ISSN : 2455-9679
SJIF Impact Factor : 6.190

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"SECURE AND ENERGY-EFFICIENT ROUTING IN RPL-BASED IOT NETWORKS UNDER DIO SUPPRESSION ATTACKS"

Sanskriti Maheshwari [1], Mohit Jain [2]

[1]M.Tech Scholar, Department of Computer Science and Engineering, B.M. Group of Institutions, Indore, M.P., India
[2] Assistant Professor, Department of Computer Science and Engineering, B.M. Group of Institutions, Indore, M.P., India

ABSTRACT

The Internet of Things (IoT) has emerged as a transformative technology that enables seamless communication among interconnected devices and systems. Wireless Sensor Networks (WSNs) play a critical role in IoT environments by facilitating real-time data collection, monitoring, and communication. However, the Routing Protocol for Low-Power and Lossy Networks (RPL), widely used in IoT-based WSNs, is vulnerable to various security threats, including the DIO suppression attack. This attack disrupts routing topology formation by preventing the transmission of DIO messages, resulting in degraded network performance, increased packet loss, and reduced routing efficiency. This research proposes an enhanced routing framework based on the NLBGNDO algorithm to mitigate the impact of DIO suppression attacks in IoT-enabled wireless sensor networks. The proposed approach focuses on identifying optimal and trustworthy routing paths while minimizing delay, energy consumption, and routing disruption. Simulation experiments were conducted to evaluate network performance using key metrics such as Packet Delivery Ratio (PDR), path stretch, and power consumption. The results demonstrate that the proposed system significantly improves network reliability and security under attack conditions. The DODAG-based routing mechanism achieved a Packet Delivery Ratio of 88% while reducing power consumption to 11 mW compared with the existing IPv6-based approach. The findings indicate that the proposed method effectively enhances routing performance, energy efficiency, and attack resilience in resource-constrained IoT environments. This study contributes to the development of secure and reliable routing mechanisms for next-generation IoT and wireless sensor network applications.

Keywords: *Internet of Things (IoT) ,Wireless Sensor Networks (WSNs) ,Routing Protocol for Low-Power and Lossy Networks (RPL) ,DIO Suppression Attack ,Secure Routing.*

I. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most significant technological advancements of the twenty-first century. It has attracted considerable attention from researchers, industries, and governments due to its potential to transform everyday life through intelligent connectivity and automation. The concept of IoT was first introduced by Kevin Ashton in 1999 with the vision of connecting anything, anytime, anywhere through the Internet. The fundamental objective of IoT is to enable seamless communication among physical objects, people, and systems, thereby creating a smart and interconnected environment.

IoT refers to a network of physical objects, commonly known as "things," that are embedded with sensors, software, processors, and communication technologies. These devices collect, exchange, and analyze data through the Internet,

ISSN : 2455-9679
SJIF Impact Factor : 6.190

enabling them to perform tasks autonomously and provide intelligent services. By integrating sensing, computing, and communication capabilities, IoT facilitates real-time monitoring, decision-making, and automation across various domains.

The architecture of IoT comprises several essential components, including sensors, actuators, communication networks, cloud computing platforms, and data analytics systems. These components work together to gather information from the physical environment, process the collected data, and generate meaningful insights. Various communication protocols such as MQTT, CoAP, HTTP, ZigBee, Bluetooth, Wi-Fi, and LoRaWAN are employed to ensure efficient data transmission between devices and applications (Alanhdi, 2024)

One of the key objectives of IoT is to support the development of smart environments and improve the quality of life. IoT applications provide four major categories of services: identity-related services, information aggregation services, collaborative-aware services, and ubiquitous services. Identity-related services focus on recognizing and identifying objects, while information aggregation services collect and process data from multiple devices. Collaborative-aware services analyze the gathered information and support intelligent decision-making. Ubiquitous services ensure that information and services are available anytime and anywhere, enabling continuous connectivity and accessibility.

The application areas of IoT are extensive and continuously expanding. In healthcare, IoT enables remote patient monitoring, real-time health tracking, and intelligent medical systems that improve healthcare delivery and patient outcomes. In agriculture, IoT-based smart farming solutions utilize sensors and automated systems to monitor soil conditions, irrigation, crop health, and environmental factors, leading to increased productivity and sustainable farming practices. In transportation and smart cities, IoT facilitates intelligent traffic management, smart parking systems, vehicle tracking, and efficient public transportation services. Similarly, IoT applications in home automation allow users to control lighting, security systems, appliances, and energy consumption remotely.

Industrial sectors are also benefiting significantly from IoT technologies through the implementation of Industry 4.0 concepts. Smart manufacturing systems use connected sensors and devices to monitor production processes, predict equipment failures, optimize resource utilization, and enhance operational efficiency. Furthermore, IoT integrated with cloud computing provides scalable storage, real-time data processing, and improved computational performance for large-scale applications.

Despite its numerous advantages, IoT faces several challenges, including security, privacy, interoperability, scalability, and energy efficiency. The increasing number of connected devices creates vulnerabilities that may expose sensitive information to cyber threats. Therefore, developing secure communication mechanisms, robust authentication techniques, and efficient resource management strategies remains a critical area of research.

The wireless sensor network (WSN) is an area of networking that is growing quickly at the moment. It is a wireless network that can set itself up and is made up of many devices spread out over a large area. In its simplest form, a wireless sensor network (WSN) is a group of small, simple units that connect to each other wirelessly and send data to a central processing and decision-making unit. A WSN is just a network that is made up of nodes. The information is then sent to a sink or base station through a number of nodes in between. This central node, which is also called a sink or base station, is where users join to the network. The data can be used directly at the sink, or it can be sent through a gateway to other networks, including the Internet. In a normal wireless sensor network, thousands of sensor nodes are linked together and share information using radio waves. This means that the network infrastructure needs to have power sources, radio transceivers, and sensors. In a wireless sensor network, each node has limited abilities, such as a slow maximum processing speed, a slow maximum storage capacity, and a slow maximum connection bandwidth.

