© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 01 | January - March 2023
Accepted on 13 March 2023
Published on 30 March 2023
DOI : https://doi.org/10.36676/urr.2023-v10i1-032

Performance of DIO Suppression attack in RPL based IoT networks

Vikas Sindhu*

*Department of ECE, University Institute of Engineering & Technology, Maharshi Dayanand University, Rohtak.

Abstract- Wireless sensor networks are very important in many uses, but they can be attacked, which can make the network less secure and less effective. The Routing Protocol for Low-Power and Lossy Networks (RPL) is the target of the DIO silencing attack. The goal of this study is to figure out how the DIO suppression attack affects RPL and how well the NLBGNDO algorithm stops the attack. To reach this goal, an accurate model of the RPL protocol and the DIO silence attack are built into a modelling code. The modelling code includes the NLBGNDO routing algorithm, which is a suggested safe and effective routing method for RPL. Key measures, like the number of packets delivered, the length of the path, and the amount of power used, are recorded and analysed both when the network is working normally and when it is under attack. The results of the study show how vulnerable RPL is to the DIO suppression attack and how well the NLBGNDO algorithm works to protect against its effects. The packet delivery ratio shows how the attack affects the network's ability to send data, and the route stretch measure shows how well the routing method works when under attack.

Keywords: IoT, RPL DIO suppression attack, NLBGNDO

I INTRODUCTION

Over the past few years, the Internet of Things (IoT) has gotten a lot of attention because it could have a huge number of benefits for people. Kevin Ashton came up with the idea of the IoT in 1999. Its main goal is to connect everything, everywhere, and at any time. [1]. In the IoT , things have the ability to feel, process, and act, and they work together to provide clever and cutting-edge services in a way that doesn't depend on anyone else. The IoT is used in a wide range of areas, such as healthcare, home control, tracking the environment, and many more. The main goal of the IoT is to put all of these different types of applications under one name called smart life. [2]. The IoT is made so that it can work with many different kinds of gadgets and different ways to talk to them. These technologies make it possible for IoT gadgets to talk to each other and give people the services they need. In this part, we'll talk about some of the main ideas behind the IoT. The IoT and its possible uses and design, which includes its main parts and standards, are explained. The IoT is the next step in the growth of the internet. It will let tools and people all over the world connect with each other. IoT is a network of real items, sometimes called "things," that have been equipped with sensors, software, and other technologies so they can talk to and share data with other devices and systems over the internet. IoT is the name of this network. The IoT is a concept and way of thinking that takes into account the fact that there are many different objects that can talk to each other and to other objects to create new applications and reach shared goals using wired and wireless connections and specific addressing schemes. [5]. The main goal of the IoT is to make it possible to join things to anything and anyone, at any time, in any place, and ideally using any method, network, or service.

The administrator is in charge of setting up the DODAG root node, which is the part in charge of making the whole DODAG system. At the beginning, the root node [6] figures out the RPL instance ID, DODAGID, DODAG version number, base rank, objective function (OF), and route cost, among other things. The Sink node sends the information to the other nodes in the area in the form of DIO control messages. This is called multicast. Neighbouring nodes will take the

Accepted on 13 March 2023
Published on 30 March 2023
DOI : https://doi.org/10.36676/urr.2023-v10i1-032

information they get from DIO messages and use it to update their rank, join DODAG, and choose their chosen parent based on their best rank. They let their preferred parent know right away that they have joined the network through DAO by sending a message that says they have joined the network. Each child node has a chosen parent, which works as an intermediate node in the network and as a link between the child node and the master node. [7-9]

Since the root node is the starting point for the whole network, it is the best parent for the first hop nodes. The nodes on the first hop keep sending DIO signals towards the next hop down, while the nodes that are getting data send DAO messages to the parent node. After doing their own math and keeping the goal function in mind, nearby nodes (5, 12, and 19) decide that adding DODAG root as their chosen parent is the best choice. Because they are part of DOADG, nodes 5, 12, and 19 use rank 2 to send their DIO messages to their friends. The ranks in the DODAG go from highest to lowest. The DODAG root doesn't care about the DIO when it comes from these nodes because it has a higher rank number, which means it came from downhill. If the node is in the same radio range as node 12, it can add nodes 5 and 19 as possible parents. Notably, all nodes further down the tree get DIO messages from several nodes nearby, but they choose the parent with the highest rank as their chosen parent. This is a strange thing to happen. The structure won't be finished until all of the nodes are connected to the DODAG.[10-11]

