International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Performance Evaluation of DIO Suppression Attacks in RPL-Based IoT Networks

Dr. Anjali Khokhar
Assistant professor, BITS Engineering college, Bhiwani
Email id -ashu.ishu34@gmail.com

Abstract

Wireless Sensor Networks (WSNs) play a crucial role in a wide range of applications; however, their open and resource-constrained nature makes them vulnerable to various security attacks, which can significantly degrade network performance and reliability. One such attack is the DIO suppression (silencing) attack, which specifically targets the Routing Protocol for Low-Power and Lossy Networks (RPL). This study aims to investigate the impact of the DIO suppression attack on RPL performance and to evaluate the effectiveness of the NLBGNDO routing algorithm in mitigating this attack. To achieve this objective, a detailed and accurate model of the RPL protocol and the DIO suppression attack is developed within a simulation-based modeling framework. The proposed framework integrates the NLBGNDO algorithm, which is designed to enhance routing security and efficiency in RPL-based networks. Key performance metrics including packet delivery ratio, route stretch and energy consumption are measured and analyzed under both normal network conditions and attack scenarios. The results provide critical insights into the vulnerability of RPL to DIO suppression attacks and demonstrate the capability of the NLBGNDO algorithm to reduce their adverse effects. Specifically, the packet delivery ratio reflects the impact of the attack on data transmission reliability, while the route stretch metric evaluates routing efficiency under malicious conditions.

Keywords: IoT, RPL DIO suppression attack, NLBGNDO

Introduction

Over the past few years, the Internet of Things (IoT) has gained significant attention due to its possibility to provide extensive positive effects in different spheres of human life. Kevin Ashton was the first person to present the concept of the Internet of Things in 1999 and focused more on the vision of a scenario where physical objects integrate fully with each other. The main aim of the IoT is to provide the ability to connect devices, systems and services anywhere and at any time and exchange data and communicate intelligently on a worldwide scale [1]. Things in the Internet of Things (IoT) paradigm have the ability to sense, process, and act on the surrounding environment and, interacting with each other in an autonomous way, they provide intelligent and innovative services. IoT technologies are very common in various applications such as in healthcare systems, homes automation, monitoring of the environment and numerous other areas. The long-term goal of the Internet of Things is to bring these heterogeneous applications together on a unified platform otherwise known as the smart life, where tied-togethers will make all systems more efficient, convenient and comfortable to live [2]. Internet of Things (IoT) is also supposed to work with as many heterogeneous devices and communication technologies as possible, which allows a smooth communication between disparate systems. These technologies enable the IoT devices to communicate with each other in order to provide the user with the necessary services in a cost-effective manner. Here, the basic concepts of the Internet of Things are described, its definition, possible utilization, and architecture. The IoT architecture includes the important components and communication protocols, which facilitate the interoperability and scalability. The Internet of Things is viewed as the step of further evolution of the Internet, which allows uniting the physical objects and human communication of the globe together. Essentially, IoT can be described as a network of physical entities popularly referred to as things that have sensors, software and other technologies that enable them to gather, share and analyze data with other devices and systems via the Internet [4]. Internet of Things (IoT) is a theoretical paradigm that acknowledges interactions between various physical objects that can communicate with and interact with others and the external environment to create innovative applications and pursue shared goals. This communication is facilitated by the wired and wireless communication technologies and backed by special addressing plans which guarantee smooth identification and data transfer between the connected devices [5]. The main goal of the Internet of Things (IoT) is to make the connection between the objects, systems and people to be seamlessly connected, through any form of communication technology, network and possibly any way, everywhere and at any moment. The network administrator in RPL based networks is tasked with the responsibility of configuring the DODAG root node which will serve as a hub in configuring and maintaining the full DODAG structure. In the initialization stage, the root node defines the necessary RPL parameters: the RPL instance ID, the DODAG ID, DODAG version number, the base rank, objective function (OF) and routing cost among others. This data is shared with the adjacent nodes by multicast DODAG Information Object (DIO) control messages. When the neighboring nodes get the DIO messages, they process the information in order to update their rank values, enter the DODAG structure and choose a preferred parent on the basis of the best rank. Once a node has become a part of the network, it instantly informs its chosen parent by sending a Destination Advertisement Object (DAO) message, which it means it is a part of the routing topology. In this hierarchical routing model, every child node has a preferred parent which acts as a forwarding node in the middle and thus, a communication path is created between the child node and the root node. [7-9].

The root node is a special node because it is the source of the whole network topology; therefore, it is the favorite parent of all the first-hop nodes. These first-hop nodes constantly send DODAG Information Object (DIO) packets to the lower level nodes and those having successfully joined the network send Destination Advertisement Object (DAO) packets to the parent nodes. As shown in Figure II.2, the DODAG root (Node 1) produces and propagates DIO control messages with all the required routing information whose rank is included to other network nodes. On the receipt of these messages, the neighbor nodes like Nodes 5, 12 and 19 compute the information based on the objective function and decide that the root node is the parent of their choice offering the best path to follow. Once these nodes become part of the DODAG, they choose a rank value of 2 and then send network communication messages about themselves as DIO to other nodes around them. The values of rank of the nodes in the DODAG hierarchy increase as the nodes get farther away in the hierarchies and the root node does not pay attention to the DIO messages sent by the lower-ranked nodes (which are downward in the hierarchies). Nodes that are within the communication range of Node 12 can use Nodes 5 and 19 as their parent candidate. Though, interestingly enough, nodes further down the topology are normally sent several DIO messages by their neighbors, nodes choose their parent of choice as the one with the best rank as calculated by the objective function. The construction process of DODAG is repeated until all the network nodes are connected to the DODAG structure successfully. [10-11].

