Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778320

THE METHOD USED TO IDENTIFY AND EVADE DOS ATTACKS IN WSNS

Oshin Sharma
Department of CSE , SRMIST Delhi -NCR Campus, Modinagar, Ghaziabad, UP

Abstract - A few of the many uses for wireless sensor networks (WSNs) include the military, the medical industry, the monitoring of the ocean and animals, the functioning of manufacturing machinery, the safety of structures, and even the detection of earthquakes. WSNs are more prone to intrusion than wired networks because of their complexity and upkeep requirements. Each node has a limited number of resources it can use, including electricity, random access memory (RAM), and a central processing unit (CPU). Developing a quick and dependable security protocol is crucial to thwarting attacks on WSNs, particularly Denial-of-Service (DoS) attacks. However, suppose an attacker sends many phone signals or retransmits signals that have already been sent. In that case, they may be able to take control of some sensors and launch a DoS assault. If it were severed by a DoS attack, whether purposefully or unintentionally, the quantity of bandwidth available for wireless communications would be significantly decreased. The network is hampered by this, which increases the likelihood of a crash. The procedures described, including message observation and shared key authentication, enable the cluster head (CH) and other sensor nodes in the network to now assess whether the communicating node is an attacker node or not. This method enables the quick identification and mitigation of the source of DoS attacks.

Keywords – Cluster Head (CH), Denial of Service (DoS), Wireless Sensor Network (WSN), Sensor Network (SN), One-Way Hash Chain

1. Introduction

The environment is monitored by wireless sensor networks (WSNs) for physical and chemical changes, disaster areas, and weather. WSNs are viewed as a self-organized network of affordable, energy-efficient, intelligent sensor nodes [1]. The sensor nodes are used in a wide range of essential sensing applications because they are small, light, and furnished with processing and communication boards. WSN nodes that collect data. The main duties are measurement, analysis, and user communication via a sink. The user communicates with the sink online or through a satellite. Wireless networks are more susceptible to attacks than cable ones, and these attacks could be purposeful or unintentional [2]. Wireless networks are often set up ad hoc and unplanned, and wireless sensor networks have constrained resources per node (such as electricity, computer power, and storage space). Denial-of-service (DoS) assaults are the simplest attacks because they break any reliable connections. However, by sending out a barrage of phone or duplicate signals, the attackers can seize control of some sensors and launch the DoS assault. DoS attack aims to deny authorized users access to a network-based service or resource. The numerous security holes in wireless media directly contribute to the network's serious issues. Now, protecting networks from DoS attacks is essential [3]. This research safeguards the cluster leaders. The cluster administrator keeps track of all messages, whether legitimate or not. Therefore, it will be necessary to update the threshold values for each type

of communication [4]. The attacking node's access is further limited when a shared key is used. An authentication server will provide a shared key to each sensor node and the cluster leader. Any network device that wants to interact with other devices must first authenticate and broadcast the specifics of its authentication process. A hashing method is applied to the certificate credential to create the authentication data. The message is compared to the threshold as soon as it is received. The comparison's results are evaluated to ensure no problems exist [5]. The number of messages is compared to a predefined threshold, and only unexpected ones are eliminated. If it is higher than that, the sending node is likely engaging in illegal activity. S1 won't be able to communicate with CH1 until it can authenticate itself to that node (the cluster head). It has these characteristics as shown in figure:1.

