ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

# "DIO SUPPRESSION ATTACK DETECTION BASED ON RPL AND IOT NETWORKS"

***Vaidehi Bakshi***
*Assistant Professor, Dr. C.V.Raman University Khandwa, M.P., India*
*Email: vaidehibakshi35@gmail.com*

## ABSTRACT

***Wireless sensor networks play a critical role in various applications, but they are vulnerable to attacks that can compromise network security and performance. One such attack is the DIO suppression attack, which targets the Routing Protocol for Low-Power and Lossy Networks (RPL). This research aims to analyze the impact of the DIO suppression attack on RPL and evaluate the effectiveness of the NLBGNDO algorithm in mitigating the attack. To achieve this objective, a simulation code is developed to accurately model the RPL protocol and incorporate the DIO suppression attack. The NLBGNDO algorithm, a proposed trustworthy and efficient routing algorithm for RPL, is integrated into the simulation code. Key metrics such as packet delivery ratio, path stretch, and power consumption are measured and analyzed under normal network conditions and during the attack. The results of the analysis provide insights into the vulnerabilities of RPL to the DIO suppression attack and the effectiveness of the NLBGNDO algorithm in mitigating its impact. The packet delivery ratio reveals the attack's effect on the network's ability to deliver data, while the path stretch metric indicates the efficiency of the routing algorithm under attack conditions.***

***Key Words:*** *IoT, RPL DIO suppression attack, NLBGNDO.*

## I. INTRODUCTION

The Internet of Things (IoT) has received a lot of attention over the past few years due to the fact that it might provide humans with an incredible amount of benefits. Kevin Ashton first presented the idea of the Internet of Things in 1999; its primary objective is to connect everything, at any time and in any location [1]. "Things" in the Internet of Things are imbued with the ability to sense, process, and take action, and they collaborate with one another to provide intelligent and cutting-edge services in an independent manner. The Internet of Things encompasses a wide variety of application fields, including but not limited to healthcare, home automation, environmental monitoring, and many more.The Internet of Things' fundamental goal is to bring together all of these different application fields under a single heading called "smart life." [2]. The Internet of Things is built so that it can handle a large number of different kinds of devices and use different kinds of communication methods. These technologies allow IoT devices to communicate with each other so that end users can get the services they need. This part is an introduction to some of the main ideas behind the Internet of Things (IoT). The Internet of Things (IoT) is explained, along with its possible uses and design, which includes the main components and protocols used in IoT. The term "Internet of Things" (IoT) refers to the next stage of growth for the internet, which will give machines and people a global way to connect.[3]The Internet of Things (IoT) is

ISSN : 2455-9679
SJIF Impact Factor : 6.008

a network of actual items, sometimes called "things," that have been equipped with sensors, software, and other technologies so that they can communicate and share data with other devices and systems through the internet. The name for this network is the "Internet of Things."[4] The concept and paradigm known as "the Internet of Things" recognizes the prevalence of numerous different objects that can communicate with one another and with other objects to develop new applications and accomplish shared objectives using wired and wireless connections as well as specific addressing schemes. [5]. the ability to connect things with anything and anybody at any time, in any location, and preferably utilizing any path, network, or service is the main objective of the Internet of Things.

The administrator is the one that configures the DODAG root node, which is the component that is in charge of building the comprehensive DODAG topology. Initially, the root node [6] determines the RPL instance ID, DODAGID, DODAG version number, base rank, objective function (OF), and routing cost, in addition to other information that is connected. The information is distributed to the surrounding nodes by the Sink node in the form of DIO control messages and is multicast. Neighboring nodes will extract and use the information they receive when they receive DIO messages to update their rank, to join DODAG, and based on their best rank, they will choose their preferred parent. Instantaneously, they communicate to their desired parent via DAO that they have entered the network by sending a message representing that they have joined the network. Each child node has a preferred parent, who acts as an intermediate node in the network and acts as a router between the child node and the root node. [7-9]

The root node is the most desirable parent for the network's initial hop nodes because it is the starting point for the whole network. The first hop nodes continue to send DIO signals in the direction of the downward hop, whereas the nodes that are receiving data send DAO messages upwards to the parent node that they like. Figure II.2 shows that the DODAG root (node 1) fills out the DIO control message with all of the necessary information, including its rank, and then multicasts the message to the other nodes in the network. After doing their own calculations and keeping the objective function in mind, neighbour nodes (5, 12, and 19) come to the conclusion that adding DODAG root as their preferred parent is the best option. As a result of their participation in DOADG, nodes 5, 12, and 19 multicast their DIO messages to their neighbours using rank 2. Within the DODAG, the rank goes from highest to lowest. The higher rank value indicating that the DIO is coming from downhill is the reason why the DODAG root ignores it when it comes from these nodes. If the node is within the radio range of the node 12, it has the ability to add nodes 5 and 19 as potential parents. Notably, all further downward nodes get DIO messages from several neighbouring nodes, but they choose a preferred parent that has the highest rank. This is an interesting phenomenon. The creation of topology will not be complete until all of the nodes have joined the DODAG.[10-11].