II RELATED WORK

Amal Hkiri et.al. (2022) [12] The Routing Protocol for Low-Power and Lossy Networks (RPL) serves as the core routing mechanism of **6LoWPAN,** which is a fundamental connectivity standard for the Internet of Things (IoT). Compared to conventional wireless sensor and ad hoc routing protocols, RPL provides improved Quality of Service (QoS), enhanced device management and greater energy efficiency. However, the protocol is susceptible to various security threats arising from unauthenticated or unsecured control messages, centralized root management, compromised nodes and unverified devices. Consequently, the objective of this study is to investigate the impact of attacks targeting network architecture and resource availability on the performance of RPL. In particular, the analysis focuses on resource-based and topology-based attacks, including **Hello Flooding, Rank Increase and Rank Decrease** attacks. Key performance metrics such as End-to-End Delay (E2ED), throughput, Packet Delivery Ratio (PDR) and average energy consumption are evaluated to assess the effects of these attacks. The results reveal that all three attack scenarios lead to increased end-to-end delay, reduced packet delivery ratio and throughput, degradation of network Quality of Service and increased energy consumption among network nodes.

Usha Kiran et.al. (2022)[13] The Routing Protocol of the Low-Power and Lossy Networks (RPL) is the most popular routing protocol of the 6LoWPAN protocol stack. Nevertheless, because of the lack of strong security provisions, RPL has a number of internal and external vulnerabilities, which means that future research into the security drawbacks of this framework is necessary. To examine the effects of the Reverse Path Multicast (RPL) networks, in this work, an implementation of the Worst Parent Selection (WPS) attack is first created. Then, a proposed Intrusion Detection System (IDS) is suggested to identify and warn about WPS attacks. WPS attack works with the objective function of RPL in such way that it enhances the probability of a target node choosing the unsuitable or malicious parent. This causes routing loops where a node of lower rank selects a parent node of high rank causing partitioning of the network and inefficient topology construction. In this case, an effective WPS attack detection is suggested by proposing a Dynamic Weight Adjustment Intrusion Detection System (DWA-IDS). Experimental evaluation is done with the Contiki-Cooja simulation environment. The findings indicate that the WPS attack has severe consequences on network performance because it results in file transmission delays. In addition, the analysis of DWA-IDS provides that the suggested IDS is effective at detecting all simulated malicious nodes that start the WPS attack with the detection rate of 100 percent and true positive rate of above 95 percent. Theoretical validation is also given since no false positives were obtained. The proposed DWA-IDS is resource-efficient in terms of computational and memory, which makes it suitable to be implemented in IoT devices that have a limited resource capacity.

III PROPOSED SYSTEM

In a DIO silencing (suppression) attack, the adversary forces target nodes to cease transmitting DODAG Information Object (DIO) messages. Since DIO messages play a critical role in constructing and maintaining routing structures in RPL, suppressing these messages significantly degrades route quality and may eventually lead to network partitioning. Unlike many previously studied attacks, the DIO suppression attack does not require the generation of forged RPL control messages. Instead, the attacker repeatedly replays previously overheard DIO messages, enabling the attack to be executed without compromising cryptographic keys of legitimate nodes. This attack exploits the replay technique, a commonly used attack strategy, in a novel manner. Rather than deceiving nodes into accepting outdated information as new, the replayed messages mislead target nodes into believing that the routing information they intend to transmit has already been sufficiently disseminated by neighboring nodes. Experimental analysis demonstrates that the DIO silencing attack severely deteriorates the routing service provided by RPL. Moreover, the results indicate that this attack consumes less energy than conventional blocking attacks proposed in earlier studies. Despite its lower energy requirement, the DIO suppression attack produces comparable negative effects on network performance, allowing the adversary to disrupt routing operations more efficiently. The significant impact of the DIO silencing attack highlights critical security weaknesses in RPL-based networks and emphasizes the need for enhanced security mechanisms in IoT systems. By identifying and analyzing this attack, the study contributes to ongoing efforts to develop robust and secure routing protocols for Wireless Sensor and Actuator Networks (WSANs), thereby ensuring the reliability and efficient operation of IoT networks.