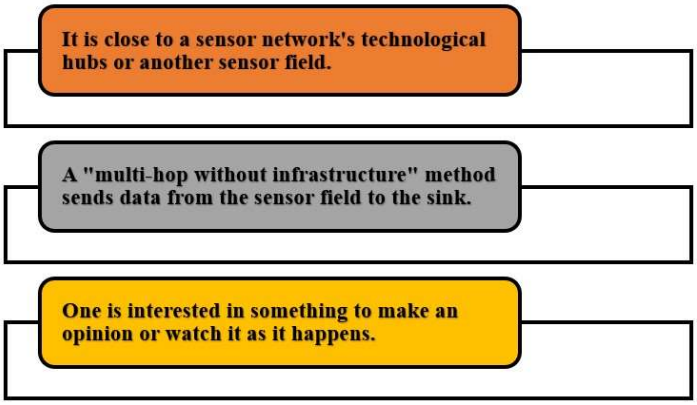

Figure:1 Characteristics of WSN

CH1 will notify the authentication server if it discovers that s1 is a malicious node. The authentication server must instantly report the rogue node to all other nodes, which must also supply a new key. Consider the case when node S1 has relocated to Cluster 2 and is attempting to contact node CH2. The creation of an authentication "hash" code is the next stage. It must create a new hash code since CH2's new key is incompatible with S1's hash value [6]. As a result, CH2 is aware that s1 is a susceptible node right away. A network of wireless sensors is shown in Figure 2.

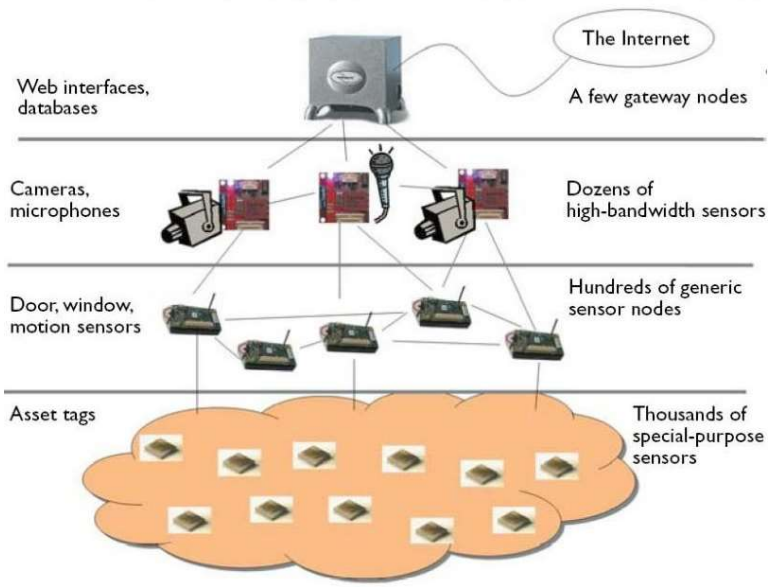

Figure:2 Wireless sensor network.

Wireless networks are more susceptible to attacks than cable ones, and these attacks could be purposeful or unintentional [7]. Several factors include the limited resources available to each node in a wireless sensor network and the frequent ad hoc and decentralized configuration of wireless networks (such as electricity, computer power, and storage space). The most basic type of such an attack, DoS assault, can interfere with even reliable connections [8]. However, by sending out a barrage of phone or duplicate signals, the attackers can seize control of some sensors and launch the DoS assault. DoS attack aims to deny authorized users access to a network-based service or resource. The numerous security holes in wireless media directly contribute to the network's serious issues. Now, protecting networks from DoS attacks is essential. This research safeguards the cluster leaders. The cluster administrator keeps track of all messages, whether legitimate or not. Therefore, it will be necessary to update the threshold values for each type of communication [9]. The attacking node's access is further limited when a shared key is used. An authentication server will provide a shared key to each sensor node and the cluster leader.

Any network device that wants to interact with other devices must first authenticate and broadcast the specifics of its authentication process. A hashing method is applied to the certificate credential [10]. The message is compared to the threshold as soon as it is received. The comparison's results are evaluated to make sure no problems exist. The number of messages is compared to a predefined threshold, and only unexpected ones are eliminated. The sending node is likely up to no good if it is significantly higher. S1 won't be able to communicate with CH1 until it can authenticate itself to that node (the cluster head). CH1 will notify the authentication server if it discovers that s1 is a malicious node. The authentication server must instantly report the rogue node to all other nodes, which must also supply a new key. Consider the case when node S1 has relocated to Cluster 2 and is attempting to contact node CH2. Creating an authentication "hash" code is the next stage [11]. It must create a new hash code since CH2's new key is incompatible with S1's hash value.