## II. RELATED WORK

**Amal Hkiri et.al. (2022)[12]** a fundamental communication standard for the Internet of Things, 6LoWPAN relies on the routing protocol for low power and lossy networks (RPL). RPL outperforms other wireless sensor and ad hoc routing protocols in terms of QoS, device management, and energy efficiency. However, various attacks may harm the network because of issues with unauthenticated or unencrypted control frames, centralised root controllers, hacked, or unauthenticated devices. As a result, the purpose of this study is to look into how attacks on the network architecture and resources can compromise the performance of RPL. For Resources attacks and Topology attacks, we'll be focusing on "Hello Flooding," "Increase Number," and "Decrease Rank." End-to-End Delay (E2ED), throughput, Packet Delivery Ratio (PDR), and average power consumption are some of the performance measures for RPL that were simulated to see how they might be affected by the three separate assaults. According to the results, all three attacks lead to an increase in E2ED, a drop in PDR and network throughput, and a degradation of the network's quality of service, all of which contribute to higher energy costs for the nodes in the network.

**Usha Kiran et.al. (2022)**[13] The Routing Protocol for Low Power and Lossy (RPL) Network is the most popular routing protocol used in the 6LoWPAN stack. However, there are a lot of holes in RPL's defences, both internally and externally, because of the lack of proper security measures. Much more study is needed to reveal RPL's limitations. Therefore, in this research, we begin by developing an implementation of the worst parent selection (WPS) attack. Second, we provide an IDS that can spot a WPS attack and alert you to it. By altering the victim node's objective

ISSN : 2455-9679
SJIF Impact Factor : 6.008

function, WPS makes it more likely that it will pick the worst node as its preferred parent. Nodes form the loop when a lower-ranking node chooses a parent with a higher rank, essentially cutting off numerous nodes from the rest of the network and preventing it from converging optimally. Furthermore, we suggest DWA-IDS as an IDS for discovering WPS assaults. The Contiki-cooja simulator is used for testing purposes. The simulation findings show that the WPS attack has a negative impact on system performance by lengthening the time it takes to send a packet. Our IDS is able to identify all simulated hostile nodes launching the WPS attack, as shown by the DWA-IDS simulation results. The proposed DWA-IDS has a true positive rate of over 95% and a detection rate of 100%. Due to the absence of a false-positive instance in our DWA-IDS, we also think about the proof in theory. DWA-IDS has a low enough setup overhead that even low-power and memory-constrained devices can use it.

## 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 utilised 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.

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.

**RPL (Routing Protocol for Low-Power and Lossy Networks)**

**RPL (Routing Protocol for Low-Power and Lossy Networks)** is a standardized routing protocol designed specifically for wireless networks with constrained resources, such as low-power devices and lossy links. It is primarily used in the context of Wireless Sensor Networks (WSNs) and Internet of Things (IoT) deployments. RPL provides a flexible and energy-efficient routing solution for networks with resource-constrained devices. It enables the establishment of routes among the network nodes, allowing efficient communication and data forwarding. RPL operates in a proactive manner, meaning that it builds and maintains routes in advance, ensuring timely and reliable delivery of packets[14]

**RPL suppression attacks** refer to a class of security threats aimed at disrupting the operation of the RPL (Routing Protocol for Low-Power and Lossy Networks) protocol. These attacks exploit vulnerabilities in RPL to hinder the routing service and potentially cause network disruptions or misbehavior. Here are two common RPL suppression attacks.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

**DIO Suppression Attack:** The DIO (DODAG Information Object) suppression attack targets the suppression of DIO messages within RPL. DIO messages are essential for building and maintaining the routing topology in RPL. In this attack, the adversary induces victim nodes to suppress the transmission of DIO messages, leading to a degradation of the routes' quality. This can result in network partitioning and disruption of communication within the network. Unlike other RPL attacks, the DIO suppression attack doesn't require forging bogus RPL messages. Instead, the attacker periodically replays previously heard messages to make victim nodes believe the routing information they are about to send is already being transmitted multiple times by other nodes.

**DAO Suppression Attack**

The DAO (Destination Advertisement Object) suppression attack focuses on suppressing DAO messages in RPL. DAO messages are used by nodes to advertise their presence and available services within the network. By suppressing DAO messages, an attacker can hinder the dissemination of routing information, leading to disrupted or inefficient routing in the network. This can result in communication failures, increased latency, and decreased network performance. The DAO suppression attack may exploit vulnerabilities in the forwarding process or target specific nodes to prevent them from broadcasting DAO messages.

The DIO (DODAG Information Object) suppression attack is a novel type of degradation-of-service attack specifically targeting the RPL (Routing Protocol for Low-Power and Lossy Networks) protocol. It aims to disrupt the routing service provided by RPL, potentially leading to network partitioning and degradation of routing efficiency.

In the DIO suppression attack, the adversary's goal is to induce victim nodes in the network to suppress the transmission of DIO messages. DIO messages play a crucial role in RPL as they carry important information for building and maintaining the routing topology. By suppressing DIO messages, the attacker disrupts the network's ability to establish and update routes, resulting in a degradation of the quality of available routes.

