© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 04 | July - September 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

A Comprehensive Review of Low-Power Internet of Things Networks under DIO-Suppression Attacks and Countermeasures

Pooja Suhag[1], Akshaya Dhingra[2], Vikas Sindhu[3] and Anil Sangwan[4]
[1,2,3,4] Department of Electronics and Communication Engineering,
University Institute of Engineering and Technology,
Maharshi Dayanand University, Rohtak, Haryana, India
psuhag0107@gmail.com
akshaya.rs.uiet@mdurohtak.ac.in
vikassindhu.uiet@mdurohtak.ac.in
anilsangwan.uiet@mdurohtak.ac.in

Abstract

The Internet of Things (IoT) is a system of devices connected over the Internet. It is currently being utilized in various applications such as smart agriculture, smart industrial monitoring, smart homes, and smart vehicles, which rely on low-power and lossy networks (LLNs). To ensure the reliability and enhancement of the IoT system, it is essential to investigate the threats against the standardized Routing Protocol for LLNs (RPL) developed by the IETF. This paper aims to provide a concise study of IoT technology and its vulnerabilities to attacks that compromise its security. It also presents an overview of different attacks that can occur in RPL technology. Specifically, the paper delves deeper into the DIO Suppression attack, examining its impact on the routing service and the potential for deterioration.

Keywords: IoT, RPL, DIO, classification of attacks, LLNs, trickle algorithm

1. Introduction

The Internet of Things (IoT) comprises a vast network wherein objects and individuals interconnect, gathering and exchanging data pertaining to the environment [1]. The IoT is often referred to as a network of physical sensors with processing capabilities, software, and other technologies that communicate and connect with other devices and systems over the Internet [2].

The term "IoT" was first coined and introduced by computer scientist Kevin Ashton in 1999 in an article titled "A New Sensor Project." However, the history of connected devices dates back to 1832 when the concept was initially conceived. In 1837, scientists further advanced the technology with the development of the electromagnetic telegraph, enabling direct communication between two machines through the transmission of electrical signals. In the late 1960s, as the Internet began to evolve, scientists started contemplating the idea of connecting every device to it. This marks the evolution of IoT technology [3].

The first application of IoT was developed by a group of college students who created a Coca-Cola vending machine on their campus. This vending machine was equipped with sensors to monitor its contents and transmit data over the network. The purpose was to track the availability of Coke and prevent it from running out [1][3]. To achieve this, they installed a micro switch in the machine, allowing it to detect the number of available cans and their temperature. In 1990, John Romkey established the first toaster connected to the Internet. A year later, students from Cambridge University used webcams to monitor the availability of coffee. They ingeniously utilized the first webcam prototype to keep track of the coffee stock in a computer lab's coffee maker [4].

In 2000, LG Electronics introduced the first Internet-enabled refrigerator. In 2005, a small rabbit-shaped robot was developed, capable of providing stock market updates, weather forecasts, and breaking news. In 2008, Switzerland hosted the first global IoT meeting. Currently, the number of IoT-connected devices has surpassed 27 billion, and experts predict that this number will exceed 100 billion by 2030 [5].

According to the ITU-T, the IoT is a worldwide infrastructure within the information society that facilitates improved services by linking physical and virtual entities, enabling them to exchange information using both existing and advanced communication technologies [6].

Figure 1 below illustrates a 3-tier IoT architecture that includes the perception, network, and application layers:

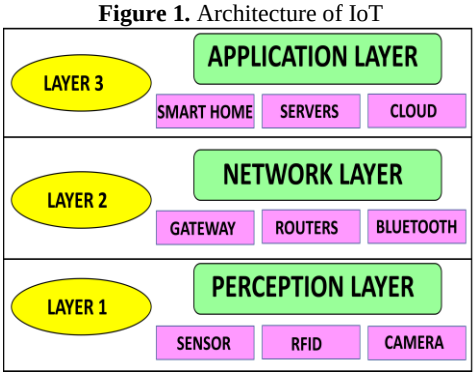
1. Perception layer: The main purpose of this layer is to gather data from the physical environment, such as temperature, and transform analog input into a digital format suitable for transmission. Technologies like WSN (Wireless Sensor Networks) support this layer, which encompasses sensors, gateways, radio frequency identification tags (RFIDs), and barcodes [2],[7].