In situations where the deployment of sensor nodes is required to monitor physical or environmental variables, wireless sensor networks (WSNs) are crucial elements of the Internet of Things (IoT) ecosystem. WSNs make use of sensors that can record information on a range of events, including motion, temperature, vibration, pressure, sound, or pollution. These sensors' data collection offers useful information on how the environment around them is doing. WSNs are used in a variety of industries, including surveillance, target tracking, intrusion detection, infrastructure monitoring, and habitat monitoring. For instance, WSNs can be used to monitor the structural health of bridges, buildings, or dams in infrastructure monitoring, enabling the early discovery of possible defects or damages. WSNs work with habitat monitoring to study wildlife activity, keep an eye on the environment, and ensure the preservation of

ISSN : 2455-9679
SJIF Impact Factor : 6.190

natural resources.

It takes a thorough understanding of many different domains and technologies to implement WSNs successfully. This includes understanding wireless network-specific communication protocols and techniques, signal processing techniques for deriving informational value from sensor data, hardware technologies for designing and deploying sensor nodes, embedded system design for effective resource utilization, and software engineering for creating dependable and scalable WSN applications.The seamless connectivity and communication between sensor nodes and other IoT devices is made possible by the integration of WSNs into the wider IoT framework. WSNs are essential for collecting real-time data from the physical world and sending it to more complex systems for automation, analysis, and decision-making (Balasbaneh,2026).

II. RELATED WORK

Choudhary (2024) presented a comprehensive review of Internet of Things (IoT) architectures, applications, simulation tools, challenges, and future directions. The study highlighted that IoT has evolved into a transformative technology connecting intelligent devices across healthcare, transportation, agriculture, smart cities, and industrial automation. The author identified interoperability, security, scalability, and energy efficiency as major challenges affecting large-scale IoT deployment.

Alanhdi et al. (2024) investigated the integration of Artificial Intelligence (AI) and Edge Computing with IoT systems. Their survey demonstrated that edge intelligence enables real-time data processing, reduces network latency, and enhances decision-making capabilities in IoT environments. The study emphasized the importance of AI-powered IoT applications in Industry 5.0 and smart infrastructures.

Allam et al. (2024) reviewed blockchain-enabled IoT healthcare systems and analyzed various integration frameworks. The researchers concluded that blockchain technology improves data integrity, privacy, authentication, and secure information sharing in healthcare IoT environments. However, challenges related to scalability and computational overhead remain significant.

Mu et al. (2024) conducted a science-mapping review of IoT applications in industrial management. The study found that IoT technologies contribute significantly to predictive maintenance, resource optimization, production monitoring, and operational efficiency in Industry 4.0 environments. The authors highlighted digital transformation as a major driver of industrial IoT adoption.

Yaraziz et al. (2024) examined Edge Computing in Internet of Medical Things (IoMT) systems. Their findings indicated that edge-based healthcare architectures improve response time, reduce cloud dependency, and enhance patient monitoring efficiency. The study demonstrated the effectiveness of edge computing for real-time medical applications.

Ali et al. (2024) provided a comprehensive review of IoT applications and challenges. The study reported that IoT technologies have expanded rapidly in healthcare, transportation, environmental monitoring, and smart city infrastructures. Security, privacy, and standardization were identified as major research concerns requiring further investigation.

III. PROPOSED SYSTEM

In the DIO suppression attack, the attacker induces victim nodes to suppress the transmission of DIO messages. DIO messages are crucial for building the routing topology in RPL. By suppressing these messages, the attacker disrupts the quality of the routes, which can eventually result in network partitions.

What makes the DIO suppression attack distinct from other attacks discussed in the literature is that it does not require the adversary to forge bogus RPL messages. Instead, the attacker simply replays previously heard messages periodically. This allows the attack to be carried out without resorting to the theft of cryptographic keys from honest nodes. The DIO suppression assault makes advantage of the replay technique, a common attack method with a unique use in this case. The goal of the replay technique is to trick the victim into thinking that previously presented information is brand new. However, the replay technique is utilized in the DIO suppression attack to trick a target into thinking that the routing information it is about to provide has already been sent several times by other nodes.

ISSN : 2455-9679
SJIF Impact Factor : 6.190

The Work demonstrates that the DIO suppression attack significantly degrades the routing service provided by RPL. Furthermore, it highlights that this attack is less energy-expensive compared to a jamming attack proposed in the system.

The impact of the DIO suppression attack on the network is severe, causing significant degradation of the routing service. However, compared to a traditional jamming attack, this new attack is less energy-expensive. In other words, the attacker can achieve a similar impact on the network without expending as much energy as a jamming attack would require.

By identifying and exploring this novel attack, the researchers aim to raise awareness about potential vulnerabilities in RPL and the need for enhanced security measures in IoT systems. This research contributes to the ongoing efforts to develop robust and secure routing protocols for WSANs, ensuring the reliable and efficient operation of IoT network.

IV. RESULT DISCUSSION

The focus is on proposing a novel algorithm called NLBGNDO to address the problem of finding an optimal path from source to destination sensor nodes in RPL. The algorithm aims to provide trustworthy and efficient routing in the presence of the DIO suppression attack. To evaluate the performance of the proposed algorithm, simulations are conducted. The simulation model is designed to find the best route and minimize delay in the presence of the attack. Some specific results are mentioned:

Packet Delivery Ratio: The simulation measures the packet delivery ratio, which indicates the percentage of successfully delivered packets compared to the total number of packets sent. This metric helps evaluate the efficiency and reliability of the proposed algorithm in maintaining packet delivery despite the DIO suppression attack.