What sets the DIO suppression attack apart from other attacks against RPL is that it doesn't require the adversary to forge bogus RPL messages. Instead, the attacker leverages the replay technique by periodically replaying previously heard DIO messages. This makes victim nodes believe that the routing information they are about to send is already being transmitted multiple times by other nodes.

The DIO suppression attack takes advantage of the victim nodes' trust in the routing information received from their neighbors. By convincing the victims that the routing information is already being propagated, the attacker disrupts the normal functioning of the routing protocol without the need to steal cryptographic keys or forge messages.

The consequences of the DIO suppression attack can be severe. It degrades the quality of routes, potentially leading to increased latency, packet loss, and network partitions. This attack can impact the reliability and performance of IoT systems and wireless sensor networks that rely on RPL for efficient communication. To mitigate the DIO suppression attack and enhance the security of RPL, research efforts focus on developing intrusion detection mechanisms, secure message authentication, anomaly detection techniques, and improved cryptographic mechanisms. These countermeasures aim to detect and prevent the suppression of DIO messages, ensuring the robustness and reliability of the RPL protocol in the face of such attacks.

**DIO Algorithm**

The DIO (DODAG Information Object) is an essential message in the RPL (Routing Protocol for Low-Power and Lossy Networks) protocol that carries information about the network's topology and configuration. While the exact DIO algorithm may vary based on the specific implementation or objective function used in RPL, I can provide a general overview of the DIO algorithm and its mathematical expressions.

**Rank Calculation:**The rank calculation in the DIO algorithm determines the position of a node in the network's routing hierarchy. The mathematical expression for rank calculation can be based on various metrics and constraints. One possible mathematical expression for rank calculation is:

**Rank = BaseRank + (RankFactor * Metric)**

Here, BaseRank represents a constant base rank value assigned to the root node, RankFactor is a parameter that scales

ISSN : 2455-9679
SJIF Impact Factor : 6.008

the metric value, and Metric represents a specific metric used for rank calculation (e.g., hop count, energy, or link quality). The RankFactor can be adjusted to reflect the importance of the metric in the routing decision.

**Objective Function:**The DIO algorithm may utilize an objective function to evaluate and compare different routes based on specific metrics and constraints. The objective function can be represented by a mathematical expression that combines different parameters and weights them accordingly. For example:

**Objective Function = (Weight1 * Metric1) + (Weight2 * Metric2) + ... + (WeightN * MetricN)**
Here, Weight1 to WeightN represent the weights assigned to each metric, and Metric1 to MetricN represent the specific metrics used in the objective function (e.g., energy consumption, latency, or link quality).

**Trickle Timer:**The DIO algorithm employs a trickle timer mechanism to control the frequency of DIO message transmission. The trickle timer is based on mathematical expressions and randomization to determine the intervals between DIO message transmissions. The exact mathematical expression for the trickle timer depends on the specific implementation. However, it typically involves variables such as minimum interval, maximum interval, and a random backoff factor to introduce randomness and avoid message collisions

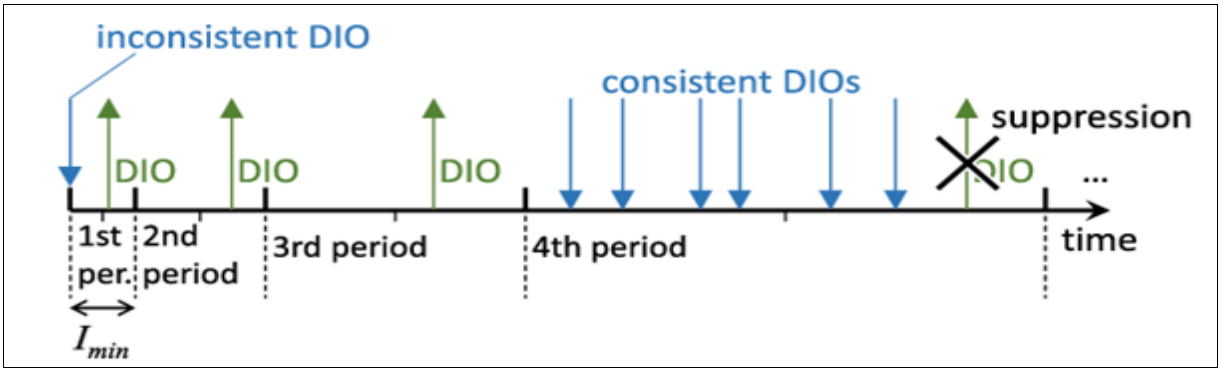


Fig.1 timer mechanism

**(NLBGNDO**
To solve the challenge of determining the best route through a network, the Non-Linear Brownian Generalised Normal Distribution Optimisation (NLBGNDO) algorithm is developed.This algorithm utilizes a combination of non-linear optimization, Brownian motion, and the generalized normal distribution to optimize the path selection process.