2. Network layer: Within this layer, a variety of network types are encompassed, including wired networks, wireless networks, private networks, and public networks [7]. Its role is to securely transmit data from the perception layer to the application layer. Technologies such as WLAN, WPAN, LoWPAN, and GSM support this layer.
3. Application layer: The primary role of this layer is to deliver customized services to end users. It delivers the information received from the network layer to the user according to their specific needs. Examples of

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 04 | July - September 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

applications in this layer include environmental monitoring, smart home systems, and intelligent transportation systems [8].

Figure 1. Architecture of IoT



RPL is a standardized routing protocol specifically designed for networks characterized by low power and high loss, known as Low-Power and Lossy Networks (LLNs). It utilizes a directed acyclic graph (DAG) topology to determine the optimal path for transmitting packets from a source node to a destination node. Each node in the network possesses a unique IPv6 address and a rank value, which signifies its position within the DAG. The DAG is constructed using a distributed algorithm that enables nodes to discover their neighbors and exchange information about the network's topology. Every node maintains a list of its parent nodes and child nodes [9] within the DAG. The parent node represents the next hop towards the root of the DAG, while the child nodes serve as the next hop towards the leaves of the DAG [14].

When a node needs to route a packet to a destination node, it first checks whether the destination node is a child node or a descendant of one of its child nodes. If so, the packet is directly forwarded to the child node or one of its descendants. Otherwise, the node selects its parent node with the lowest rank value as the next hop and forwards the packet to it. The parent node then repeats this process until the packet reaches the destination node [10]. RPL also incorporates the concept of routing metrics, which are utilized to assess the quality of a path in the DAG. Each node maintains a routing table that contains information about the available paths to all other nodes in the network, along with their associated metrics [11]. Overall, RPL provides a systematic and flexible routing solution for LLNs, offering support for hierarchical addressing, multicast, and security. Its design enables seamless integration with other IPv6-based protocols and applications, making it a popular choice for numerous IoT and industrial automation use cases [12].

A DIO suppression attack is a type of topological routing attack that involves a malicious host suppressing the propagation of DIO messages, which are essential for creating a DAG topology [13],[14]. The attacker node not only suppresses the DIO messages but also repeatedly advertises a fake DIO message to deceive receiver nodes into thinking it is a legitimate node. As a result, this attack negatively impacts the efficiency of LLN-IoT in terms of metrics such as throughput, end-to-end delay, and energy consumption [5] by nodes. This paper provides an overview of the DIO suppression routing attack in the LLN-IoT network [15].

Main Highlights

The main highlights of this research article are-

1. To study and review .RPL based IoT network history and architecture.
2. To review the previous studies related to RPL protocol.
3. To explain RPL DODAG formation and attacks inherited against RPL protocol.
4. To explain the effect of DIO Suppression attack on RPL network
5. To propose different methods used for prevention of DIO Suppression attacks and future prospects.

Abbreviations

Table 1 shows the list of abbreviations used throughout the article.

Table 1. List of Abbreviations

Term	Abbreviation
IoT	Internet of Things
RPL	Routing Protocol for Low-Power and Lossy Networks
RFID	Radio Frequency Identification
LLN	Low-Power and Lossy Networks
WPAN	Wireless Personal Area Networks
DODAG	Destination-Oriented Directed Acyclic Graph
GSM	Global System for Mobile Communications
IPv6	Internet Protocol version 6
DAG	Directed Acyclic Graph
DIO	DODAG Information Object
MRM	Multipath Ray-tracer Medium Model
WLAN	Wireless Local Area Network
DETONAR	DETector Of Network Attacks in RPL
IDS	Intrusion Detection System

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 04 | July - September 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

OmNeT++	Objective Modular Network Testbed in C++
SLR	Security Lifecycle Review
WSN	Wireless Sensor Networks
DIS	DODAG Information Solicitation
6BR	6LoWPAN Border Router
LoWPAN	Low-Power Wireless Personal Area Networks
DAO	Destination Advertisement Object
DIS	DODAG Information Solicitation
OCP	Objective Code Point
PLC	Power Line Communication Internet of Things
ETX	Expected Transmission Count
PDR	Packet Delivery Ratio
NIDS	Network Intrusion Detection Systems

2. Literature Survey

This section gives an overview of previous literature related to DIO-Suppression attacks and techniques to mitigate these types of attacks.