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

RPL (Routing Protocol for Low-Power and Lossy Networks) Routing Protocol Low power and Lossy Network (RPL) Routing protocol is a standardized routing protocol that is specially created to support wireless connections based on resource-constrained devices that use unreliable and lossy communications. It is commonly applied to Wireless Sensor Networks (WSNs) and Internet of Things (IoT). RPL provides a routing mechanism, which is flexible and uses less energy based on the constraints of low-power devices. The protocol allows the systematic creation and maintenance of the routing paths between the network nodes, which allows efficient data transport and communication. RPL works proactively, which means that routing structures are built and constantly updated beforehand, after which the delivery of packets over the network is realized in time, reliably and consistently. [14]

RPL suppression attacks are a form of security threats that aims at disrupting the regular functionality of the Routing Protocol of Low-Power and Lossy Networks (RPL). These attacks take advantage of default flaws in the protocol to cause disruption in routing functions resulting in poor performance, routing anomalies or even network outage. Such attacks can lead to misbehavior in the network by repressing vital control messages or by manipulating routing choices. There are two popular forms of RPL suppression attack and are listed below:

DIO Suppression Attack: The DIO (DODAG Information Object) suppression attack is the attack that specifically attacks the DIO control messages suppression in the RPL protocol. Because DIO messages are vital to building and maintaining the routing topology of RPL, their inhibition seriously affects the quality of the routes and the overall performance of the network. This attack can result in network partitioning and disconnection of communication between nodes by deterring the frequent spread of routing information. The DIO suppression attack is not based on the creation of forged RPL control messages as many other RPL attacks. Rather, the opponent re-plays earlier heard messages of DIO on a periodic basis, which makes the victim nodes believe that sufficient propagation of routing information they wish to send has already occurred by the neighboring nodes.

DAO Suppression Attack

The denial attack of DAO (Destination Advertisement Object) is aimed at the suppression or blocking of the RPL messages of DAO. Nodes communicate with other nodes on the network through advertisement messages known as DAO messages, which inform the other node about their presence, reachability and available services. By blocking the transmission of the DAO messages, the assailant interferes with the process of sharing routing information, which results into routing inconsistencies and poor network performance. Such disturbance can cause communication breakdowns, add latency, and decrease throughput and general worsening of network performance. The DAO denial attack can use the vulnerabilities of the routing procedure or forcefully attack certain nodes to deny them the opportunity to send the DAO messages. DODAG Information Object (DIO) suppression attack is a type of degradation-of-service attack which targets the RPL routing protocol. It is mainly aimed at disrupting routing service of RPL, which can lead to partitioning of the network and a substantial deterioration of the performance. The attacker in this type of attack causes the victim machines to cease to send messages of the form of DIO which are required to create and sustain the routing topology. The attacker prevents route setup and adaptation by inhibiting such control messages, which leads to low quality routes. In contrast with other RPL attacks, the DIO suppression attack does not demand for the generation of forged RPL control messages and the cracking of cryptographic keys. Rather, the attacker makes use of a replay approach, whereby already received DIO messages have been replayed. This causes a confusion of target nodes that the routing information they are about to broadcast has already been adequately distributed by the neighboring nodes. The success of DIO suppression attack depends on the confidence that the nodes have into routing information that is received by their neighbors. Using this trust, the attacker will be able to interfere with the normal functionality of the routing protocol without causing any false messages. The effects associated with this attack are worsening of route quality, augmented delay of packets, amplified packet loss and in the extreme scenario, network fragmentation. These impacts have a great negative effect on the performance and stability of IoT systems and Wireless Sensor Networks that use RPL to ensure effective communication. In order to reduce the DIO suppression attacks and the security of RPL, the current studies aim at intrusion detection schemes, secure message authentication, anomaly detection strategies as well as better cryptographic schemes and practices. These countermeasures will be used to ensure that the DIO messages are not silenced and that the RPL protocol is resistant and reliable against any adversarial threat.

DIO Algorithm

The **DODAG Information Object (DIO)** is a fundamental control message in the Routing Protocol for Low-Power and Lossy Networks (RPL) that disseminates information related to network topology and configuration. While the specific operation of the DIO algorithm may vary depending on the application requirements or the objective function employed in RPL, a general outline of the DIO mechanism and its associated mathematical formulations can be described.

Rank Calculation: In the DIO mechanism, **rank calculation** determines the position of a node within the routing topology of the network. The computation of rank depends on the selected objective function and may incorporate various routing metrics and constraints. Accordingly, the mathematical expression used to calculate a node's rank can be formulated in different ways based on the chosen routing criteria. One possible mathematical representation for rank calculation is as follows:

Rank = BaseRank + (RankFactor * Metric)

In this formulation, **BaseRank** represents a fixed reference rank assigned to the root node, while **RankFactor** is a scaling parameter applied to the selected routing metric. The **Metric** denotes the specific parameter used for rank computation, such as hop count, residual energy, or link quality. The RankFactor can be adjusted to reflect the relative importance of the chosen metric in determining routing decisions and packet forwarding behavior.

Objective Function: The DIO mechanism may employ an **objective function** to evaluate and compare multiple routing paths based on specific metrics and constraints. This objective function can be mathematically expressed as a weighted combination of different factors, where each metric is assigned a corresponding weight to reflect its relative importance in the routing decision process. For example, the objective function can be represented as follows:

Objective Function = (Weight1 * Metric1) + (Weight2 * Metric2) + ... + (WeightN * MetricN)

Here, **Weight_1 to Weight_n** denote the weighting coefficients assigned to each routing metric, while **Metric_1 to Metric_n** represent the specific parameters considered in the objective function, such as energy consumption, latency, or link quality.