**NLBGNDO algorithm**
The NLBGNDO algorithm aims to improve the efficiency and effectiveness of routing by considering various factors such as energy consumption, latency, link quality, or path length. By incorporating non-linear optimization techniques, it can better adapt to the specific requirements and constraints of the network.
Additionally, the algorithm leverages Brownian motion, which is a random process that models unpredictable movements, to explore the search space. This random behavior helps in efficiently exploring different paths and finding better solutions.
The generalized normal distribution is employed to model the probability density function of the variables involved in the optimization process. This distribution allows for controlling parameters related to skewness and kurtosis, which can be advantageous in optimizing the routing paths based on specific metrics.
By integrating these techniques, the NLBGNDO algorithm aims to provide an improved solution for finding the optimal path in a network, considering multiple objectives and constraints. However, without further specific details or implementation guidelines, it is not possible to provide a more detailed description of the algorithm

ISSN : 2455-9679
SJIF Impact Factor : 6.008

## IV. RESULT DISCUSSION

The focus is on proposing a novel algorithm called NLBGNDO (Non-Linear Brownian Generalized Normal Distribution Optimization) 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.

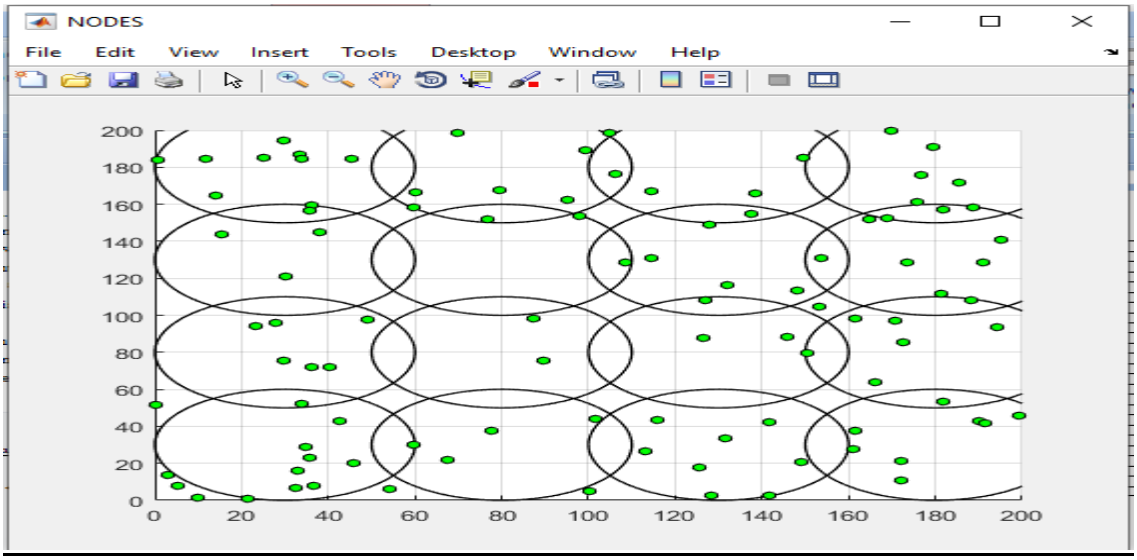



**Fig.2 initial network**

Set up the original network's parameters and copy its node count. Initial network dimensions are depicted in Figure 2 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.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

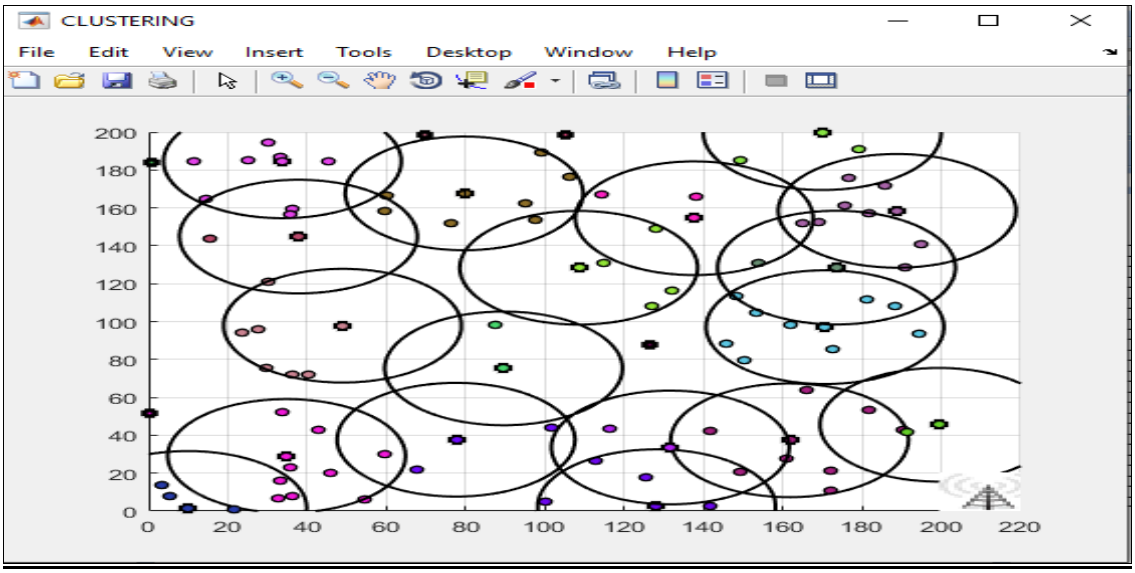



Fig 3 Cluster Head

The WSN partitions each cluster, and the administrator (cluster head) of each cluster is in charge of gathering information from the nodes in their cluster and transmitting it to the receiver (base station).