In [1], Pericle Perazzo et.al. concluded results, after studying the RPL protocol, the Trickle algorithm, and working on the MRM model, that the DIO suppression attack can be executed without the need to steal cryptographic keys from trustworthy nodes. They developed a DIO suppression attack that tricks a victim node into suppressing the transmission of DIO messages. In [2], Andrea Agiollo et.al. designed a novel mechanism called DETONAR, which helps detect 14 known attacks against RPL in IoT networks. DETONAR achieves excellent intruder identification results without the overhead of RPL communication, using a data eavesdropping approach. DETONAR is a practical solution that does not require complex calculations or modifications in IoT devices. Moreover, it allows for future adaptability, as the attack classification procedure can be modified to incorporate new rules for identifying new attacks. DETONAR's flexibility enables it to be quickly deployed in core networks without the need to update IoT devices. In [3], Rashmi Sahay et.al. presented a unique topological attack known as the Network Partitioning Attack. They investigated the RPL vulnerability related to the downward technique, which can be exploited to launch an IoT-LLN Network Partitioning Attack. In this attack scenario, the victim nodes experience isolation from both the sink node and the IoT implementation, resulting in reduced availability of nodes and a decrease in the transmission of packets to the sink node. This attack has a significant impact on the performance of IoT-LLNs, leading to packet loss. To address the Network Partitioning Attack, suggested enhancements to the RPL routing procedure were also proposed.

In [4], Linus Wallgren, et.al. focused on the strengths and weaknesses of IoT protocols that can be exploited by intrusion detection systems (IDS). While the RPL protocol has built-in defenses against HELLO Flood attacks and funnel attacks, it is susceptible to certain routing attacks. They highlighted the importance of security in IoT, particularly based on RPL, and laid the foundation for future researchers aiming to develop and implement IDS for IoT. In [5], Ahmed Raoof et.al. discovered that RPLs are vulnerable and their security is a high concern topic. They proposed a hybrid detection IDS with hybrid placement, combining SVELTE and RPL's specification-based IDS. This approach proves to be effective in mitigating various RPL attacks simultaneously. In [6] and [12], Cong Pu focused on the analysis and defense mechanisms against the DIS and Sybil attacks. They suggested a GINI countermeasure by working with OMNeT++ and evaluating its outcomes compared to Sec RPL and two-step detection. A countermeasure technique was developed by the researchers, utilizing the Gini index, to detect and prevent Sybil attacks. Extensive simulations demonstrated that the proposed countermeasure effectively identifies and mitigates Sybil attacks, providing operational defense against them in IoT systems. The technique notably improves the detection rate, detection latency, and energy consumption, as supported by the simulation results. In [7], Karen Avila et.al. thoroughly discussed the systematic approach of IoT, RPL, and attack coding. SLR was developed as a defensive mechanism to combat frequent network layer attacks in wireless sensor networks that employ the RPL protocol.

In [8] and [10], Abhishek Verma et. al. discussed IoT, a taxonomy of RPL attacks, future challenges in IoT, and defense mechanisms. They analyzed the impact of Copycat attacks and experimentally validated them using the Cooja Simulator, which operates on the Contiki operating system. They also focused on the DIS flooding attack, classifying it as Multicast DIS flooding and Unicast DIS flooding, and experimentally verified the effectiveness of the Secure-RPL mechanism. In [11], Shimaa A. Abdel Hakeem et.al. conducted experiments on two different hardware platforms, using constant and randomized network topologies. They evaluated RPL in various configuration settings and network environments, considering variables such as power utilization, latency, and PDR.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 04 | July - September 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

The rest of the paper is organized as follows: Section I defines IoT and its design model, including an explanation of RPL and DIO Suppression attacks. Section II presents the literature review on IoT and its network attacks. Section III discusses RPL terminology and topology. Section IV outlines the different attacks in RPL. Section V provides a detailed analysis of the DIO Suppression attack. Finally, Section VI covers the strategies for preventing and mitigating the DIO attack.