2. Related Works

Sensor networks (SNs) are susceptible to DoS attacks due to their design as low-powered devices without a centralized monitoring system. The multilayer protocol of the sensor network has now been designed to withstand various kinds of denial-of-service assaults [12]. According to the attacker's skill, attacks may come from the outside or the inside (node compromise). An insider attack occurs when authorized nodes in a WSN take a harmful or unanticipated activity. "Outside attacks" are actions taken by nodes outside of a WSN to undermine it. Attacks can be both violent and nonaggressive. Active attacks change or produce a new data stream, whereas passive attacks only need to watch the traffic across a WSN. Numerous techniques for various routing protocols have been developed to increase the security of sensor networks [13].

Each node along the path has a one-way hash chain (OHC) installed so that it can recognize a DoS attack. Each broadcast from a particular source received an OHC number. The messages can only be delivered if the chain can confirm their integrity [14]. Even yet, OHC failed to protect the data while it was being sent between the member nodes and the CH, leaving it open to outside meddling. The network from operating correctly since it puts its leader open to assault from any other node.

3. System Architecture

The authorized server generates and distributes a distinct key assigned to each node in the network. Additionally, it keeps track of the hacked nodes. Each node creates its hash value after obtaining the server's key [15]. Before beginning communication with another network node for the first time, a node must always authenticate and identify itself to the appropriate cluster head. The authentication is given and verified by the cluster chiefs. Users could start creating a connection to that sensor node if the verification was successful. After communication has started, the cluster head system checks to determine if it has received normal or abnormal signals, dismissing the latter. The attacker node is in charge of disseminating inaccurate data. It is crucial to identify the rogue node and notify the server. The attacking node will then transmit updated data and create new keys for each node in the cluster [16]. When the attacking node tries to resume communication, the cluster leader will check its authentication. Contact is broken when one party suspects the other that the message is false.

4. System Modules

4.1 Normal Case

Think of a network where many of the nodes are sensors. The next technique is to segment the network, as shown in Figure: 3. The CH (cluster head) node of each cluster serves as a manager for the others, collecting information, verifying that release criteria are adhered to, etc. Before any data is delivered to the central station, the network's nodes gather it and send it to the central hub [17]. The particular sensor's unique identity is added to CH once the cluster has been built. The unique keys are created by the authorized server and distributed to each node. The cluster head and sensor nodes are given keys, using hashing operations to create a hash code. When the initial phase is over, the new node will undergo CH and neighbour node authentication.