Path Stretch with Attack and Without Attack: Path stretch refers to the elongation of the routing path compared to the optimal or shortest path. The simulation measures the path stretch under both attack and non-attack conditions. This provides insights into how the proposed algorithm performs in maintaining efficient routing paths despite the attack.

Power Consumption**:** Power consumption is an important factor in resource-constrained networks like WSNs and IoT systems. The simulation includes the measurement of power consumption to assess the energy efficiency of the proposed algorithm, considering both the attack scenario and the normal operation.

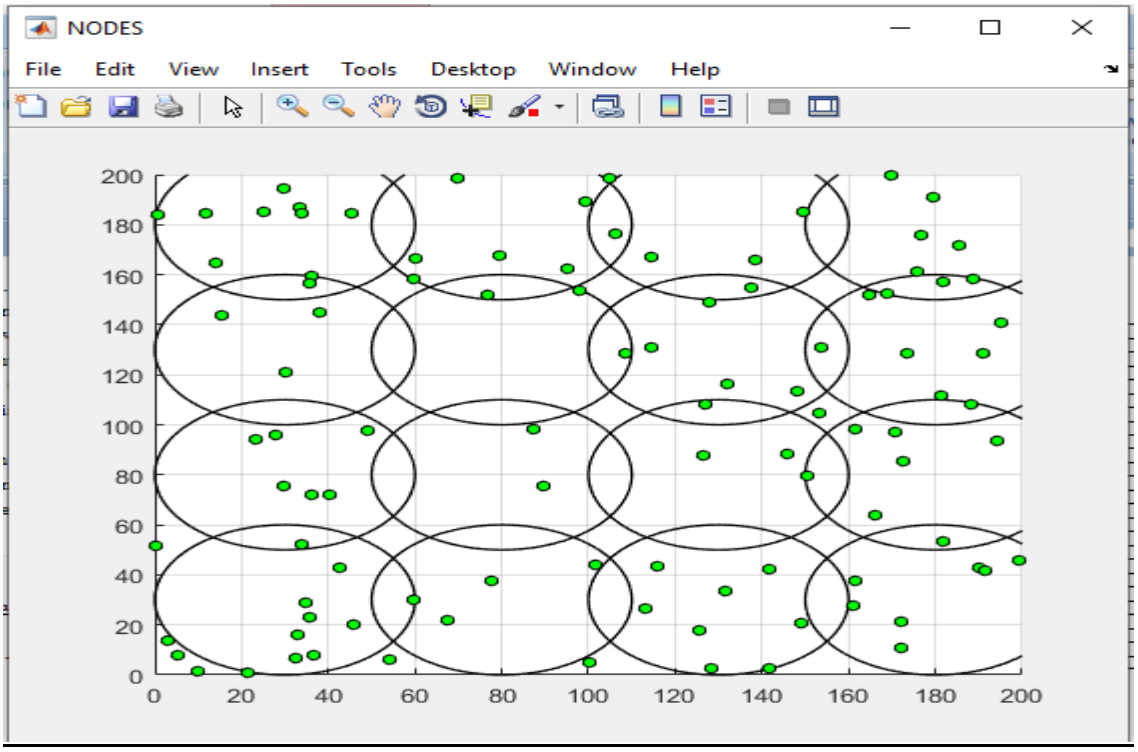


Fig. 1. initial network

ISSN : 2455-9679
SJIF Impact Factor : 6.190

Set up the original network's parameters and copy its node count. Initial network dimensions are depicted in Figure 1; they are 200 metres in length, 200 metres in Sensing_region_width (the width of clusters), 30 metres in radius, and 36 metres in sensation distance.