3. RPL Topology and Background

RPL is an IPv6-based distance vector and source routing algorithm designed to address the challenges posed by unreliable wireless communications and power-constrained devices. It achieves this by reducing functional complexity and minimizing overhead. RPL generates a Directed Acyclic Graph (DODAG) to establish the routing structure.

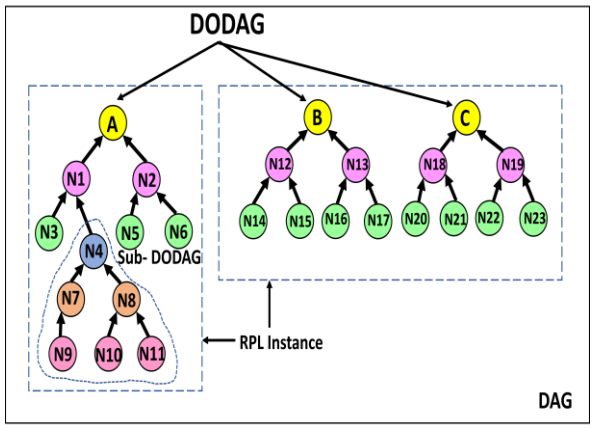
The DODAG, an essential element of the RPL protocol, is designed to facilitate network routing in LLNs such as those found in IoT environments. It represents a directed acyclic graph where nodes in the network self-organize hierarchically based on their proximity to the root node. The root node serves as the ultimate destination, and the DODAG structure establishes the paths and routes for efficient data transmission between nodes. DODAGs are dynamically constructed as nodes join or leave the network, ensuring reliable and efficient routing in resource-constrained environments [16].

There are two categories of DODAG: grounded and floating.

4. In a grounded DODAG, a node directs traffic towards a gateway, which subsequently forwards it to the destination.
5. A floating DODAG is a type of DODAG that lacks a gateway node, with each individual node assuming the responsibility of forwarding its own traffic [11][17].

A DODAG graph (Figure 2) is formed by connecting IoT devices using a combination of grid and tree structures. During the initiation of a DODAG network, a root node acts as an intermediary connecting LLN nodes and the Internet. Within the DODAG, each node is allocated a rank, which is a 16-bit value indicating its distinctive position in relation to other nodes within the DODAG hierarchy, specifically concerning the DODAG root [5][11][16].

Figure 2. RPL DODAG Formation

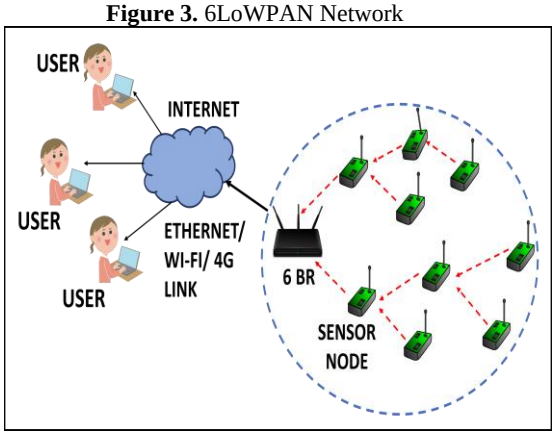


A 6LoWPAN network (Figure 3) is made up of smart sensor nodes that use the IEEE 802.15.4 protocol and can interact via IPv6 utilizing a 6 BR. This allows the network to make decisions together and choose the most efficient path to a destination [8],[9],[10],[11].

The RPL protocol consists of three kinds of control messages -

1. DIO- To establish a new DODAG, the DODAG route offers DIO messages in multicast mode. Any node can locate an RPL instance, choose a set of parents, understand the configuration, and ultimately create a DODAG using the network information contained in a DIO message [11],[13].
2. DAO- Upon the formation of a DODAG, each individual node sends a message to its predecessor node, which is responsible for handling downstream traffic. This message transmission facilitates the exchange of rank and routing table information, thereby populating the predecessor node's data.
3. DIS- Nodes transmit these messages to compel other nodes to deliver DIO messages to the target node. when a node goes an extended period without receiving a legitimate DIO message [13],[17].