II RELATED WORK

Amal Hkiri et.al. (2022)[12] The RPL is at the heart of 6LoWPAN, which is a key connectivity standard for the IoT. RPL is better than other wireless sensor and ad hoc routing protocols in terms of quality of service (QoS), device control, and how well they use energy. But different threats could hurt the network if there are problems with unauthenticated or open control frames, centralised root controllers, stolen devices, or devices that haven't been verified. So, the goal of this study is to find out how attacks on the design and resources of the network can hurt the performance of RPL. For Resources attacks and Topology attacks, we will focus on Hello Flooding, Increase Number, and Decrease Rank. Some of RPL's performance measures, like End-to-End Delay (E2ED), speed, Packet Delivery Ratio (PDR), and average power usage, were tested to see how the three different attacks might affect them. According to the data, all three attacks cause a rise in E2ED, a drop in PDR and network speed, and a decrease in the quality of service on the network. All of these things lead to higher energy costs for the nodes in the network.

Usha Kiran et.al. (2022)[13] The most common routing system in the 6LoWPAN stack is the Routing system for Low Power and Lossy (RPL) Network. But because RPL doesn't have the right security measures in place, there are a lot of holes in its protections, both inside and outside. A lot more research is needed to find out what RPL can't do. So, in this study, we start by making an implementation of the WPS attack, which stands for worst parent selection. Second, we give you an IDS that can find and warn you about a WPS attack. WPS makes it more likely that the target node will choose the worst node as its chosen parent by changing its goal function. The loop is made when a node with a lower rank picks a parent with a higher rank. This cuts off many nodes from the rest of the network and keeps it from merging in the best way. Also, we recommend DWA-IDS as an IDS that can find WPS attacks. For testing, the Contiki-cooja model is used. The results of the test show that the WPS attack slows down the speed of the system by making it take longer to send a file. The DWA-IDS test results show that our IDS is able to find all of the artificial hostile nodes that start the WPS attack. The suggested DWA-IDS has an identification rate of 100% and a rate of true positives of over 95%. Since our DWA-IDS has never shown a false-positive, we also think about the proof in theory. DWA-IDS is easy enough to set up that machines with limited power and memory can use it.

Accepted on 13 March 2023
Published on 30 March 2023
DOI : https://doi.org/10.36676/urr.2023-v10i1-032

III PROPOSED SYSTEM

In a DIO silence attack, the attacker makes it so that the target nodes stop sending DIO messages. When building the route structure in RPL, DIO messages are very important. By blocking these messages, the attacker messes up the quality of the routes, which can lead to network splits in the long run.

The DIO suppression attack is different from other attacks that have been written about because the attacker doesn't have to make fake RPL messages. Instead, the attacker just keeps playing back words that have already been heard. This makes it possible to carry out the attack without stealing encryption keys from honest nodes. The DIO suppression attack uses the repeat method, which is a popular attack method that is used in a unique way in this case. The goal of the repeat method is to make the target think that information that has already been given is new. But in the DIO suppression attack, the repeat method is used to make a target think that the route information it is about to send has already been sent several times by other nodes.

The Work shows that the DIO silencing attack makes the route service that RPL offers much worse. Also, it shows that this attack uses less energy than a blocking attack that was suggested in the system.

The DIO silence attack has a big effect on the network and makes route service worse in a big way. This new strike, on the other hand, uses less energy than a standard blocking attack. In other words, the intruder can have the same effect on the network without using as much energy as they would with a blocking attack.

Researchers want to bring attention to the fact that RPL could have security flaws and that IoT systems need better security by finding and studying this new attack. This study helps with the work that is still being done to make strong and safe route methods for WSANs. This makes sure that Internet of Things networks work well and consistently.