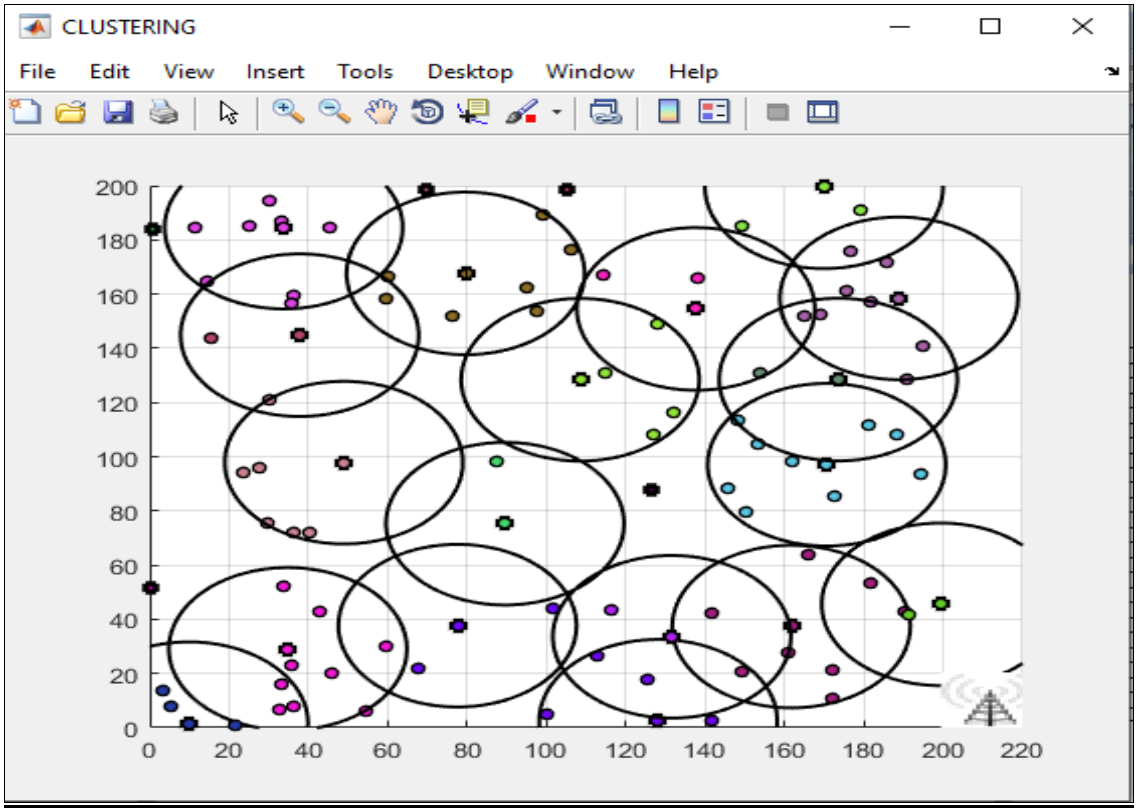


Fig. 2. Cluster Head

The cluster head has a major impact on the WSN's expected lifetime. The node that has the most power, the most neighboring nodes, and the shortest distance to the base station is the best candidate for the cluster head position.

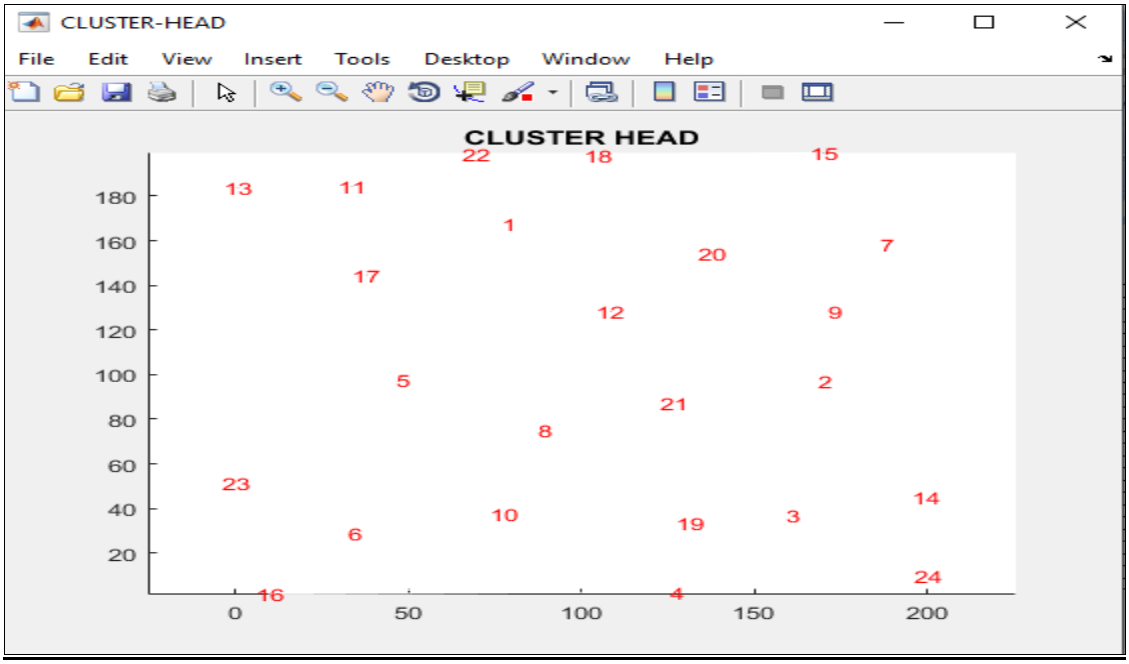


Fig. 3. number of cluster head

ISSN : 2455-9679
SJIF Impact Factor : 6.190

Figure 3 displays the node count distribution throughout the network's various node clusters. Each cluster in the WSN is led by a manager who is in charge of gathering information from its nodes and transmitting it to the network's hub.