Figure 3. 6LoWPAN Network



The parent of each node in the RPL network serves as the node's gateway to destinations. If the RPL node does not

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 04 | July - September 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

find a route for the packet in the routing table, the node can forward the packet back to its parent, and so on, until it strikes its terminus or further up to the tree to reach a common parent destination. A node must have a path to all nodes under the tree [14].

The creation of a new RPL is initiated by the root node through the provision of a DIO message [12],[15]. The DIO message encompasses all the information pertaining to the DODAG, including:

1. DODAG ID: It is utilized for the identification of the root node and the corresponding DODAG.
2. Rank: Nodes utilize rank values to determine their relative position w.r.t. the root node or other nodes.
3. OCP: OCP is employed to determine the objective function necessary for computing the DODAG rank, considering the predefined constraints and metrics utilized in constructing the DODAG.
4. Upon receiving the first DIO message, the node incorporates the sender's address into the parent list and interprets the sender's rank value in accordance with the objective function.
5. Always remember that a node's rank must be higher than its parent node.

RPL is a pre-emptive routing protocol outlined specifically for LLNs. LLNs line is lossy, so it can become unreliable shortly due to various causes such as interference and noise [11].

4. Attacks on RPL Protocol

The security threats targeting RPL networks are commonly referred to as attacks [8]. RPL network structure attacks are characterized by deliberate actions aimed at compromising the hierarchical structure of RPL-based networks, leading to a degradation in their stability and efficiency.

These attacks can be categorized into three main types: resource attacks, topology attacks, and traffic attacks [8][9]. Further classification is based on the specific method of attack. Figure 4 illustrates a taxonomy of RPL protocol attacks, while Table 2 provides a concise explanation of how these attacks influence network efficiency.

Figure 4. Classification of Attacks

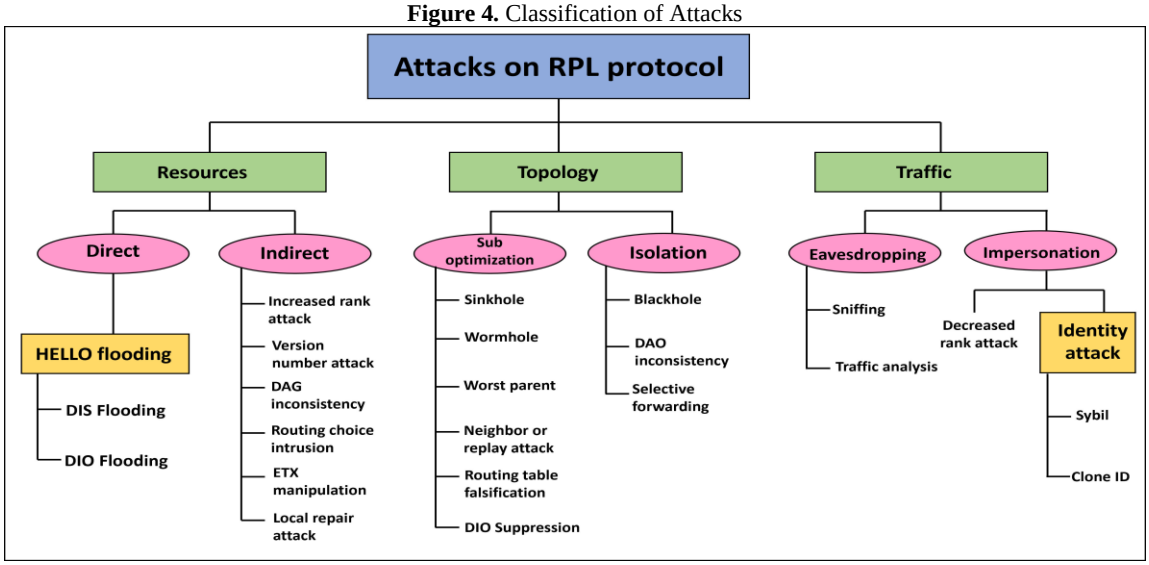


Table 2. RPL Protocol Attacks

Attacks	*Category*	*Prerequisites*	*Specifications*	*Influence on network efficiency*
Rank	Insider	-	Exploiting the rank field and rigid rank regulations.	Improves consumption of energy, congestion, PDR, control packet overhead, and E2E latency. Creates routing loops. Provides unproductive routes.[1]
Neighbor/ Replay	Insider	-	The attacker node intercepts legitimate neighbors' DIO signals and sends them to its neighbors afterwards.	Improves network congestion, low PDR, delayed routes, and unwanted interference.[2],[3]