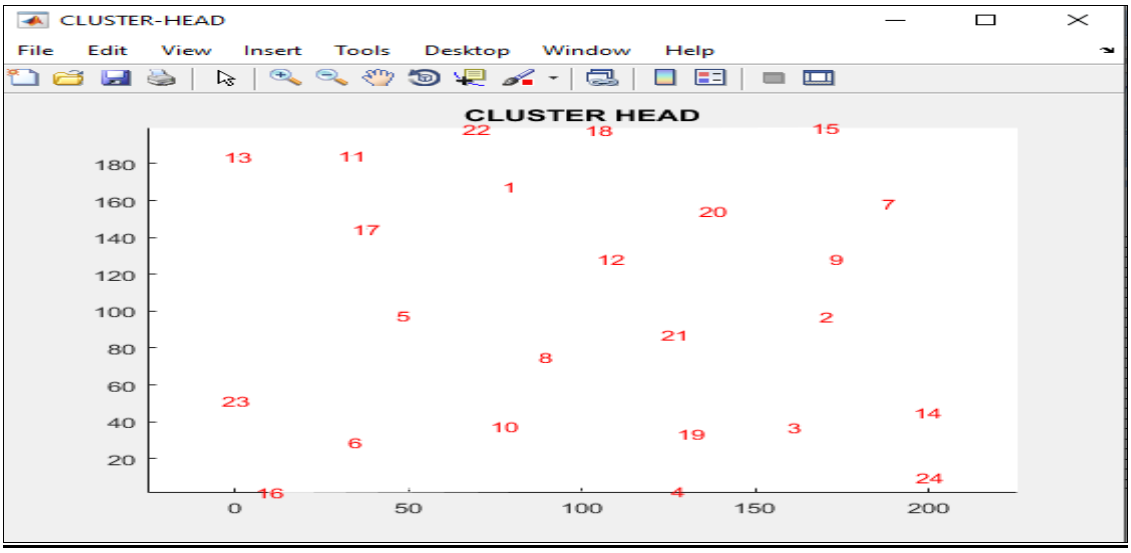



Fig 4 number of cluster head

Figure 4 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.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