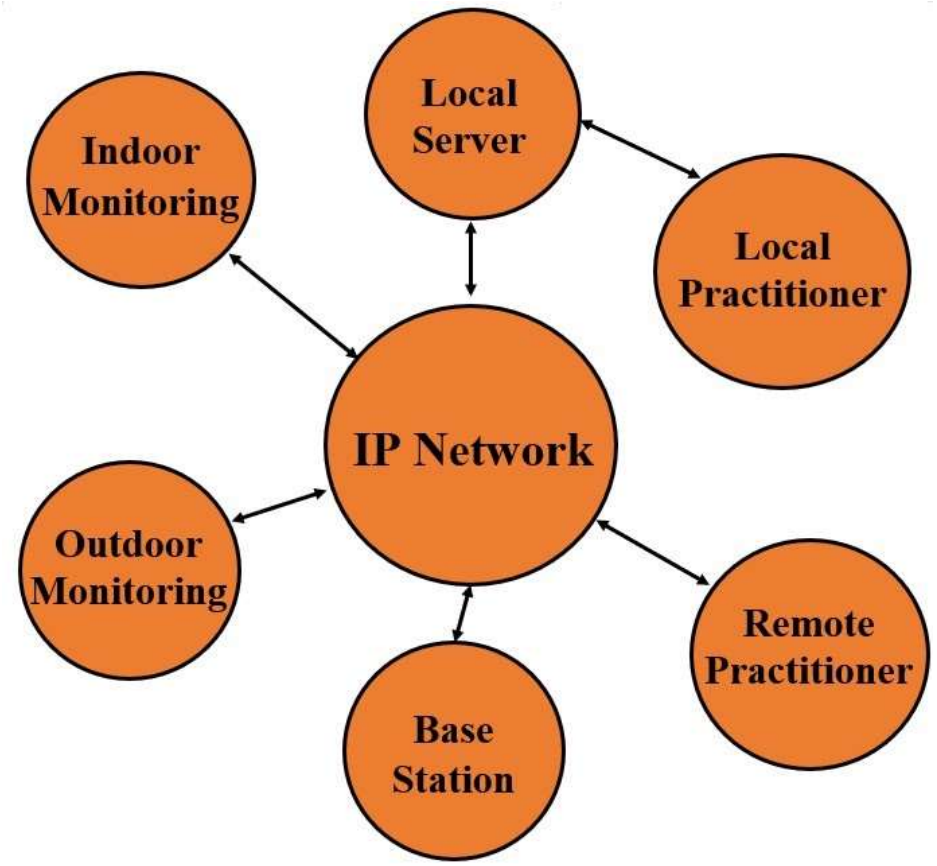

Figure:3. System architecture [18]

4.2 Attack Case

When the attack module turns one node into an attacker node, bad things take place. The malicious node shown in the next graphic tries to overwhelm the cluster leader with false or duplicate messages to silence it [19]. Finally, the authors have produced a virus that spreads across the entire system as shown in figure:4.

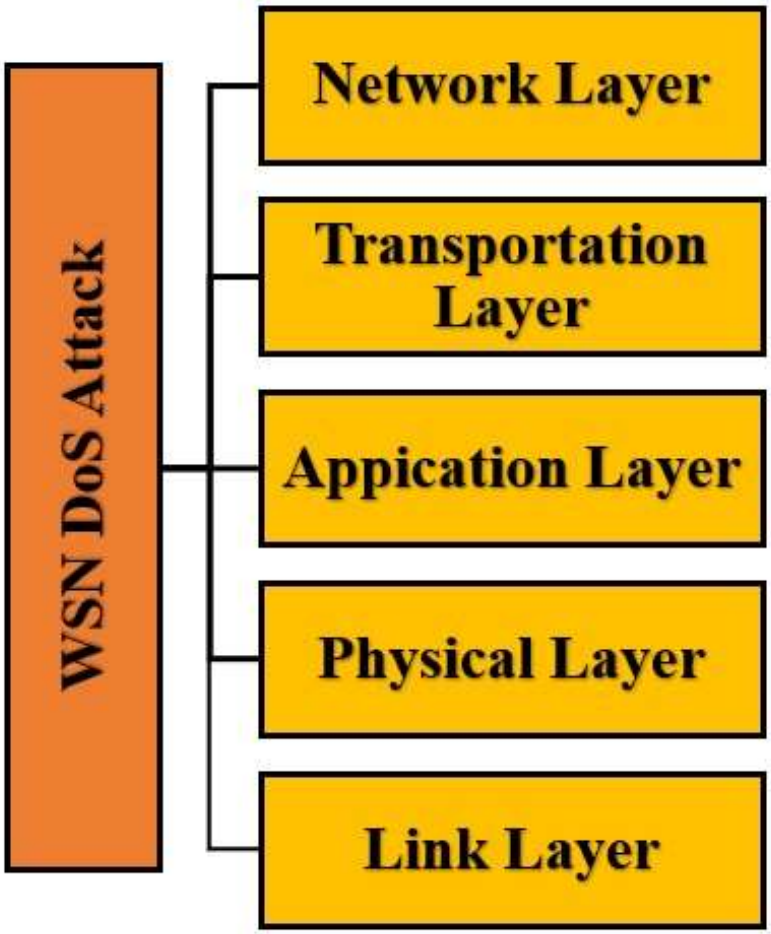

Figure: 4 Attack model [20]

4.3 Detection and avoidance protocol case

Before connecting to a node in the network, a request containing a hash code must be sent to the cluster head of that node. The cluster master will next verify the sender node's validity. The message will be the only one accepted if it is successfully sent; else, all earlier messages affecting that node will be ignored [21]. Message observation can identify DoS assaults and send the right protocol for mitigating and fending them off.