Trickle Timer: The **Trickle timer** is employed by the DIO mechanism to regulate the transmission frequency of DIO messages. It utilizes mathematical formulations and probabilistic techniques to determine the time interval between successive DIO transmissions. Although the exact numerical expression of the Trickle timer depends on its specific implementation, it generally incorporates parameters such as a minimum interval, a maximum interval and a randomized backoff factor. These elements introduce controlled randomness into message scheduling, helping to reduce transmission collisions and minimize redundant control traffic.

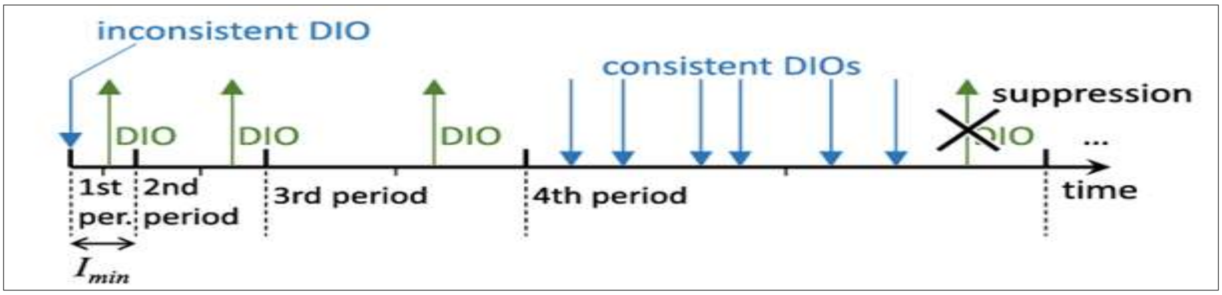


fig.1 timer mechanism

(NLBGNDO

The **Non-Linear Brownian Generalised Normal Distribution Optimisation** (NLBGNDO) method is designed to determine optimal routing paths within a network. This approach integrates principles of non-linear optimization, Brownian motion and the generalized normal distribution to efficiently explore the solution space and identify the most optimal routing paths.

NLBGNDO algorithm

The NLBGNDO algorithm focuses on optimizing routing performance and effectiveness by taking into account several performance aspects at the same time including energy consumption, delay, link quality and path length. The algorithm is dynamically adjusted to the constraints and needs of the network by using non-linear methods of optimization. Also, the algorithm will use Brownian motion, a stochastic process, which simulates random and unpredictable movements, to search the search space more efficiently. This is randomness that prevents the presence of local optima and allows finding better routing solutions.

In the course of optimization, the generalized normal distribution is applied in modeling the probability density functions of the parameters involved. The benefit of this distribution is that skewness and kurtosis are less controlled, which is important in modeling network conditions more closely and finding the best routing paths in networks by choosing performance metrics. The NLBGNDO algorithm incorporates the concept of non-linear optimization, Brownian motion modelling, and generalized normal distribution modelling, to offer a powerful multi-objective routing framework which is able to determine the best routes by meeting all the different network constraints.

IV RESULT DISCUSSION

The main aim of the given study is to present a new optimization model, which could be called NLBGNDO (Non-Linear Brownian Generalised Normal Distribution Optimisation), to solve the task of optimal route choice between the source and destination sensing nodes in the networks based on RPL. The suggested approach will guarantee high-quality routing and low-latency routing despite the occurrence of DIO suppression attacks. An immense amount of simulation is done to assess the effectiveness of the approach with a computational model which identifies optimum routing paths and reduces delay under adversarial conditions. The efficiency of the suggested approach is evaluated based on a number of major findings, which are listed and elaborated on the following.

Packet Delivery Ratio: The performance is evaluated by the Packet Delivery Ratio (PDR) which is a ratio of successfully delivered packets in relation to the amount of packets delivered. This measure is employed to determine the quality and efficiency of the suggested approach in sustaining the successful delivery of packets even when there is the presence of DIO suppression attacks.

Path Stretch with and Without Attack: Path stretch is the growth of the length of the routing path as compared to the optimum or shortest path. Path stretch is assessed in the simulation study in both the normal and attack conditions. This measure gives useful information on how well the suggested algorithm can maintain routing efficiency and limit the path elongation even with a DIO suppression attack.

Power Consumption: Power consumption is a critical performance metric in resource-constrained environments such as Wireless Sensor Networks (WSNs) and Internet of Things (IoT) systems. Accordingly, the simulation framework incorporates power consumption measurements to evaluate the energy efficiency of the proposed algorithm under both normal operating conditions and DIO suppression attack scenarios.