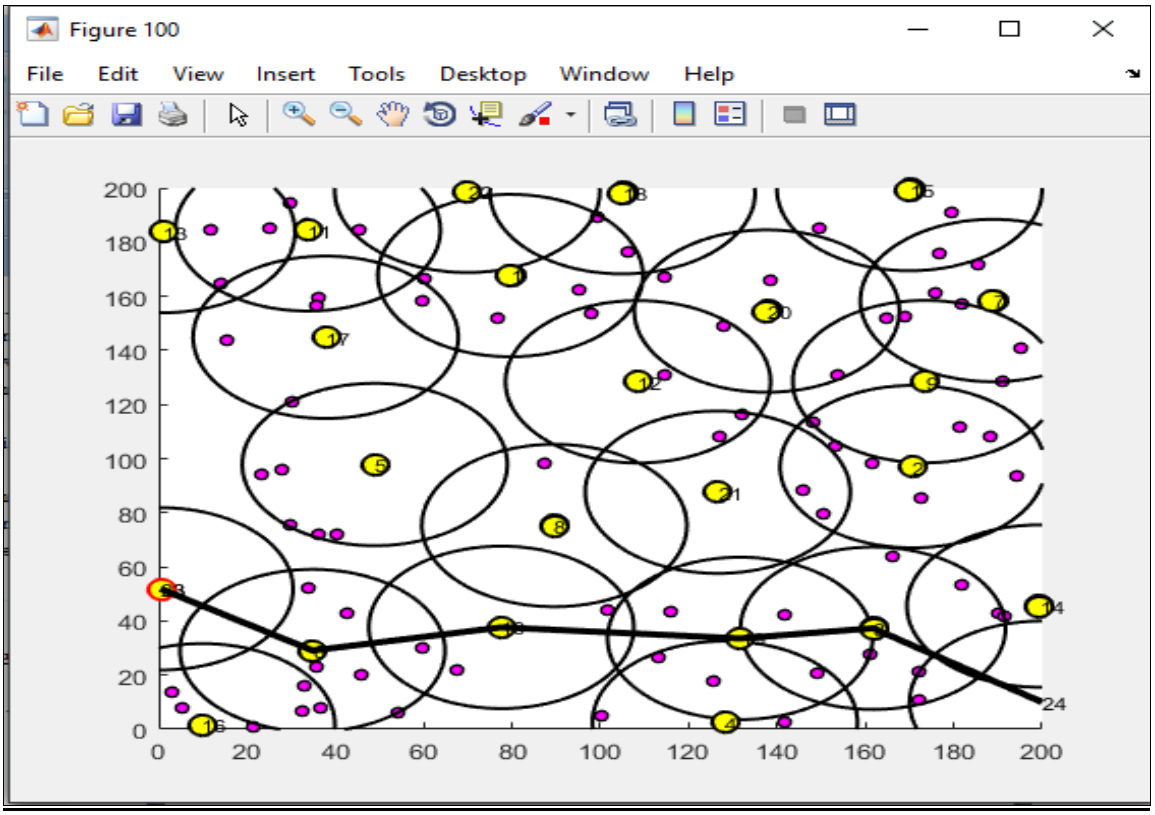


Fig.4 node discovers the optimal network path

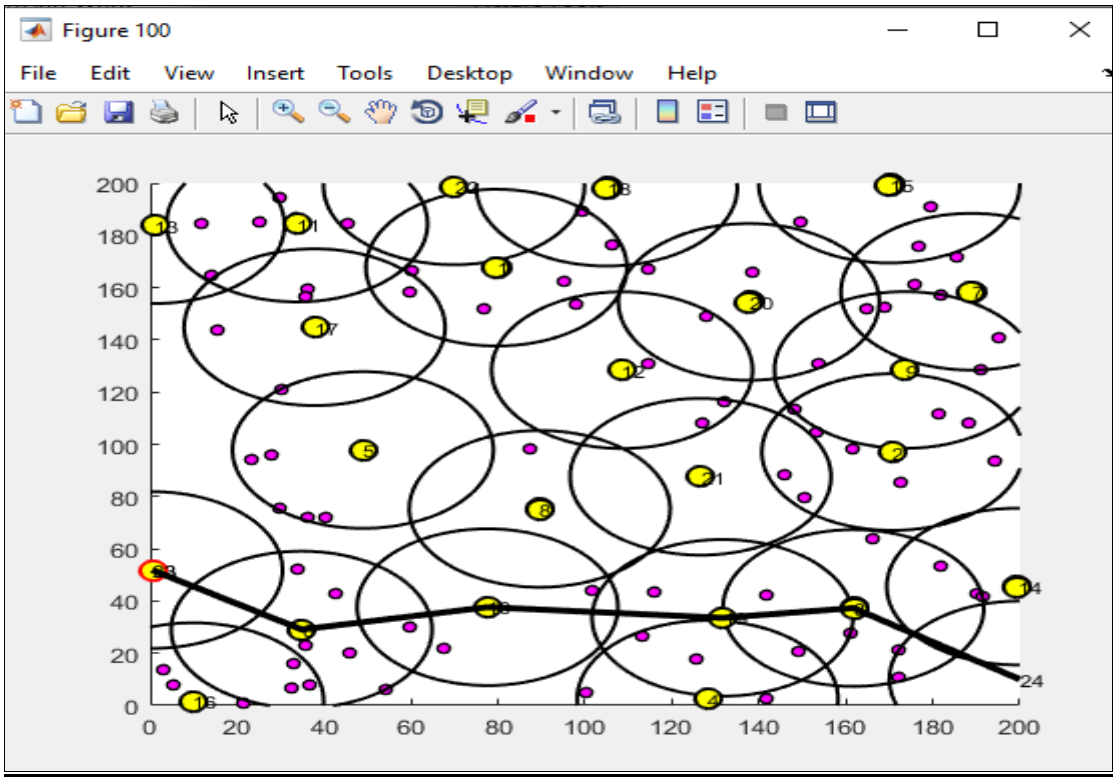


Fig. 5. node seeking path in the network to secure communication

ISSN : 2455-9679
SJIF Impact Factor : 6.190

In a network, finding the optimum path refers to identifying the most efficient route for transmitting data from a source node to a destination node