5. Detection protocol

The quantity and nature of the messages broadcast are frequently used to identify the source of a DOS attack. It determines whether the communication is unique, exceptional, or normal after receiving it. A message's normalcy can be ascertained by comparing the counter value to a predetermined threshold [22]. The sender is more likely to be a malicious node if the target value is more than the counter value. Furthermore, it wrongly assumes that an attacking node is sending a strange message. The set of default messages is expanded to include any novel messages, and the threshold is then assessed. Algorithm to determine whether the attack is a DoS attack.

Step: 1 User wrote the disputed letter.

Step: 2 Check to see if this message is unusual or not.

Step: 3 Sending node is up to no good if something about the message seems strange.

Step: 4 To determine whether the message is normal, compare the count to the threshold value. If the count exceeds the threshold, it is presumed that the sending node is malicious.

Step: 5 Return to step 1.

6. Avoidance protocol

After receiving a notification from the cluster head that the attacker node has been found, the server node updates its list of intruders. The attacker node never receives a new key when the server generates and distributes them to the nodes in a specific cluster zone. The cluster head also relays the attacker's id to all of the sensor nodes in the cluster so that if they suddenly stop getting messages from that id, they will be aware that something is wrong [23]. The attempts of the attacker node to communicate are still being rejected since they are not authorized.

Step:1 The cluster head can inform a server about who is hitting it and what they are doing.

Step:2 The server produces new keys and distributes them to the other nodes in the cluster when a node in a cluster is attacked. The system stores the information in its database of historical events.

The full process is depicted in the diagram below. The cluster head examines any messages sent by sensor nodes to see if they are normal or if there is a problem. The system then compares the count to a standard to determine if it is abnormal [24]. The connection is disconnected, and the node is considered a potential danger if the sum exceeds a predetermined threshold. The base station produces and distributes the new key to all of the cluster's nodes after receiving a notification from the cluster leader that it is required. The cluster head relays the signal to the alleged attacker once an attack candidate node receives it from the base station as shown in figure:5 [25].