RPL (RPL)

RPL is a standard routing system made for wireless networks with limited resources, like low-power devices and links with a lot of packet loss. It is mostly used to set up Wireless Sensor Networks (WSNs) and the Internet of Things (IoT). RPL offers a flexible and energy-efficient routing option for networks with resource-constrained devices. It makes it possible to set up routes between the network points, which speeds up contact and data transfer. RPL works in a proactive way, which means that it builds and keeps routes in advance to make sure packets are delivered on time and reliably. 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:

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) denial attack is all about blocking DAO messages in RPL. Nodes use DAO messages to let other nodes in the network know they are there and what

Accepted on 13 March 2023
Published on 30 March 2023
DOI : https://doi.org/10.36676/urr.2023-v10i1-032

services they can offer. By blocking DAO messages, an attacker can stop routing information from getting out, which can cause routing problems or make them worse. This can lead to problems with contact, longer wait times, and slower network speed. The DAO shutdown attack could take advantage of flaws in the process of routing or target certain nodes to stop them from sending DAO messages.

The DIO (DODAG Information Object) suppression attack is a new type of degradation-of-service attack that especially targets the RPL protocol. It wants to mess up the routing service that RPL provides, which could cause networks to split up and routing performance to go down.

The goal of the DIO silence attack is to get nodes in the network that are being attacked to stop sending DIO messages. DIO messages are very important to RPL because they carry important information needed to build and keep up the route structure. By blocking DIO messages, the attacker makes it hard for the network to set up and change routes, which lowers the quality of the routes accessible.

The DIO suppression attack is different from other attacks on RPL because the enemy doesn't have to make fake RPL messages. Instead, the attacker uses a method called "replay" to send DIO messages that have already been heard. This makes the target nodes think that the route information they are about to send is already being sent multiple times by other nodes.

The DIO suppression attack works because the nodes being attacked believe the route information they get from their neighbours. By getting the victims to believe that the routing information is already being spread, the attacker can stop the routing protocol from working normally without having to steal cryptographic keys or make fake messages.

When the DIO suppression technique is used, it can have bad results. It lowers the quality of the lines, which could cause more delay, data loss, and even network splits. This hack can hurt the efficiency and stability of IoT systems and wireless sensor networks that use RPL to communicate well. To stop the DIO suppressing attack and make RPL more secure, researchers are working on ways to identify intrusions, authenticate messages securely, find strange behaviour, and better cryptographic methods. These steps are meant to find and stop the silencing of DIO messages, making sure that the RPL protocol is strong and reliable in the face of such threats.

DIO Algorithm

The DIO (DODAG Information Object) is an important message in the RPL protocol that sends information about the structure and setup of the network. Even though the exact DIO algorithm may change depending on the application or goal function used in RPL, I can give a basic outline of the DIO algorithm and its mathematical expressions.

Rank Calculation: The rank calculation in the DIO method tells us where a node is in the route structure of the network. The math phrase for figuring out a person's rank can be based on different measures and rules. One possible math statement for figuring out rank is:

Rank = BaseRank + (RankFactor * Metric)

Here, BaseRank is a fixed base rank value given to the root node, RankFactor is a number that scales the metric value, and Metric is a unique metric used to calculate rank, such as hop count, energy, or link quality. The RankFactor can be changed to show how important the measure is in deciding how to route the packets.

Objective Function: The DIO method may use an objective function to evaluate and compare different routes based on certain measures and limitations. The goal function can be shown by a math statement that mixes different factors and gives each one a certain weight. For example:

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

Accepted on 13 March 2023
Published on 30 March 2023
DOI : https://doi.org/10.36676/urr.2023-v10i1-032

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 drip timer is used by the DIO method to control how often DIO messages are sent. The trickle timer uses mathematical formulas and chance to figure out how long to wait between sending DIO messages. The drip timer's exact numeric formula depends on how it is put together. But it usually includes variables like minimum interval, maximum interval, and a random backoff factor to add randomness and avoid message clashes.