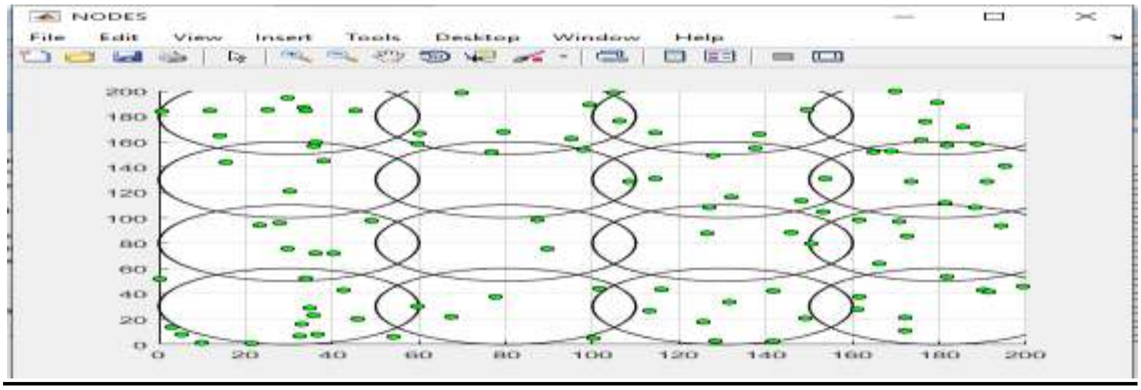


Fig.2 initial network

The initial network parameters are configured to replicate the original network setup, including the same number of nodes. As illustrated in Figure 2, the network area is defined with dimensions of 200 meters in length and 200 meters in sensing region width (cluster width). The network employs a communication radius of 30 meters This study proposes an effective method for detecting DIO suppression attacks in RPL-based networks and evaluates its performance through comprehensive testing. The experimental results demonstrate that the proposed detection mechanism performs exceptionally well, achieving a 100% detection rate with false alarm rates below 10% across all evaluated scenarios. In recent years, the Internet of Things (IoT) has rapidly become an integral part of everyday life, with billions of smart, autonomous devices interconnected worldwide. IoT systems rely on diverse digital communication technologies to interconnect intelligent objects capable of sensing, analyzing, processing, generating and sharing information, thereby enabling advanced and complex services.

RPL has been chosen as the standard routing protocol to overcome a weak processing power and memory capacity of the Low-Power and Lossy Networks (LLNs), which has a low-powered processing unit and limited memory. Although it is appropriate in resource-constrained settings, RPL is also prone to a number of attacks, especially those that take advantage of control message exchanges. In this paper, a detection mechanism that is particularly created to detect the presence of DIO suppression attacks and detect malicious nodes is presented so as to contribute to the effectiveness of this protocol in terms of security and reliability.

The suggested strategy is premised on observing the DIO suppression behavior that is measured by recording the periods of suppression and analysing the time difference between consecutive DIO messages exchanged over the same node. An effective simulation platform is created to apply and test the solution offered. The effectiveness of the approach is proved by the results that have been achieved after the implementation, which prove that the detection of DIO suppression attacks with the help of the approach is reliable and proves the strength of RPL-based IoT networks.

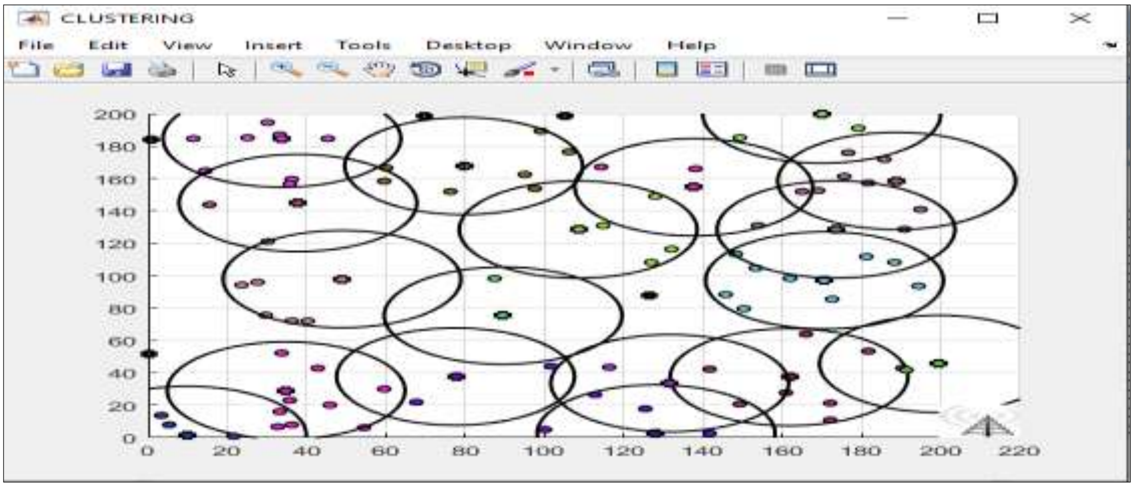


Fig 3 Cluster Head

The Wireless Sensor Network (WSN) is organized into multiple clusters, each supervised by a designated cluster head. The cluster head is responsible for gathering data from the sensor nodes within its cluster, aggregating the collected information and transmitting it to the receiver or base station.