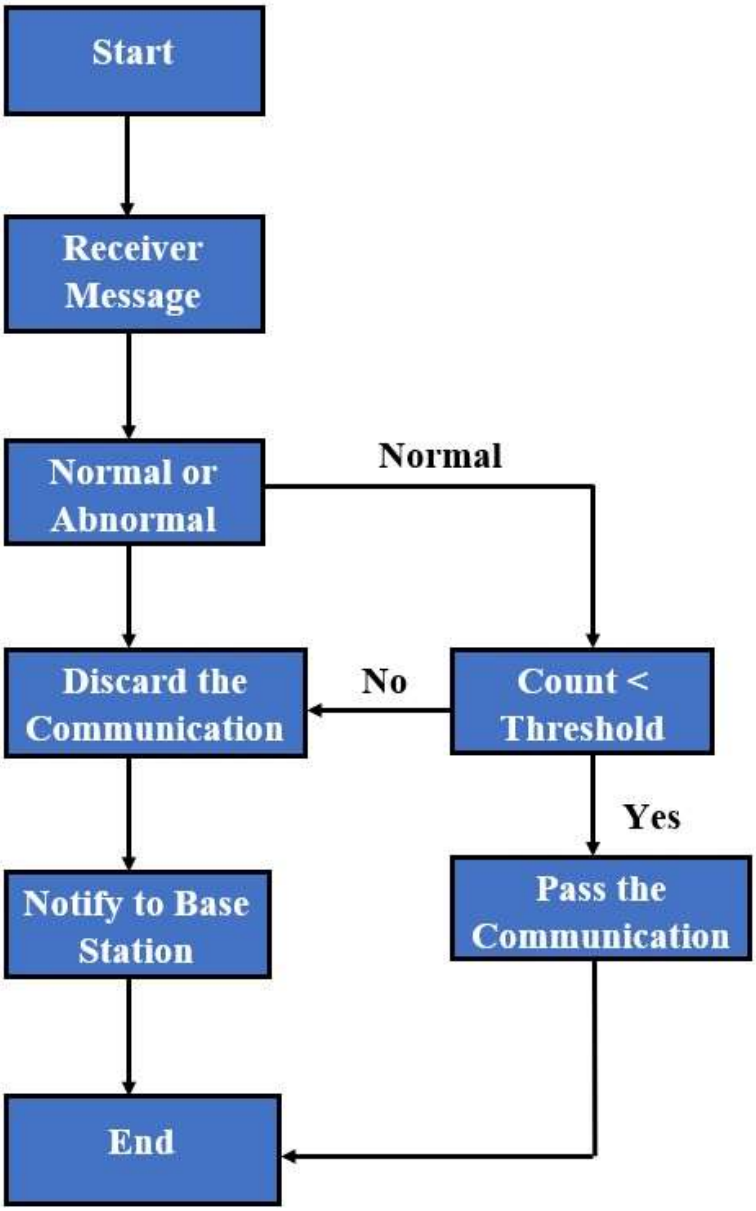

Figure: 5 Process flow

7. Conclusion

The minimal levels of interaction needed vary depending on the type of communication. By utilizing shared-key authentication, this strategy isolates the vulnerable node even more. An authentication server periodically sends a shared key to the cluster master, every sensor node, and every other node. The above technique effectively and permanently thwarts Dos attacks. Because it enables the collaboration of various systems, applications, and data, WSN is the most crucial component of IoT. Numerous ways in which the WSNs could support the Internet of Things. The advantages and disadvantages of combining the Internet and WSN are still considered. A WSN is a network of numerous nodes that can detect and keep track of data and environmental interactions. There are sensors and controllers on each node. As a result, there

is a closer connection than ever between humanity, technology, and the natural world. WSN is one of the components that support IoT. The WSN will power the IoT. The WSN serves as the central processing node of the IoT architecture's middle network tier. A microcontroller, a wireless transceiver, the sensor itself, and a power management module make up a sensor's hardware configuration.

References

1. Daanoune, Ikram, Abdennaceur Baghdad, and Waheed Ullah. "Adaptive coding clustered routing protocol for energy-efficient and reliable WSN." *Physical Communication* 52 (2022): 101705.
2. Singh, Akansha, and Khushboo Jain. "An automated lightweight key establishment method for secure communication in WSN." *Wireless Personal Communications* (2022): 1-21.
3. Yaqub, Talha Bin, et al. "Effect of Annealing Heat Treatment on the Composition, Morphology, Structure and Mechanical Properties of the WSN Coatings." *Materials* 15.12 (2022): 4088.
4. Naresh, Vankamamidi S., V. V. L. Allavarpu, and Sivaranjani Reddi. "Provably secure blockchain privacy-preserving smart contract centric dynamic group key agreement for large WSN." *The Journal of Supercomputing* 78.6 (2022): 8708-8732.
5. Pal, Tumpa, Ramesh Saha, and Suparna Biswas. "Sink Mobility-Based Energy Efficient Routing Algorithm Variants in WSN." *International Journal of Wireless Information Networks* (2022): 1-20.
6. Tošić, Aleksandar, Niki Hrovatin, and Jernej Vičič. "A WSN Framework for Privacy-Aware Indoor Location." *Applied Sciences* 12.6 (2022): 3204.
7. Truong, Van-Truong, Dac-Binh Ha, and Chakchai So-In. "On the System Performance of Mobile Edge Computing in an Uplink, NOMA WSN With a Multiantenna Access Point Over Nakagami-$ m $ Fading." *IEEE/CAA Journal of Automatica Sinica* 9.4 (2022): 668-685.
8. Dogra, Roopali, Himanshi Babbar, and Shalli Rani. "Integration of WSN and IoT: Its Applications and Technologies." *IoT and WSN based Smart Cities: A Machine Learning Perspective*. Springer, Cham, 2022. 243-256.
9. Ali, Shokat, and Rakesh Kumar. "Hybrid energy efficient network using firefly algorithm, PR-PEGASIS and ADC-ANN in WSN." *Sensors International* 3 (2022): 100154.
10. Poornimha, J., A. V. Senthil Kumar, and Ismail Bin Musirin. "Scheduling Method to Improve Energy Consumption in WSN." *Pervasive Computing and Social Networking*. Springer, Singapore, 2022. 523-537.
11. Almurisi, Nasr, and Srinivasulu Tadisetty. "Cloud-based virtualization environment for IoT-based WSN: solutions, approaches, and challenges." *Journal of Ambient Intelligence and Humanized Computing* (2022): 1-23.
12. Mahdi Elsiddig Haroun, Fathi, et al. "Towards Self-Powered WSN: The Design of Ultra-Low-Power Wireless Sensor Transmission Unit Based on Indoor Solar Energy Harvester." *Electronics* 11.13 (2022): 2077.