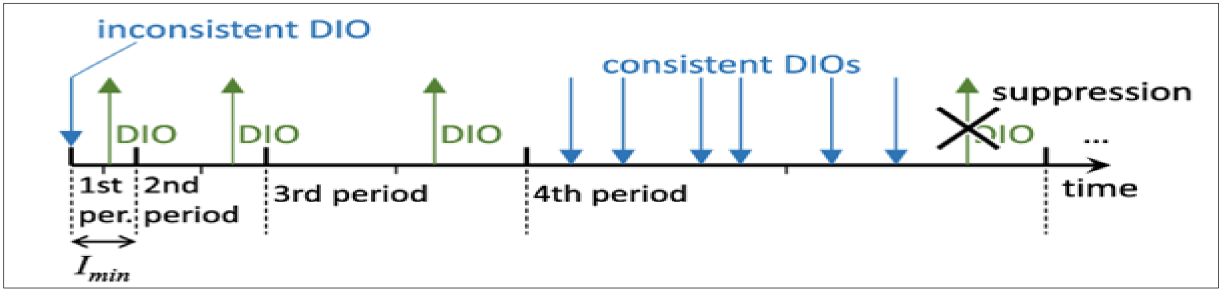


fig.1 timer mechanism

(NLBGNDO

The Non-Linear Brownian Generalised Normal Distribution Optimisation (NLBGNDO) method is made to figure out the best way to move through a network.This method uses non-linear optimisation, Brownian motion, and the generalised normal distribution to find the best path.

NLBGNDO algorithm

The NLBGNDO algorithm tries to make routes more efficient and effective by taking into account things like energy use, delay, link quality, and trip length. By using methods for non-linear optimisation, it can better adapt to the needs and limits of the network.

The programme also uses Brownian motion, which is a random process that models moves that are hard to predict, to search through the search area. This randomness makes it easier to try out different ways and find better answers.

During the optimisation process, the generalised normal distribution is used to describe the probability density function of the factors involved. This distribution lets you change the settings for skewness and kurtosis, which can help you find the best lines for routes based on certain measures.

By combining these methods, the NLBGNDO algorithm tries to find a better way to find the best path in a network while taking into account multiple goals and restrictions. But without more specific information or instructions on how to use the method, it is not possible to give a more complete account of it.

IV RESULT DISCUSSION

The main focus is on presenting a new method called NLBGNDO (Non-Linear Brownian Generalised Normal Distribution Optimisation) to solve the problem of finding the best way from source to target sensing nodes in RPL. The goal of the method is to make route reliable and fast even when the DIO suppression attack is happening.Simulations are done to figure out how well the suggested method works. The computer model is set up to find the best way and cause as little delay as possible when an attack is happening. There are some specific results:

Packet Delivery Ratio: The exercise measures the packet delivery ratio, which is the amount of packets that were sent and how many were properly delivered. This number helps measure how

ISSN : 2348 - 5612 | Volume : 10 , Issue : 01 | January - March 2023
Accepted on 13 March 2023
Published on 30 March 2023
DOI : https://doi.org/10.36676/urr.2023-v10i1-032

well and reliably the suggested method keeps packet delivery going even when the DIO suppression attack is happening.

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.

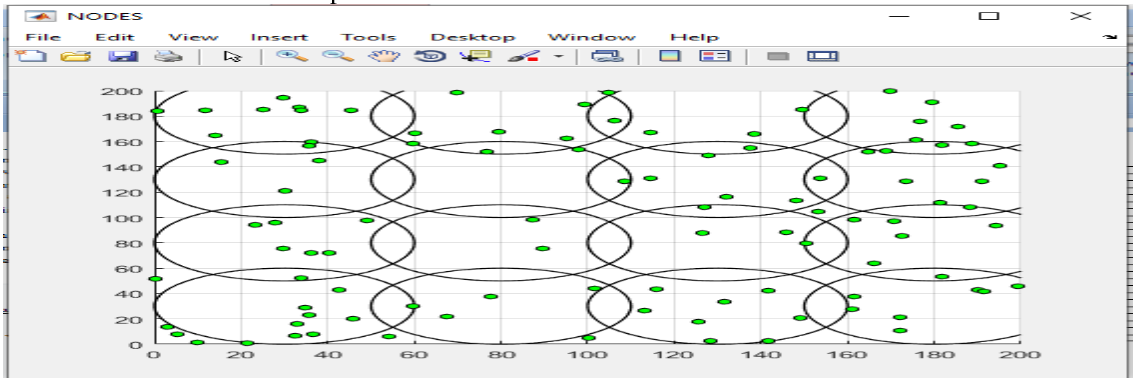


Fig.2 initial network

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.