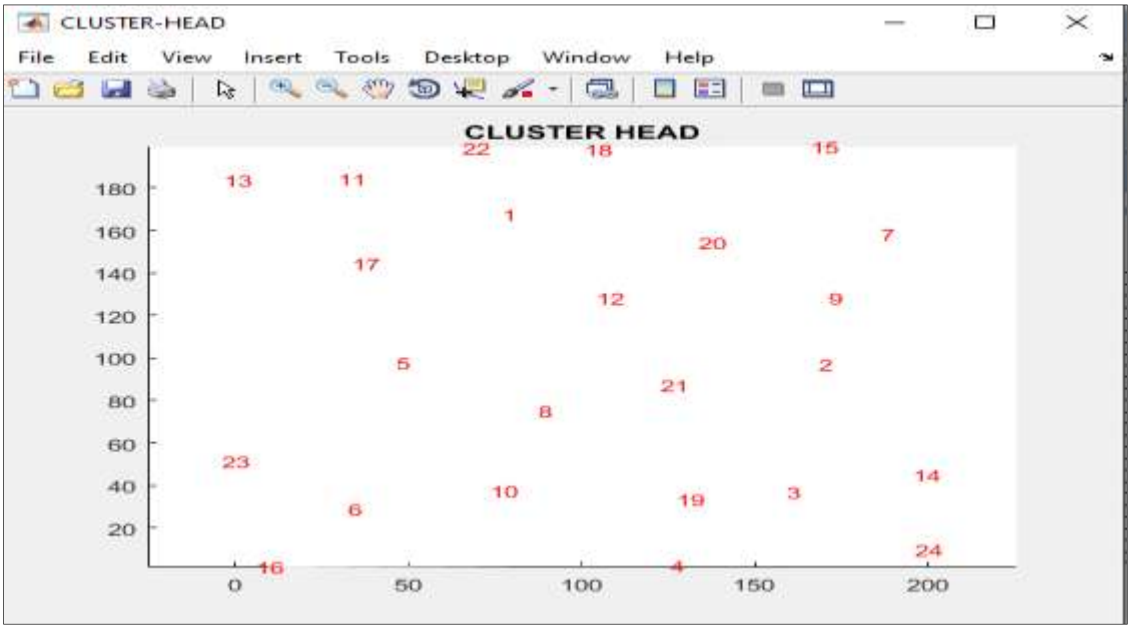


Fig 4 number of cluster head

Figure 4 presents the distribution of node counts among the different clusters in the network. In the Wireless Sensor Network (WSN), each cluster is overseen by a designated cluster head**,** which is responsible for collecting data from the nodes within the cluster and forwarding the aggregated information to the network's central hub.

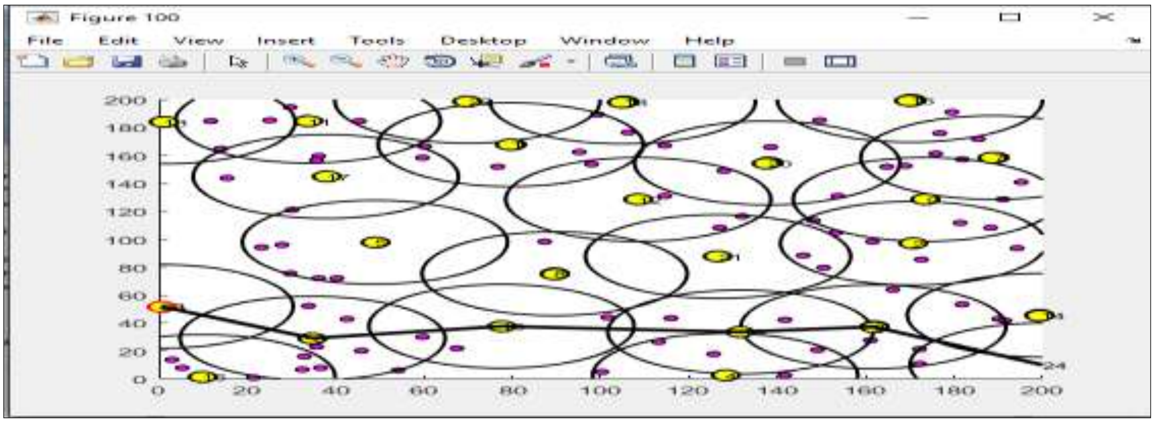


Fig.5 node finds the optimum path in the network

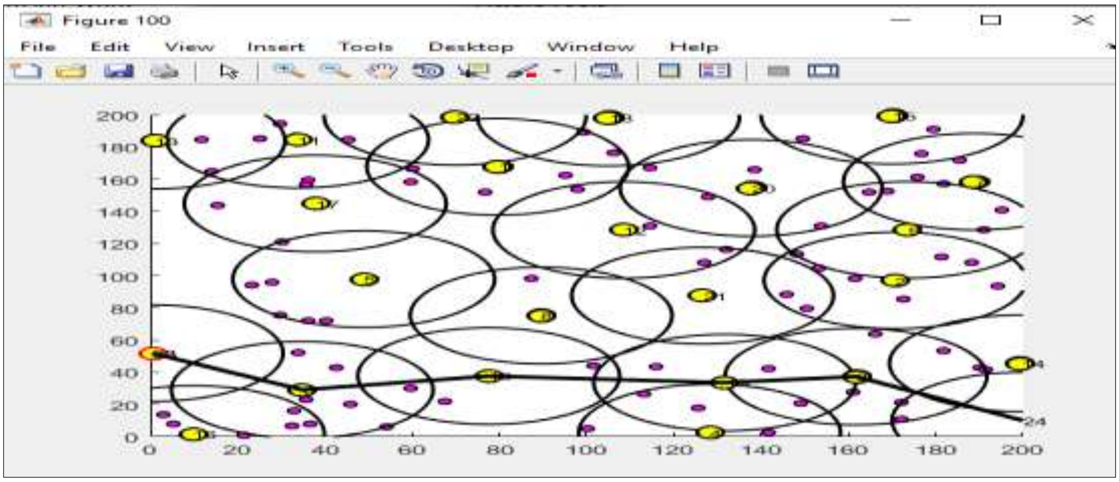


Fig.6 node searching path in the network to secure communication

In a network, optimal path selection is the process of determining the most efficient routing path for transmitting data from a source node to a destination node.