13. Kumar, Ranjit, Sachin Tripathi, and Rajeev Agrawal. "Handling dynamic network behavior and unbalanced datasets for WSN anomaly detection." *Journal of Ambient Intelligence and Humanized Computing* (2022): 1-14.

14. Sreedevi, Pogula, and S. Venkateswarlu. "An Efficient Intra-Cluster Data Aggregation and finding the Best Sink location in WSN using EEC-MA-PSOGA approach." *International Journal of Communication Systems* 35.8 (2022): e5110.

15. Wu, Juan, et al. "Multiobjective Optimization Strategy of WSN Coverage Based on IPSO-IRCD." *Journal of Sensors* 2022 (2022).

16. Sankari, B. Siva, and Ramya Nemani. "Squirrel Search Algorithm Based Support Vector Machine for Congestion Control in WSN-IoT." *Wireless Personal Communications* (2022): 1-16.

17. Hussain, Maruff, et al. "Tensile properties of cross cryo-rolled and room temperature rolled 6063 Al alloy." *Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering* (2022): 09544089221105929.

18. Shaik, Riaz, Lokesh Kanagala, and Hema Gopinath Sukavasi. "Sufficient Authentication for Energy Consumption in Wireless Sensor Networks." *International Journal of Electrical & Computer Engineering (2088-8708)* 6.2 (2016).

19. Liang, Jie, Lu Wang, and Qingchang Ji. "A Particle Swarm Optimization Algorithm for Deployment of Sensor Nodes in WSN Network." *Journal of Electrical and Computer Engineering* 2022 (2022).

20. Osanaiye, Opeyemi A., Attahiru S. Alfa, and Gerhard P. Hancke. "Denial of service defense for resource availability in wireless sensor networks." *IEEE Access* 6 (2018): 6975-7004.

21. Saxena, Aditi, et al. "Controlling of Manipulator for Performing Advance Metal Welding." *Recent Innovations in Mechanical Engineering*. Springer, Singapore, 2022. 41-48.

22. Singh, Nira, and Aasheesh Shukla. "A Review on Progress and Future Trends for Wireless Network for Communication System." *Advances in Communication, Devices, and Networking* (2022): 445-453.

23. Liu, Jinxue, and Gengxin Sun. "A Deployment Strategy of Nodes in WSN Based on "X" Partition." *Journal of Sensors* 2022 (2022).

24. Bansal, Saloni, and V. K. Tomar. "Challenges & Security Threats in IoT with Solution Architectures." *2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*. IEEE, 2022.

25. Agrawal, Reeya, et al. "Security and Privacy of Blockchain-Based Single-Bit Cache Memory Architecture for IoT Systems." *IEEE Access* 10 (2022): 35273-35286.