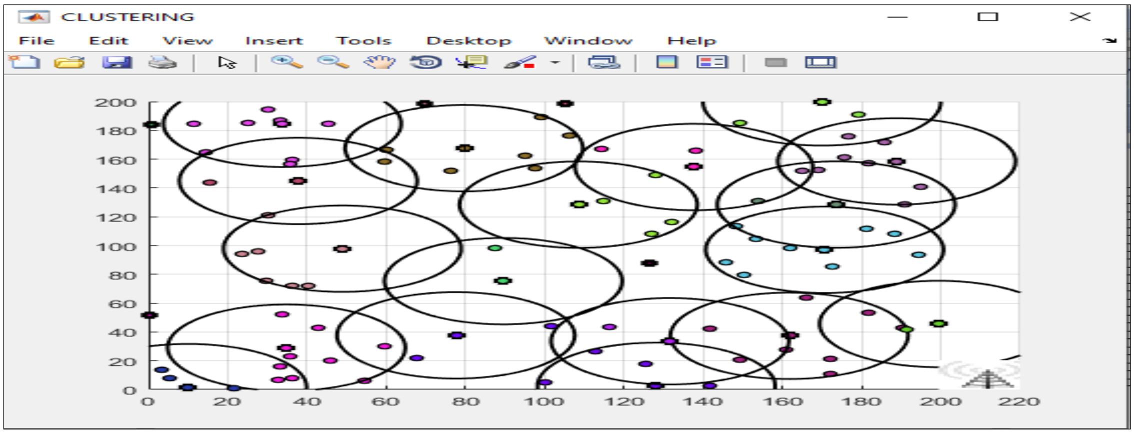


Fig 3 Cluster Head

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).

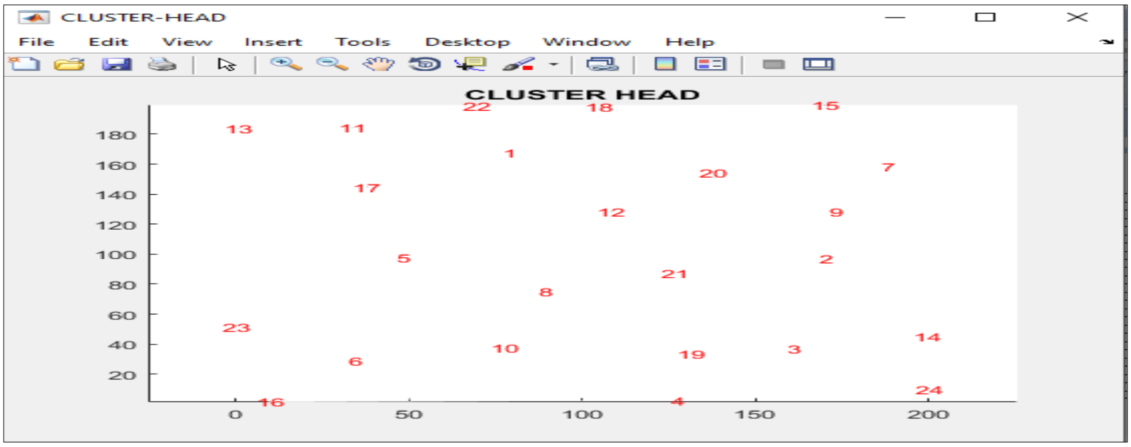


Fig 4 number of cluster head

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.