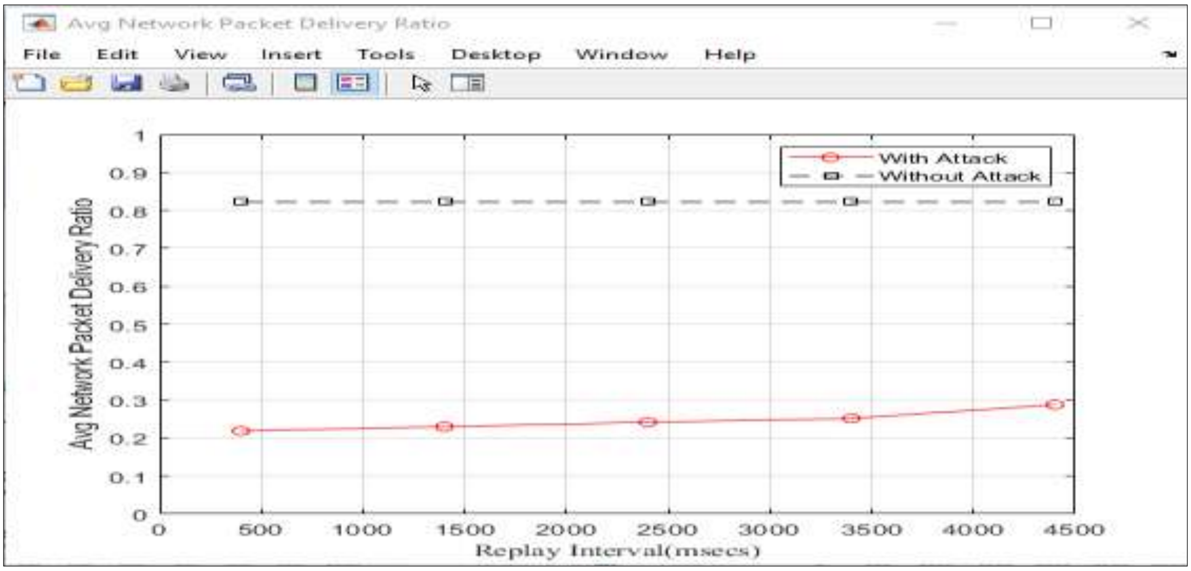


fig. 7Average network packet delivery ratio

The average packet delivery ratio indicates the effectiveness of a network in successfully delivering transmitted data packets. A higher delivery ratio reflects greater network reliability and transmission efficiency, while a lower ratio suggests the presence of issues such as congestion, packet loss, or network instability.

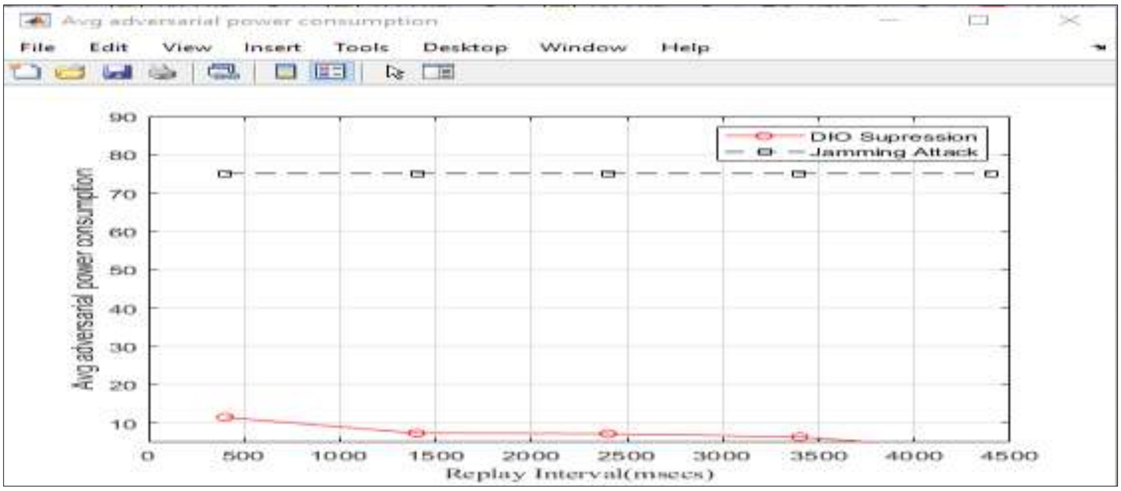
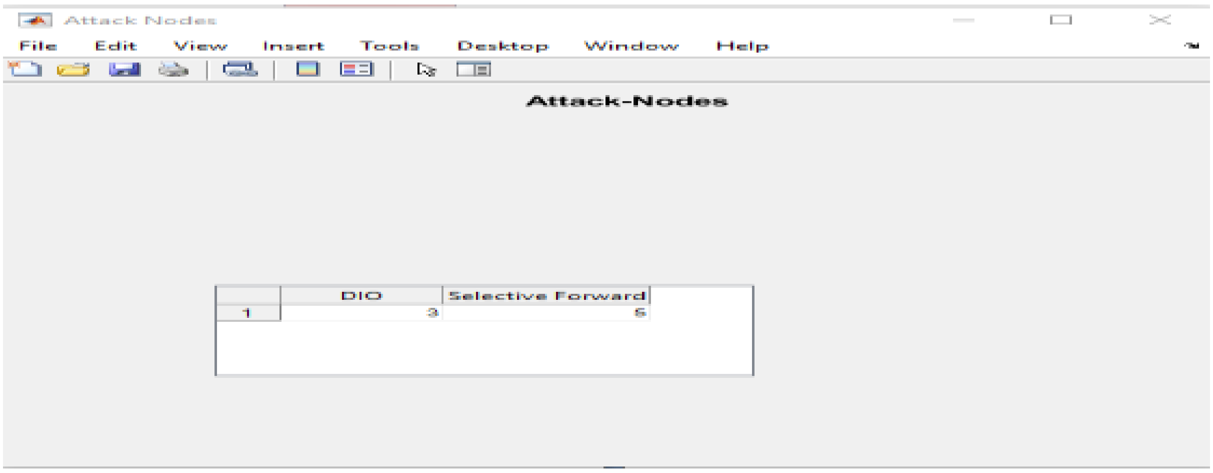