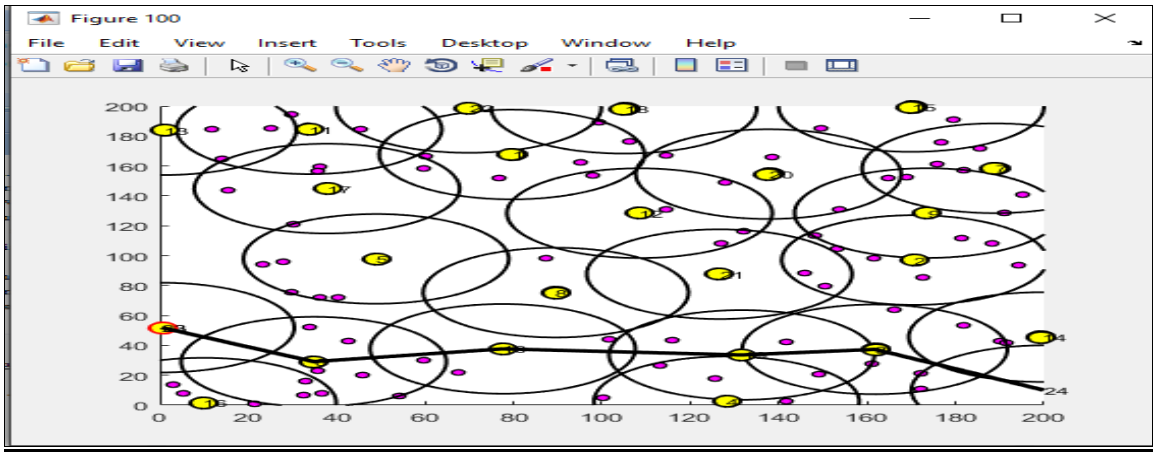



Fig.5 node finds the optimum path in the network

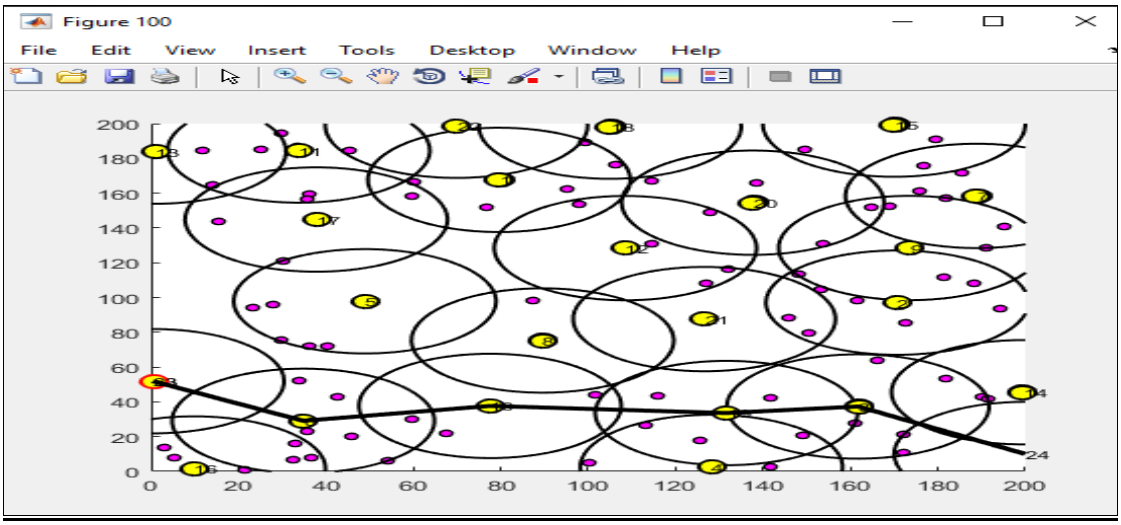



Fig.6 node searching path in the network to secure communication

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

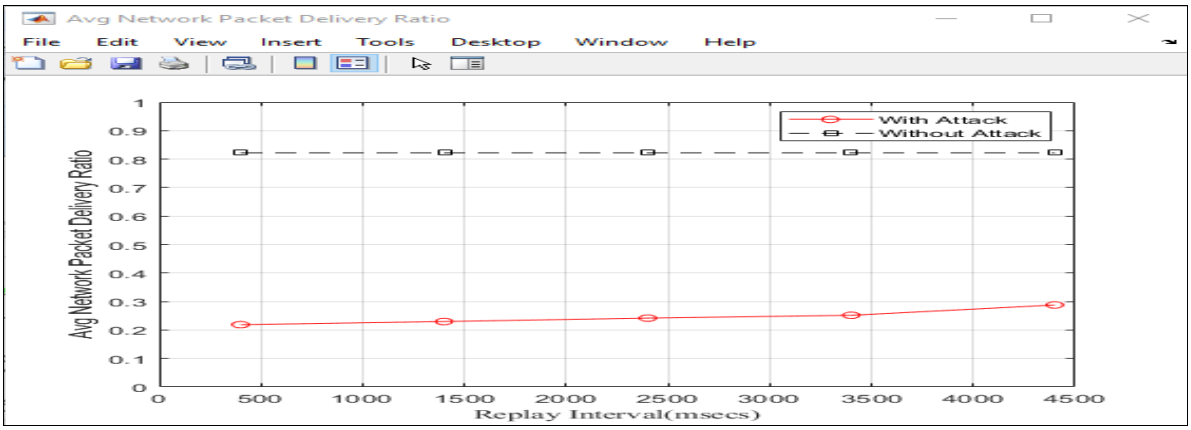



fig. 7Average network packet delivery ratio

ISSN : 2455-9679
SJIF Impact Factor : 6.008

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

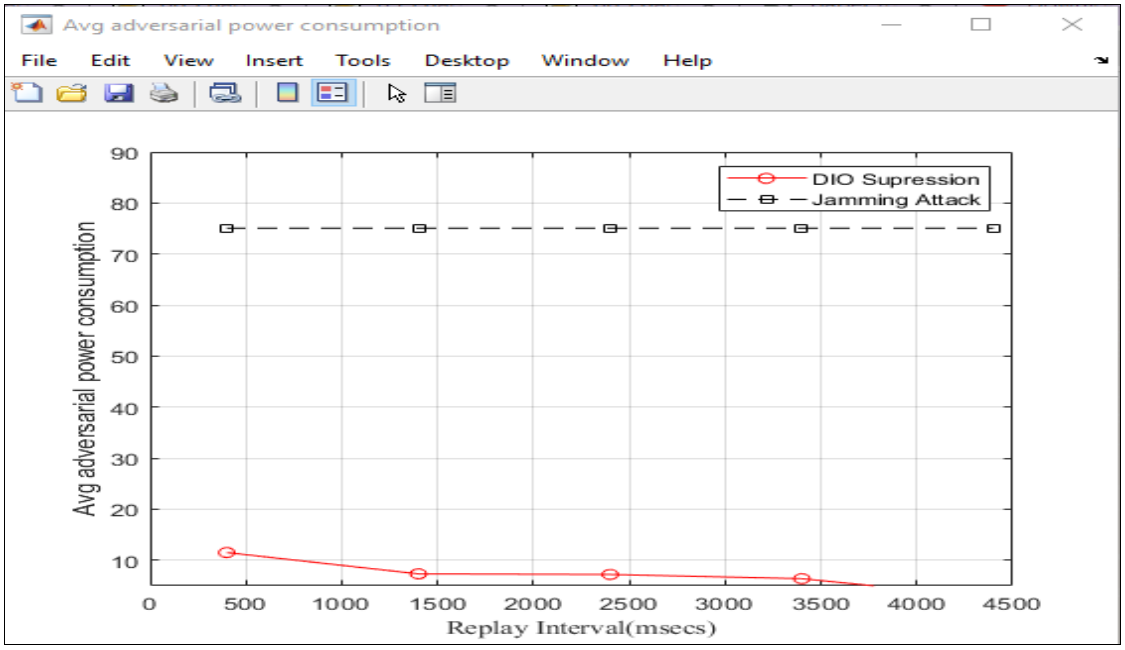



Fig.8 Average adversarial power consumption

The average amount of poer 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.