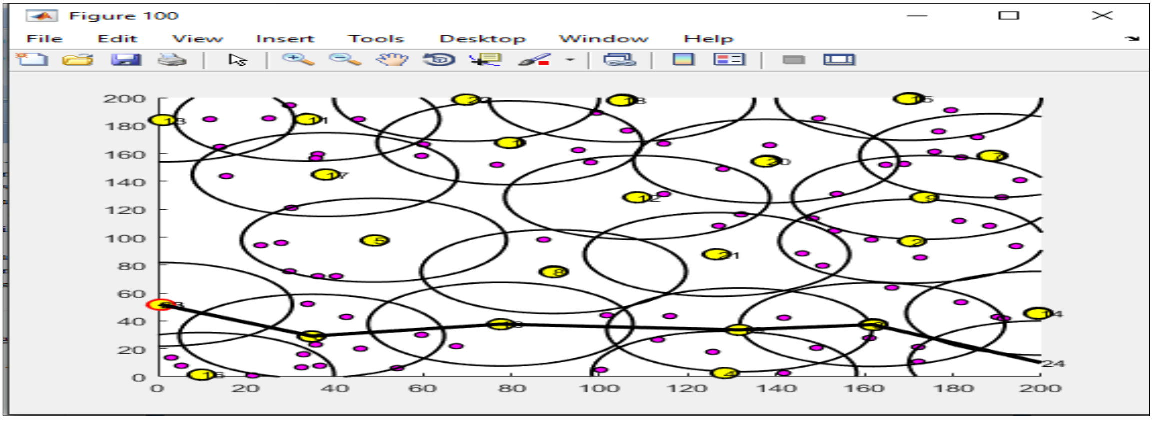


Fig.5 node finds the optimum path in the network

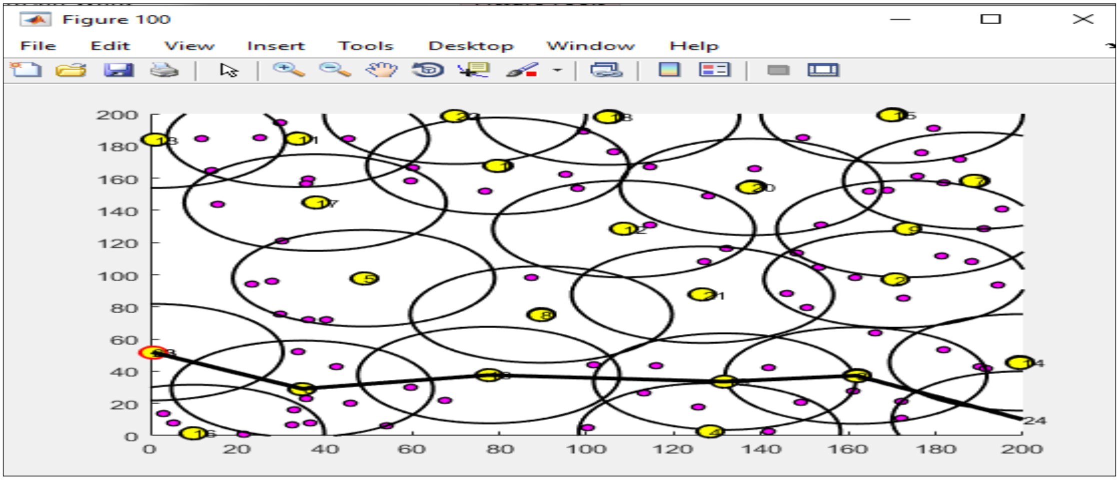


Fig.6 node searching path in the network to secure communication

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