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 04 | July - September 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

DAO inconsistency	Insider	Storing mode, Option header	The attacker takes advantage of the DAO loop recovery technique.	Improves E2E delay. Causes unoptimized topology and isolation of nodes.
Routing table falsification	Insider	Storing mode, Option header	The attacker jams false routing information into genuine nodes' routing tables.	As a result, legitimate optimized routes cannot be constructed because the buffer in the victim nodes' routing tables is filled.
Routing choice intrusion	Insider	-	The attacking node picks up the existing routing protocols. Then, it multicasts the fake DIO messages after capturing the actual DIO messages.	Improves E2E delay and energy consumption. Creates routing loops and unoptimized paths.[4],[5],[6]
DIS	Insider/ Outsider	-	As a result of being flooded with DIS messages, legitimate nodes are compelled to restart their trickle timer and respond with DIO messages.	Improves control packet overhead and energy utilization leading to routing disruption.
Version number	Insider	-	The attacker node purposefully increases the version number, which causes a network-wide fix.	Improves control packet overhead, E2E delay, and energy consumption. Generates rank inconsistencies and routing paths.[7],[8]
Local repair	Insider	-	By setting the rank value to infinite or altering the DODAG ID value, the local repair process is taken advantage of to cause insignificant local repairs.	Improves energy consumption and degrades routing procedure.[9]
Direct DODAG inconsistency	Insider/ Outsider	Option header	The attacker sets the "O" and "R" flags on the packets before multicasting them, thus exploiting the local repair method.	Traffic congestion. Increases the packet loss ratio while lowering energy usage and packet overhead.
Forced blackhole	Insider	Option header	The attacker node puts the "O" and "R" flags on the data packets it receives and sends them on to its neighbors.	Improves control packet overhead and energy consumption. Reduces PDR.[10],[11],[12],[13]
DIO suppression	Insider/ Outsider	-	The transmission of previously intercepted DIO messages results in the suppression of new DIO interactions.	Initiates inefficacious routing paths, which causes network partition.[14]
ETX manipulation	Insider	ETX objective function	ETX value manipulation is done to improve network positioning and pull traffic.	Initiates inefficacious routing paths.
HELLO/ DIO flood	Insider/ Outsider	-	DIO messages are multicast with high signal strength and favourable routing measures.	Contributes to network congestion and RPL node overload. Improves the packet loss ratio while reducing packet latency.[15],[16],[17]
Sinkhole	Insider	-	To incline the favoured parent of its neighbors, a malicious node lowers its rank.	Decreases the gross network efficiency due to unoptimized paths.
Blackhole	Insider	-	The messages that malicious nodes receive from their child nodes are all dropped.	Reduces PDR, improves end-to-end delay, and unstabilizes topology.
Selective forwarding/gray hole	Insider	-	Specifically, malicious nodes forward control messages while dropping data packets.	Negatively impacts topology structure, resulting in unstable routing. PDR is reduced.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 04 | July - September 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

Wormhole	Insider	Minimal two malicious nodes	To send data over great distances, at least two nodes are required to build a tunnel with maximum bandwidth.	Generates unoptimized paths.
Sybil	Insider	-	A single component can have more than one logical identity.	Takes possession of the network and defeats voting systems while compromising transmission paths.
Clone ID	Insider/ Outsider	-	Multiple nodes receive copies of a single logical identity.	Takes over the network and compromises transmission paths.
Jamming	Outsider	-	The attacker uses powerful radio transmissions to cause significant interference.	Reduces PDR and improves energy consumption.
Sniffing	Insider/ Outsider	-	Eavesdropping on network traffic is done to extract routing information from packets.	Generates privacy concerns.
Traffic analysis	Insider/ Outsider	-	Radio transmissions eavesdrop to examine traffic trends and gather routing and topology.	Generates privacy concerns.