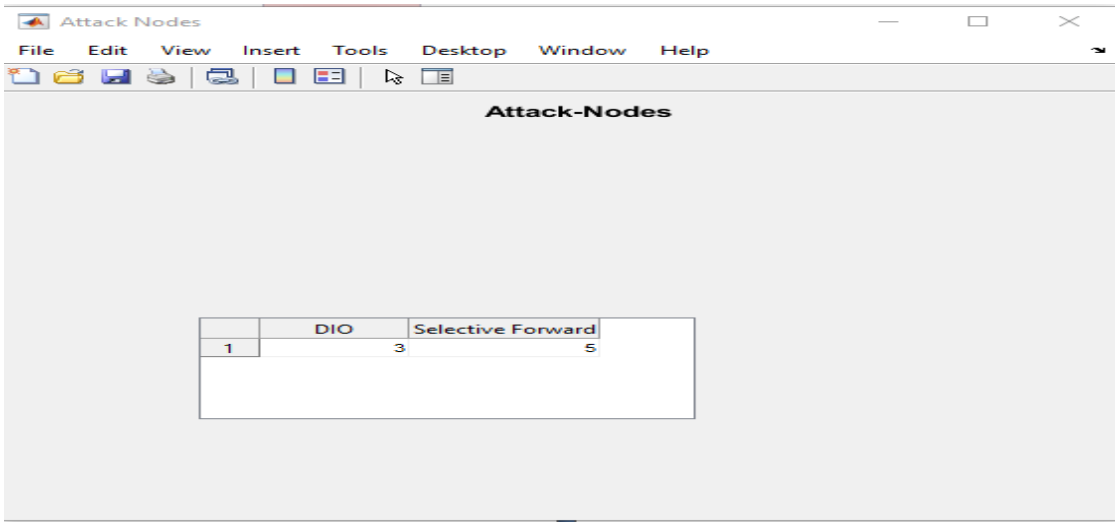
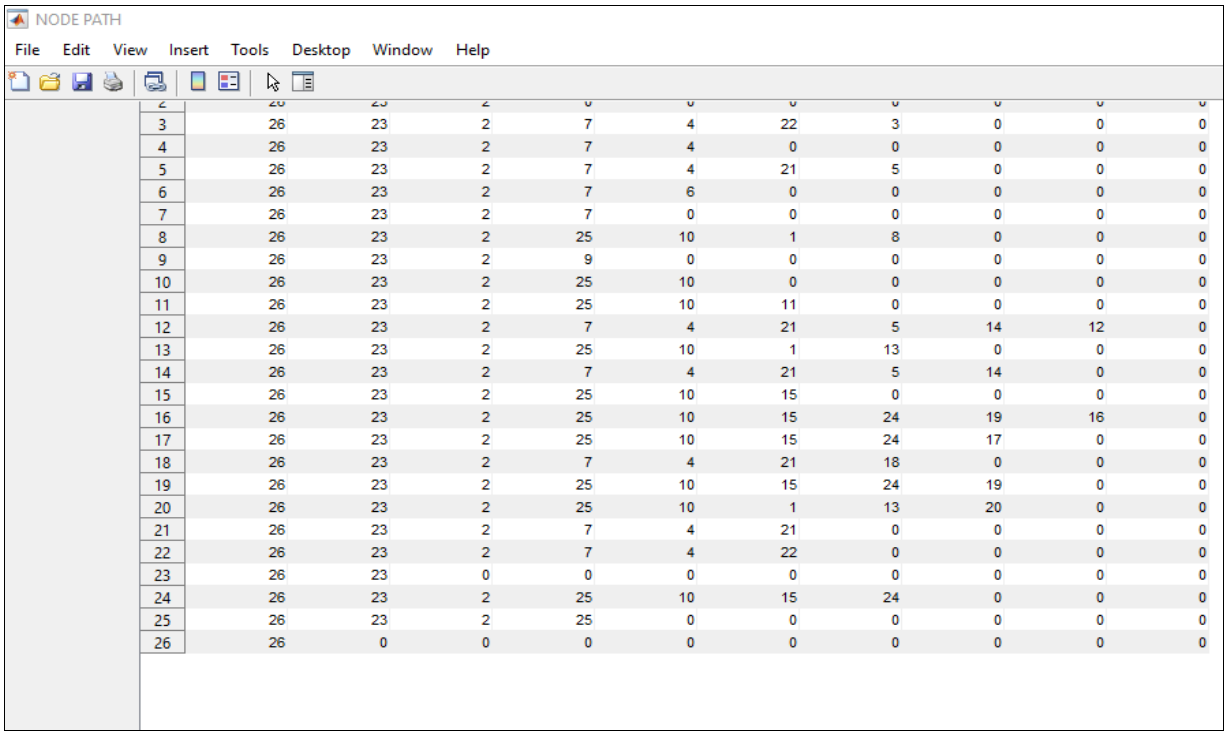