Fig.8 Average adversarial power consumption

The average power consumption of an adversary refers to the amount of energy expended by an attacker while performing malicious activities within a network. This metric represents the energy used to execute disruptive actions, compromise network security, or degrade overall system performance.

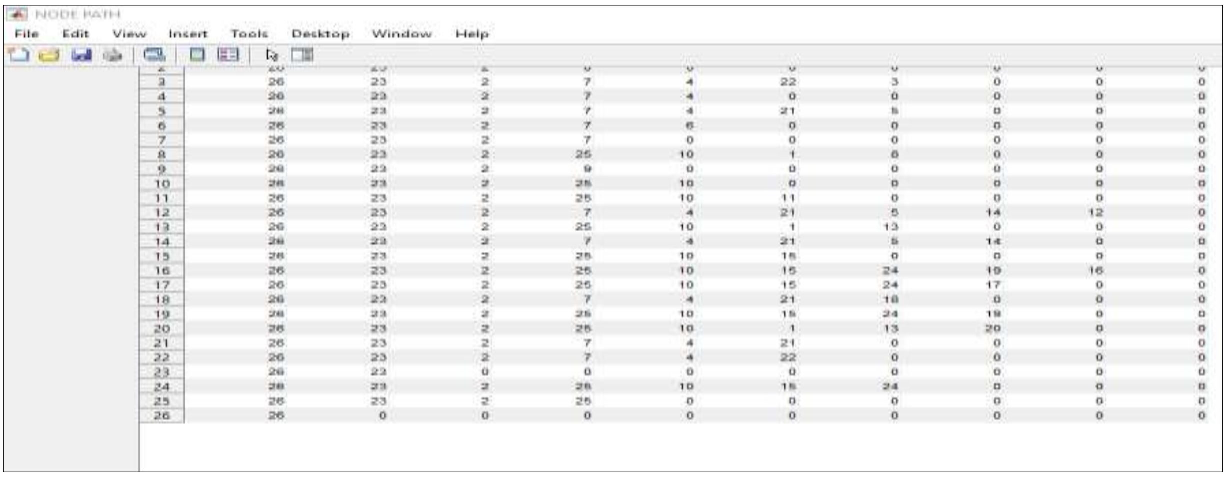


Attack-Nodes

	DIO	Selective Forward
1	3	6

Fig. 9 DIO attack

An attack node is a malicious or compromised entity within a network that intentionally engages in attacks or disruptive activities. In network security contexts, such a node may be under the control of an adversary or compromised through malware, unauthorized access, or other forms of security intrusion.



2	26	23	2	0	0	0	0	0	0	0
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	6	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

This paper offers a promising method of identifying DIO suppression attacks in RPL-based networks and demonstrates its efficiency in terms of a large scale of experiments. The findings indicate that, the detection mechanism proposed is a very good one, as it has a detection rate of 100% and false alarm rates less than 10 percent in all the given test conditions. The Internet of Things (IoT) has gained critical significance in the modern world in recent years, as billions of intelligent autonomous gadgets have been interrelated around the world. IoT systems are designed to use various digital communication technologies to interconnect with intelligent objects, which are able to sense, analyze, process, generate and share data, and hence allow complicated and value-added services. The Routing Protocol for Low-Power and Lossy Networks (RPL) is the most widespread routing solution with the purpose of supporting the low processing power, energy resources, and memory capacity of Low-Power and Lossy Networks (LLNs). Despite the fact that RPL is highly applicable in resource-constrained settings, it is susceptible to various security risks especially those that use control messages to compromise the system. To further improve the security and reliability of the RPL protocol, the paper suggests a special detecting mechanism to recognize the DIO suppression attacks and detect bad nodes.

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 |