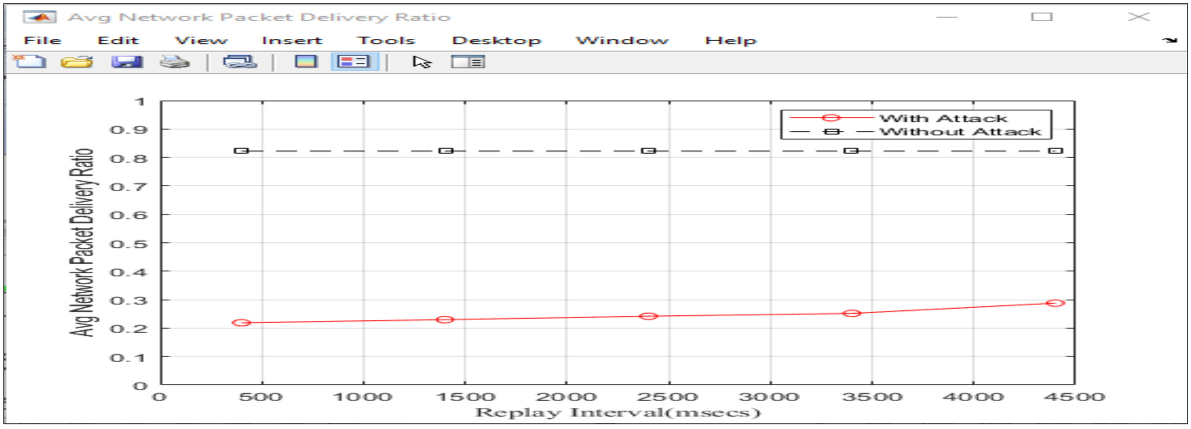


fig. 7Average network packet delivery ratio

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

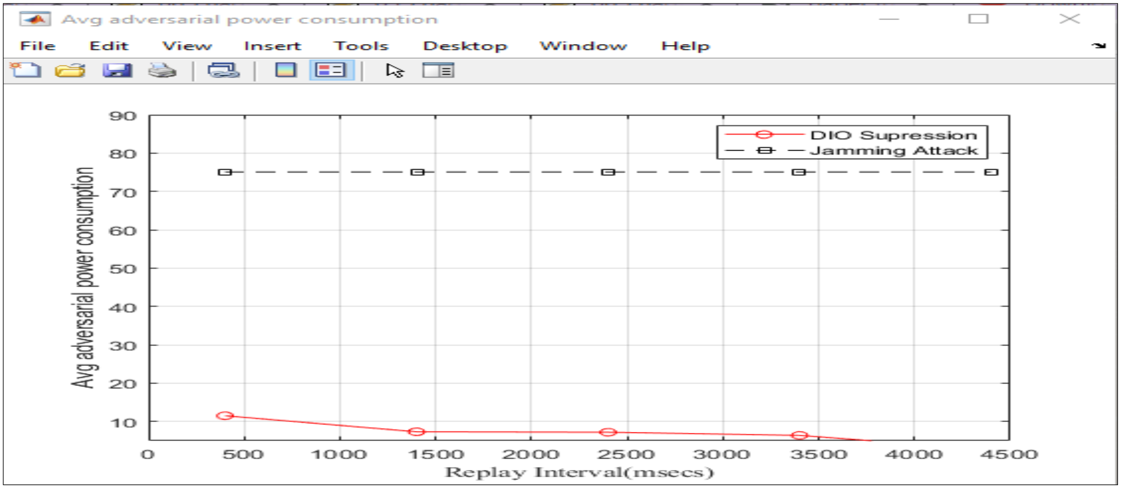
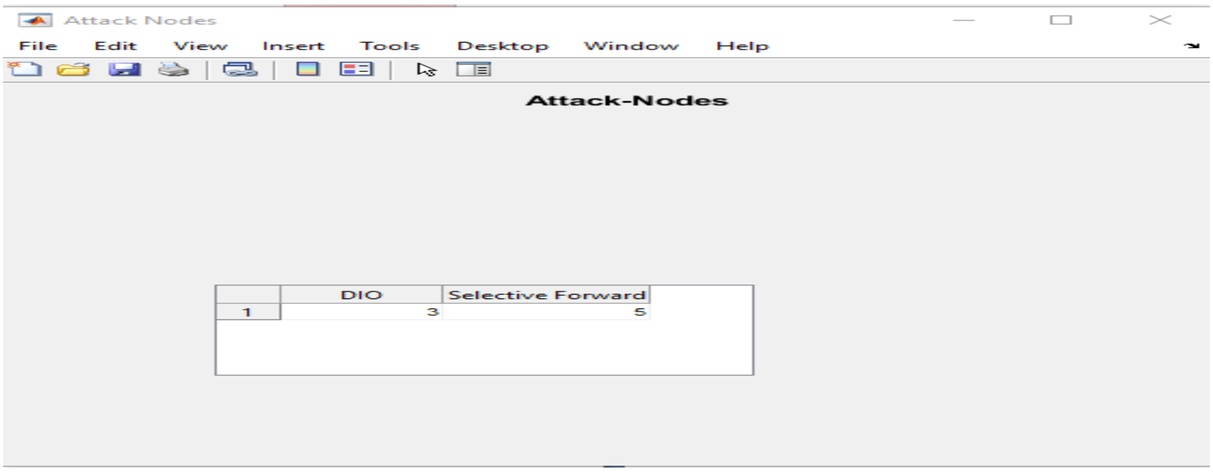