Fig. 9 DIO attack

ISSN : 2455-9679
SJIF Impact Factor : 6.008

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. 10 Node path table

## V. CONCLUSION

In this chapter, we discussed the core of our research, which is about a security mechanism for RPL communications in the IoT. We also explained the suggested detection approach for DIO suppression attacks in RPL-based networks, and we evaluated the performance of our detection method based on experiments. The findings demonstrated that the detection approach possesses very strong performance: high detection rates (100%) and low false alarm rates (less than 10%) across the board. The Internet of Things (IoT) has quickly become an indispensable component of our lives in this day and age. There are billions of intelligent and autonomous beings all around the world that are connected to each other and can communicate with one another. The Internet of Things is a system that connects intelligent and self-sufficient devices through the use of various wireless communication technologies. These things are able to gather information, analyse it, process it, create new information, and share it with other things so that more sophisticated services can be provided. RPL was selected as the actual routing protocol to solve the limits of LLN networks from low processing power and battery and memory. Because wireless networks have numerous limitations, such as power and memory, which makes routing in them hard, RPL was selected as the actual routing protocol. However, RPL is susceptible to a wide variety of attacks that are connected to cross-control communications. To enhance the safety and functionality of the RPL protocol, the following document proposes an algorithm that is able to recognise a DIO suppression attack and recognise rogue nodes.

This is based on the DIO surrender, storing the surrender time, and then executing the action by calculating the time difference between each message and a message from the same node in the sequence. a development environment to implement our solution and after we implemented the proposed solution, which lies in detection of DIO suppression attack and we came to a satisfactory result.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

## REFERENCES

[1] Ge Guo A Lightweight Countermeasure toDIS Attack in RPL Routing Protocol 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)Year: 2021

[2] Eric Garcia Ribera;Brian Martinez Alvarez;Charisma Samuel;Philokypros P. Ioulianou;Vassilios G. Vassilakis Heartbeat-Based Detection of Blackhole and Greyhole Attacks in RPL Networks 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP) Year: 2020 |

[3] Ruchi Mehta;M.M. Parmar Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole &Grayhole Attacks 2018 3rd International Conference for Convergence in Technology (I2CT) Year: 2018

[4] Abdul Rehman;Meer Muhammad Khan;M. Ali Lodhi;Faisal Bashir Hussain Rank attack using objective function in RPL for low power and lossy networks 2016 International Conference on Industrial Informatics and Computer Systems (CIICS) Year: 2019 |

[5] Syeda Mariam Muzammal;Raja Kumar Murugesan;Noor Zaman Jhanjhi;Low Tang Jung SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications 2020 International Conference on Computational Intelligence (ICCI)

[6] Anhtuan Le;Jonathan Loo;Yuan Luo;Aboubaker Lasebae Specification-based IDS for securing RPL from topology attacks 2011 IFIP Wireless Days (WD) Year: 2019 |

[7] Wijdan Choukri;Hanane Lamaazi;Nabil Benamar RPL rank attack detection using Deep Learning 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT) Year: 2020

[8] David Airehrour;Jairo Gutierrez;Sayan Kumar Ray A testbed implementation of a trust-aware RPL routing protocol 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) Year: 2019 |

[9] Faraz Idris Khan;Taeshik Shon;Taekkyeun Lee;Kihyung Kim Wormhole attack prevention mechanism for RPL based LLN network 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN) Year: 2020 |

[10] Fatima-tuz-Zahra;NZ Jhanjhi;Sarfraz Nawaz Brohi;Nazir A. Malik;Mamoona Humayun Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning 2020 2nd International Conference on Computer and Information Sciences (ICCIS) Year: 2020 |

[11] Abhay Deep Seth;Santosh Biswas;Amit Kumar Dhar Detection and Verification of Decreased Rank Attack using Round-Trip Times in RPL-Based 6LoWPAN Networks 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) Year: 2020 |

[12] Amal Hkiri;Mouna Karmani;Mohsen Machhout The Routing Protocol for low power and lossy networks (RPL) under Attack: Simulation and Analysis 2022 5th International Conference on Advanced Systems and Emergent Technologies (IC_ASET) Year: 2022 |

[13] Usha Kiran IDS To Detect Worst Parent Selection Attack In RPL-Based IoT Network 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS) Year: 2022

[14] Haitham Y. Adarbah;Mostafa Farhadi Moghadam;Rolou Lyn Rodriguez Maata;Amirhossein Mohajerzadeh;Ali H. Al-Badi Security Challenges of Selective Forwarding Attack and Design a Secure ECDH-Based Authentication Protocol to Improve RPL Security mIEEE Access Year: 2023.