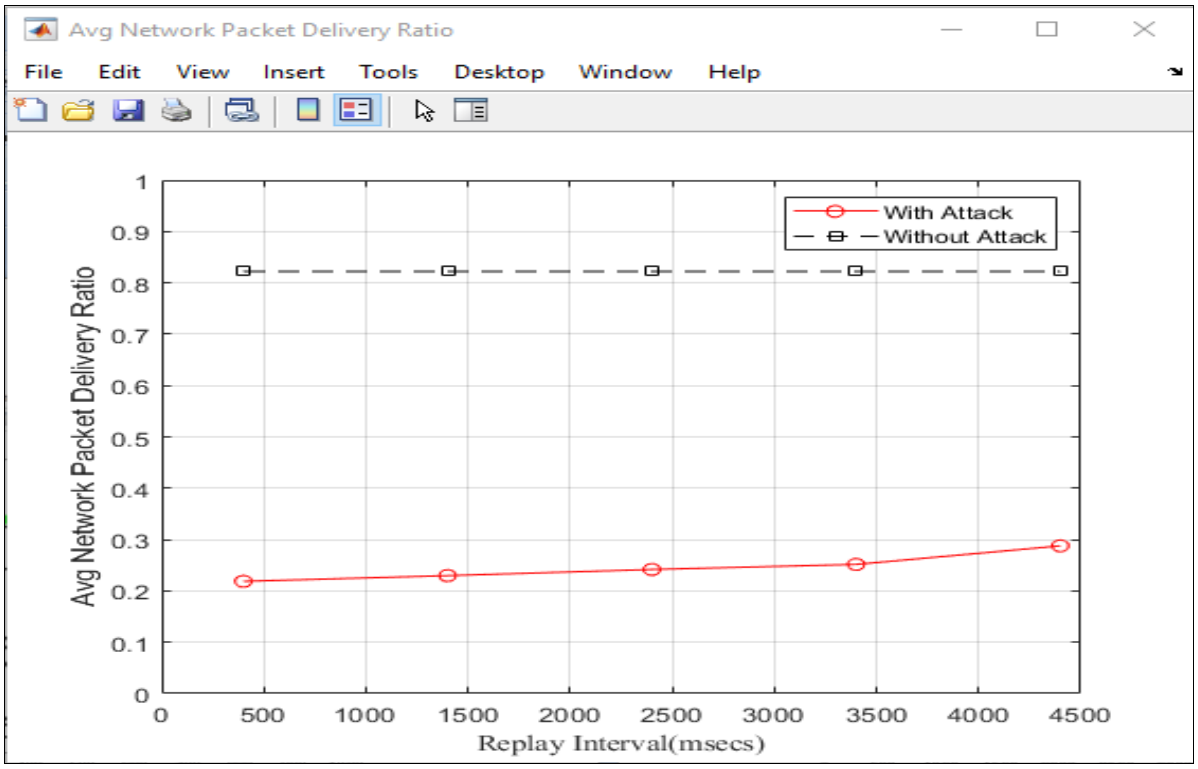


Fig. 6. Average network packet delivery ratio

The average network packet delivery ratio provides insight into the network's performance in terms of successfully delivering packets. A higher delivery ratio indicates better network reliability and efficiency, while a lower ratio suggests potential issues such as congestion, packet loss, or network disruptions

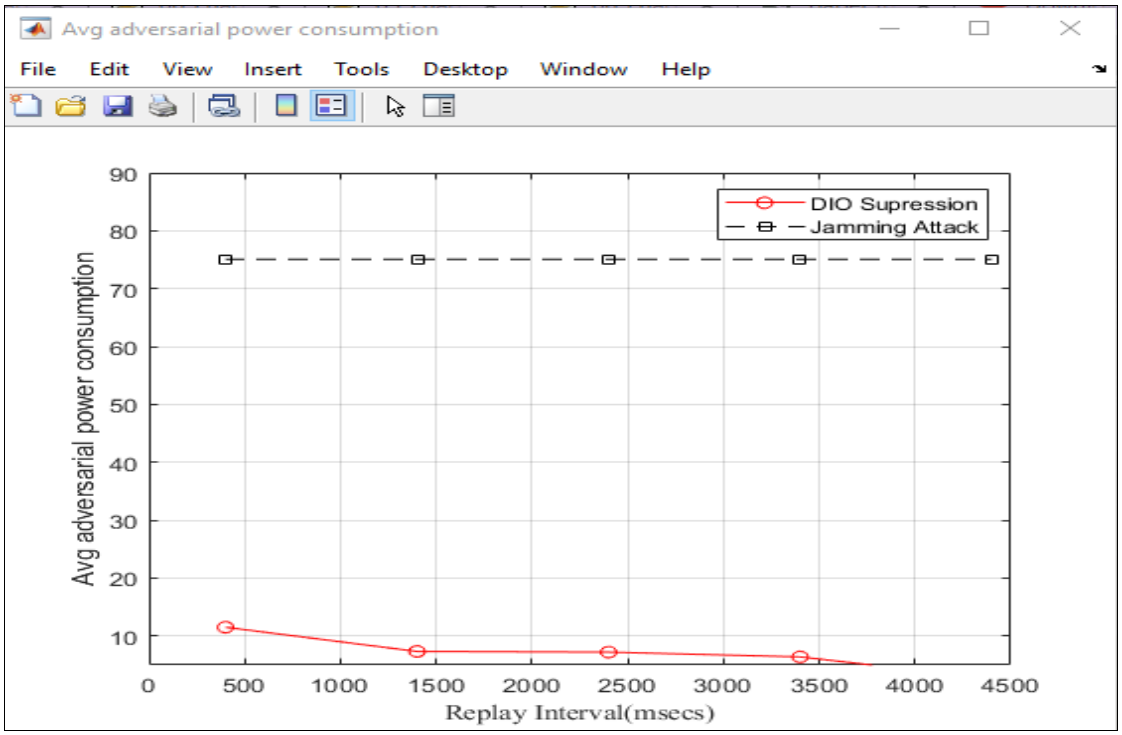


Fig.7. Average adversarial power consumption

ISSN : 2455-9679
SJIF Impact Factor : 6.190

The average amount of power consumed by an adversary or attacker during malicious activities or attacks in a network. It represents the energy expended by the adversary in carrying out disruptive actions, compromising the network's security, or causing damage to the system.

