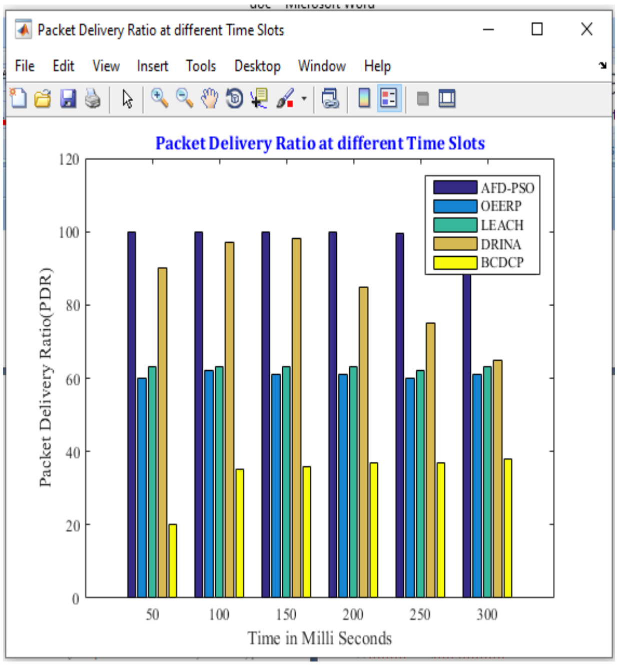


Fig 9. Packet Delivery ratio at different time slot.

However, the application of automatic finite deterministic to multifaceted dynamic problems is a difficult task. The most important function of the routing is to define the pathway among the networks and perform the transmission of secure in sequence packets along the pathway from the source node to the target node. In this work, an automated automatic finite deterministic simulation method was developed and applied along with the particle improvement method.

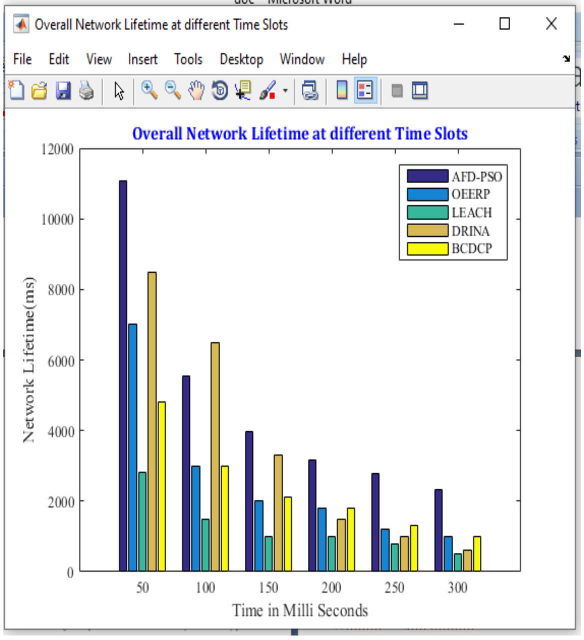
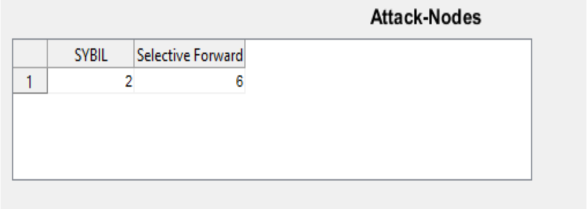


Fig 10. Network Life time at different time slot.

In this work, an AFD simulation method was developed and applied along with the particle improvement method. Fig network life time at different round.

Table 1. Cluster Head Path in the network.



Attack-Nodes

	SYBIL	Selective Forward
1	2	6

AFD-PSO immediately detects and blocks various contaminants found in the system. Designed for illustration, a node scan assist determine if the node is malware. Sybil nodes can use duplicate IDs to work, where the distribution table made to recognize duplicate node IDs. By studying all the possible paths, the best path can be determined.

Based on the ID, a selective forward attack can be identified. Comparing the data transmission paths can detect and eliminate Sybil and selective advanced attacks. Finally, by analyzing the data packets, retrieving the data packets, importing data and routing the flow, unusual data packets can be recognized and detect.Therefore, by integrating node analysis, analysis process and data packet analysis, AFD combined with PSO can work as the finest routine IDS for secure, seamless navigation in energy, efficient and optimized with WSN.

Discriminating forward attack the most common attack on a network layer is a selective forward attack. The node maintains the consistency aspect all through communication. In this attack, the intruder treats some node as a sensor node in the network. These mistrustful points will drop packets past them and send only selected packets to the subsequently sensor node.

The partition table stores current node in sequence, each time the path is found, the source node, medium node and target node information are updated in the table. Each time the AFD and PSO study the distribution table and update the table with values such as path, interdependent node, and node status, the distribution table is verified each time a path is found. If the status of the node is in the path, the AFD detection will find the best path for the network segment, and if the automaton has a target node, the automaton is accepted.

By allowing the AFD process to detect this automaton will periodically check from the distribution table whether the AFD distribution is or not, whether it is a dead point or a dangerous point for each education, and update the access. If a dirty dot or dead dot is found, it will update the message in the section table. If the dirty point and deceased point be specified as 1 in the distribution table, the path with the corresponding node will be discarded and updated in the path table.

Table 2. Comparison with Existing Work.

	Through Put (%)	Energy Consump tion E/J	Packet Delivery (%)	Network Life (Ms)
Existing Work	80(%)	450 E/J	60(%)	400(Ms)
Proposed Work	85(%)	150 E/J	100(%)	2000 (Ms) At Last Node

V. CONCLUSION

The main goal of this work is to dynamically understand network information by monitoring nodes, data packets and routes to eliminate uninvited guests and thereby complete data transmission and improve the network's energy efficiency. The proposed work combines the extended features of finite automata by preparing automata to learn according to established rules and patterns. The proposed AFD-PSO is used to determine the validity of all paths.

In addition, PSO is used for inspection and evaluation by optimizing the path. Remove uninvited guests using the information provided by the network model and the LD2F-PSO model. Several indicators are considered when measuring performance, such as throughput, network life, power consumption, and active node statistics.

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] “5G Security”, Ericsson White Paper, June, 2015.
[5] “The Road to 5G: Drivers, Applications, Requirements and Technical Development”, GSA, November, 2015.
[6] 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.
[7] 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.
[8] Haiming Wang;Peize Zhang;Jing Li;Xiaohu You Radio propagation and wireless coverage of LSAA-based 5G millimeter-wave mobile communication systems China Communications Year: 2019.
[9] Xi Zhang; Qixuan Zhu Scalable Virtualization and Offloading-Based Software-Defined Architecture for Heterogeneous Statistical QoS Provisioning Over 5G Multimedia Mobile Wireless Networks IEEE Journal on Selected Areas in Communications Year: 2019.
[10] Joonyoung Kim; Minkyu Sung; Seung-Hyun Cho; Young-Jun Won; Byoung-Chul Lim; Sung-Yeop Pyun; Joon-Ki Lee; Jong Hyun Lee MIMO-Supporting Radio-Over-Fiber System and its Application in mmWave-Based Indoor 5G Mobile Network Journal of Lightwave Technology Year: 2020.