5. DIO Suppression Attack

The DIO suppression attack is aimed at obstructing the propagation of DIO messages by specifically targeting victim nodes. DIO messages play a crucial role in establishing the routing topology within the RPL protocol [1]. Consequently, this attack results in the degradation of route quality, leading to network partitioning (as depicted in Figure 5) [3][6][12]. In contrast to other attacks, the DIO suppression attack does not necessitate the adversary to fabricate counterfeit RPL messages. Instead, it periodically replays previously intercepted messages. Therefore, it is possible to execute this attack without stealing cryptographic keys from trustworthy nodes [2][13]. The replay technique is commonly utilized to persuade a victim node to accept outdated information as current data. In the context of the DIO suppression attack, this technique is exploited to mislead the targeted node by creating the illusion that the routing information it is about to receive has been previously transmitted by multiple other nodes.

A trustworthy node's DIO message can be intercepted and subsequently replayed repeatedly at a predefined frequency to initiate a DIO suppression attack. Nearby trustworthy nodes will perceive the replayed DIO messages as genuine and reliable. The receipt of an identical DIO message by a node does not result in any changes to its parent set, preferred parent, or distance from the root.

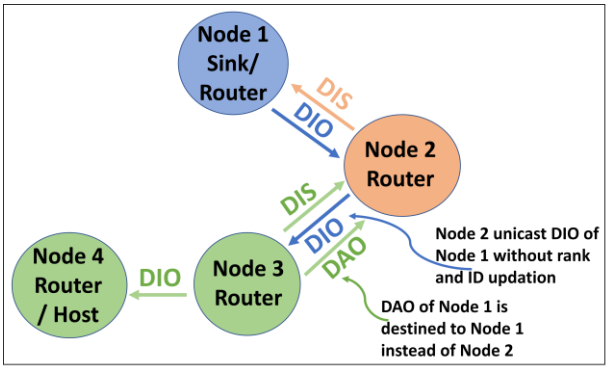


Figure 5. DIO attack network partitioning

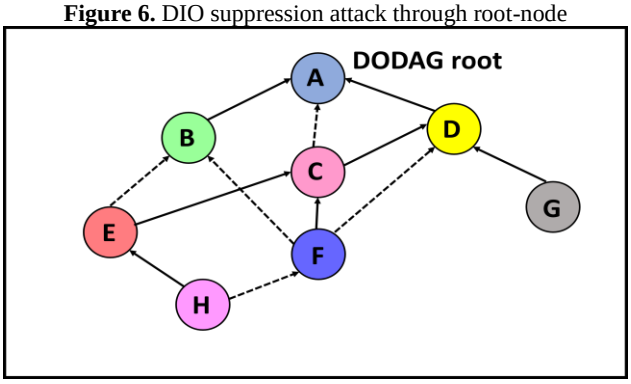
Assuming that the adversary places a malicious device near node A within the network depicted in Figure 6. Once it intercepts a DIO message sent by node A, the malicious device promptly initiates the dissemination of manipulated information, following a predetermined duration.
If the information triggers the suppression thresholds of nodes B, C, and D, all of them will cease emitting DIO messages.
As a result, the network becomes fragmented, with certain nodes (such as E) not receiving any routing information. The legitimate emission of DIO messages will be significantly reduced if a sufficient number of replayed DIO messages are present, thereby compromising the proper functioning of the network. For instance, if node E updates its parent using a more optimal route, the attack may impede the transmission of the updated route to node H. As a result, less-than-ideal paths are temporarily chosen, as demonstrated when H selects F as its preferred parent [1][15].

If an attacker were to launch a "DIO suppression attack," they would likely disrupt the transmission of DIO messages in various ways. This could involve techniques such as jamming the wireless channels used for message transmission or flooding the network with counterfeit DIO messages.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 04 | July - September 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

By disrupting the propagation of DIO messages, the attacker has the potential to prevent the network from establishing or maintaining a valid DAG. This disruption would then impair the network's ability to route traffic effectively [8][9][10].