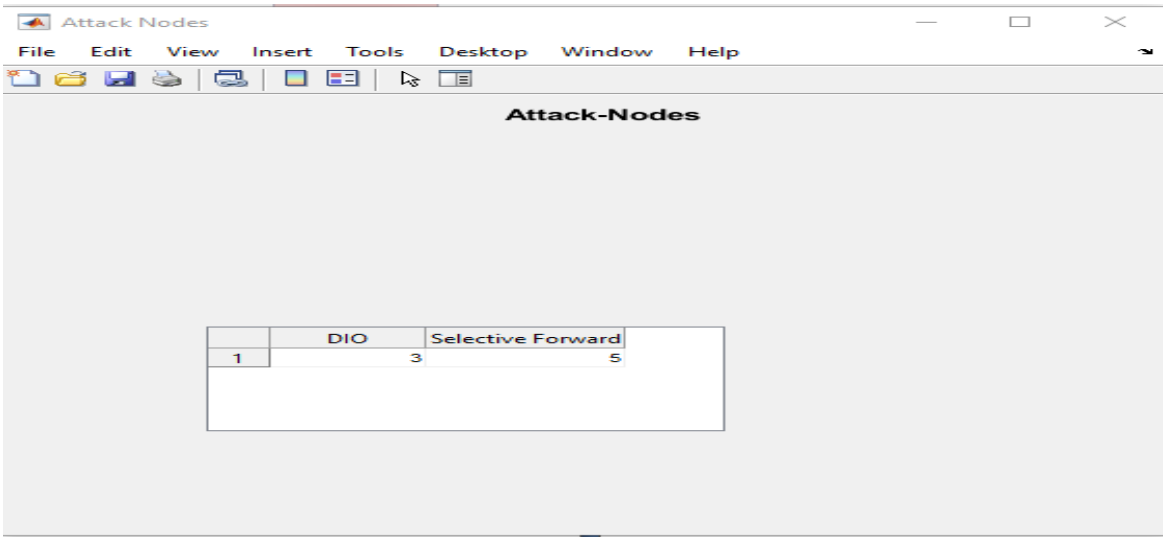
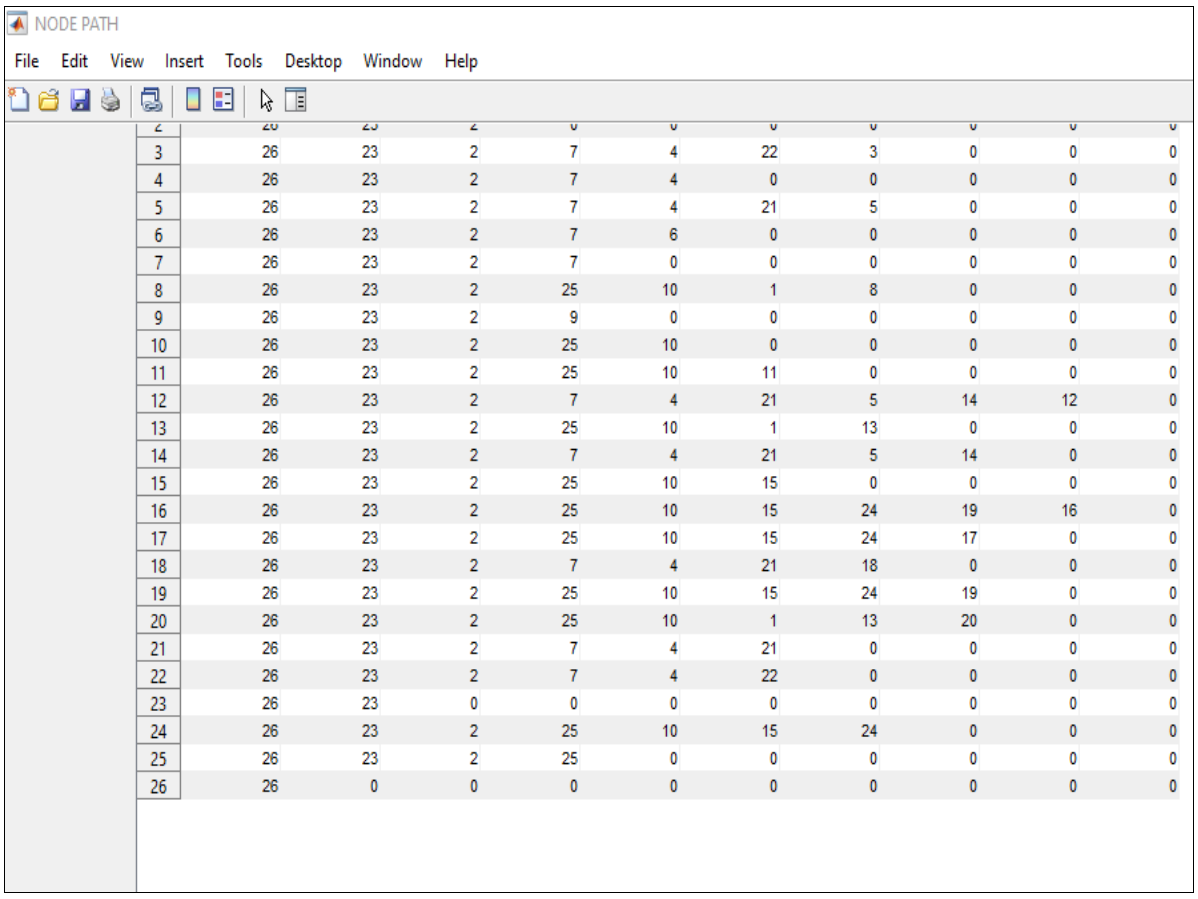


Fig. 8. DIO attack

An attack node refers to a malicious or compromised node within a network that is intentionally involved in carrying out attacks or disruptive activities. In the context of network security, an attack node may be controlled by an adversary or compromised by malware or unauthorized access