Fig.8 Average adversarial power consumption

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.

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 01 | January - March 2023
Accepted on 13 March 2023
Published on 30 March 2023
DOI : https://doi.org/10.36676/urr.2023-v10i1-032

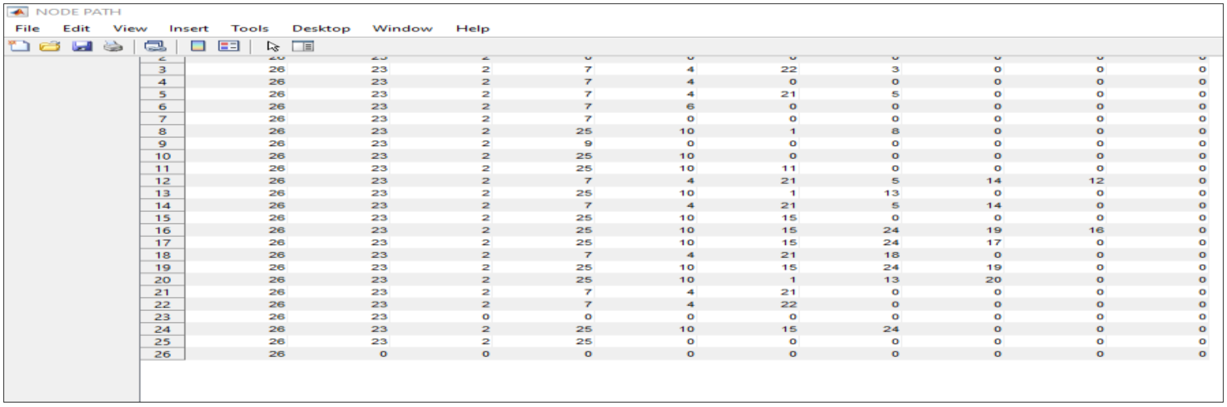


Attack-Nodes

	DIO	Selective Forward
1	3	5

Fig. 9 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. 10 Node path table

V CONCLUSION

The suggested way to find DIO suppression attacks in RPL-based networks, and we tested our detection method to see how well it worked.The results showed that the detection method works very well, with 100% detection rates and less than 10% false alarm rates across the board. The IoT has become an important part of our lives in a very short amount of time. Around the world, there are billions of smart, self-sufficient people that are linked to each other and can talk to each other. The IoT is a system that uses different kinds of digital communication technologies to link smart, self-sufficient objects. These things can collect information, look at it, examine it, process it, make new information from it, and share it with other things so that more complex services can be offered. RPL was chosen as the real routing system to get around the low processing power, battery life, and memory of LLN networks. RPL was chosen as the real routing system because wireless networks have many limits, such as power and memory, that make routing hard. But RPL can be attacked in many different ways that have to do with cross-control talks. The following paper suggests a method that can spot a DIO shutdown attack and spot rogue nodes. This would make the RPL protocol safer and more useful.

Accepted on 13 March 2023
Published on 30 March 2023
DOI : https://doi.org/10.36676/urr.2023-v10i1-032

This is based on the DIO surrender, saving the surrender time, and then doing the action by figuring out the time difference between each message and a message from the same node in the series. a working platform to put our solution into action. After putting the proposed solution into action, which is to find DIO shutdown attacks, we got a good result.

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