3	26	23	2	7	4	22	3	0	0	0
4	26	23	2	7	4	0	0	0	0	0
5	26	23	2	7	4	21	5	0	0	0
6	26	23	2	7	6	0	0	0	0	0
7	26	23	2	7	0	0	0	0	0	0
8	26	23	2	25	10	1	8	0	0	0
9	26	23	2	9	0	0	0	0	0	0
10	26	23	2	25	10	0	0	0	0	0
11	26	23	2	25	10	11	0	0	0	0
12	26	23	2	7	4	21	5	14	12	0
13	26	23	2	25	10	1	13	0	0	0
14	26	23	2	7	4	21	5	14	0	0
15	26	23	2	25	10	15	0	0	0	0
16	26	23	2	25	10	15	24	19	16	0
17	26	23	2	25	10	15	24	17	0	0
18	26	23	2	7	4	21	18	0	0	0
19	26	23	2	25	10	15	24	19	0	0
20	26	23	2	25	10	1	13	20	0	0
21	26	23	2	7	4	21	0	0	0	0
22	26	23	2	7	4	22	0	0	0	0
23	26	23	0	0	0	0	0	0	0	0
24	26	23	2	25	10	15	24	0	0	0
25	26	23	2	25	0	0	0	0	0	0
26	26	0	0	0	0	0	0	0	0	0

Fig.9 Node path

ISSN : 2455-9679
SJIF Impact Factor : 6.190

Table 1 result comparison with existing work

	Protocol	Power Consumption (Mw)	Packet Delivery Ratio (%)
Existing wok	IPv6-based	13	75
Proposed system	DODAG	11	88

Table 1 presents a comparative analysis of the results between the existing work, which utilizes an IPv6-based protocol, and the proposed system employing a DODAG (Destination-Oriented Directed Acyclic Graph) protocol. The table evaluates two key performance metrics: power consumption and packet delivery ratio. In the existing work, the IPv6-based protocol demonstrated a power consumption of 11(Mw) units and a packet delivery ratio of 13%. In contrast, the proposed system utilizing the DODAG protocol exhibited higher power consumption at 75 units but achieved a significantly improved packet delivery ratio of 88. This comparison highlights the trade-offs between power efficiency and network performance between the two protocols, with the proposed DODAG system showcasing superior reliability in packet delivery despite higher power consumption.

V. CONCLUSIONS

This research project focused on analyzing the impact of the DIO suppression attack on the Routing Protocol for Low-Power and Lossy Networks (RPL) and evaluating the effectiveness of the NLBGNDO algorithm in mitigating the attack. Through the development of a simulation code and careful analysis of key metrics, valuable insights have been gained regarding the vulnerabilities of RPL and potential countermeasures.The analysis of packet delivery ratio revealed that the DIO suppression attack significantly degrades the network's ability to deliver data. The attack disrupts the routing protocol by suppressing DIO messages, leading to decreased packet delivery and potential data loss. This highlights the importance of addressing the security challenges in RPL and developing effective countermeasures.Furthermore, the assessment of path stretch demonstrated that the attack affects the efficiency of the routing algorithm. The path stretch metric indicated that the actual paths taken by packets deviated from the optimal paths, causing suboptimal routing decisions and increased path lengths. This emphasizes the need for robust routing algorithms that can withstand attacks and maintain efficient path selection.Additionally, the measurement of power consumption highlighted the impact of the DIO suppression attack on energy efficiency. The attack increased power consumption due to the disruption of routing processes and potential retransmissions. Efficient energy usage is crucial in wireless sensor networks, and mitigating attacks like the DIO suppression attack can contribute to improved network longevity and sustainability. This is accomplished by the use of the DIO surrender, the subsequent storage of the surrender time, and the subsequent execution of the action through the calculation of the time difference between each message and a message from the same node in the sequence. a development environment so that we may put our solution into action, and when we did so, we implemented the proposed solution, which focuses on the detection of DIO suppression attacks, and we got a result that was satisfactory.

REFERENCES

[1] Alanhdi, A., et al. (2024). A survey on integrating edge computing with AI and IoT applications. *IEEE Internet of Things Journal*.

[2] Ali, S. M., Rahu, M. A., Karim, S., Jatoi, G. M., & Sattar, A. (2024). Internet of Things (IoT), applications and challenges: A comprehensive review. *Journal of Innovative Intelligent Computing and Emerging Technologies, 1*(1), 20–27.

[3] Allam, A. H., et al. (2024). IoT-based eHealth using blockchain technology: A survey. *Cluster Computing, 27*, 1–29.

[4] Balasbaneh, A. T., & Sher, W. (2026). A systematic literature review of Internet of Things (IoT) applications. *Sustainability, 18*(5), 2614.

[5] Burhan, M., Rehman, R., Khan, B., & Kim, B. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors, 18*, 2796–2812.

[6] Choudhary, A. (2024). Internet of Things: A comprehensive overview, architectures, applications, simulation tools, challenges and future directions. *Discover Internet of Things, 4*(31), 1–45.

[7] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

[8] Jara, A. J., Zamora, M. A., & Skarmeta, A. F. (2012). Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things. *Mobile Information Systems, 8*(3), 177–197.

[9] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The Internet of Things architecture, possible applications and key challenges. In *Proceedings of the 10th International Conference on Frontiers of Information Technology* (pp. 257–260).

[10] Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks, 28*, 68–90.

[11] Mu, X., Zhang, H., & Wang, L. (2024). The applications of Internet of Things (IoT) in industrial management: A science mapping review. *International Journal of Production Research, 62*(8), 2456–2478.

[12] Rahman, M., Hassan, K., & Islam, S. (2026). Realizing the potential of Internet of Things in industrial applications. *Discover Internet of Things, 6*(1), 1–20.

[13] Vermesan, O., & Friess, P. (Eds.). (2013). *Internet of Things: Converging technologies for smart environments and integrated ecosystems*. River Publishers.

[14] Wani, U. (2019). An introduction to IoT, its architecture and various protocols. *IEEE Conference Proceedings*.

[15] Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of Internet of Things. In *Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*.

[16] Xue, H., Chen, D., Zhang, N., Dai, H. N., & Yu, K. (2022). Integration of blockchain and edge computing in Internet of Things: A survey. *IEEE Open Journal*.

[17] Zhao, K., & Ge, L. (2013). A survey on the Internet of Things security. In *Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS)*.