Figure 6. DIO suppression attack through root-node



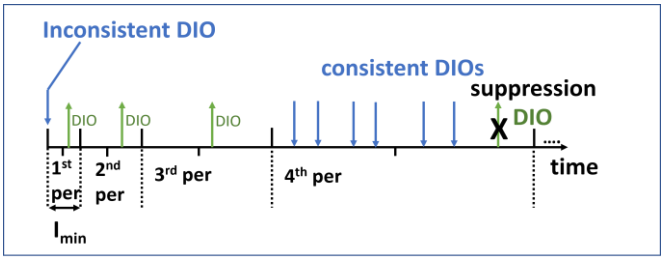
6. Prevention and Mitigation of DIO Suppression Attack

The RPL protocol and the devices utilizing it need to be adequately secured to prevent or mitigate DIO suppression attacks. Implementing various precautions can help achieve this, such as using network intrusion detection systems (NIDS) to monitor for unusual traffic patterns, authenticating and encrypting DIO messages, and deploying redundancy and failover mechanisms to ensure uninterrupted network functionality even in the event of an attack [16].

The primary objective of a DIO suppression attack is to disrupt or impede the transmission of DIO signals within the network. Figure 7 illustrates the Trickle algorithm, which is responsible for regulating the transmission of DIO messages. Originally designed to reduce node power consumption, Trickle achieves this by minimizing redundant messages and adjusting transmission rates [4]. Based on the reliability of the routing information, the rate of DIO transmission is adjusted. When both the internal routing information and the information within the local DIO are accurate, the emission rate decreases. However, if an incorrect DIO is received, the emission rate increases. RPL defines the criteria for determining DIO consistency, such as evaluating whether DIOs cause changes in supersets, preferred parents, and root distances. DIO messages that do not impact these parameters should be deemed consistent [1][12].

The algorithm categorizes time into segments of varying lengths. During each session, nodes program DIO messages to be sent at random intervals. A node receives messages up to time t and searches for the corresponding DIO [5][15]. A scheduled DIO message is broadcasted at time t (k) only if the count of negotiated DIOs obtained within the current interval falls below a specified suppression threshold. If solely a negotiated DIO is received by the end of a period, the duration of the subsequent period is doubled until it reaches the maximum length (Imax). In the event of an inconsistent DIO being received, the current time frame is terminated, and the algorithm restarts with the minimum length period (Imin) [17].

Figure 7. Illustration of Trickle algorithm



7. Future trends

In this paper, we have thoroughly studied the RPL network topology in IoT, as well as security threats and attacks in IoT. We have reviewed the research conducted by various authors in this field. Subsequently, we will conduct experimental investigations to assess the impact of the DIO Suppression attack on the RPL network. The security of IoT devices remains an ongoing concern, and several future trends are emerging to address these challenges. These trends include enhanced authentication mechanisms, secure firmware and software updates, and the use of Machine Learning and Artificial Intelligence (AI) for threat detection, privacy protection, and data encryption. It is crucial to acknowledge that the security landscape is in a constant state of evolution, with the potential for new threats and trends to emerge in the future. Therefore, ongoing research, development, and proactive security measures are necessary to ensure the continued security of IoT devices.

Detecting the DIO Suppression attack in RPL networks can be challenging due to its exploitation of the routing protocol itself. One effective way to detect the DIO Suppression attack is by analyzing rank discrepancies. Each node in RPL has a rank value that indicates its position in the network topology. Monitoring and analyzing the rank values of nodes can help identify discrepancies caused by the DIO Suppression attack. If nodes observe inconsistent or abnormal rank values in their neighbors, it can be an indication of the attack.

8. Conclusion

The DIO suppression attack seeks to disrupt the transmission of DIO (DODAG Information Object) messages, causing a decline in route quality and the partitioning of the LLN-IoT network. This paper provides an overview of various routing attacks that occur in the RPL-IoT network, with a particular focus on DIO suppression attacks. These attacks employ different techniques, such as wireless channel jamming or flooding the network with counterfeit DIO messages, to disrupt the transmission of DIO signals. The article also

covers several prevention and mitigation strategies for mitigating this type of attack.

References

[1] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, "DIO suppression attack against routing in the internet of things," IEEE Communications Letters, vol. 21, no. 11, pp. 2524–2527, Nov. 2017, doi: 10.1109/LCOMM.2017.2738629.

[2] A. Agiollo, M. Conti, P. Kaliyar, T. N. Lin, and L. Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1178–1190, Jun. 2021, doi: 10.1109/TNSM.2021.3075496.

[3] R. Sahay, G. Geethakumari, and B. Mitra, "A novel Network Partitioning Attack against Routing Protocol in Internet of Things," Ad Hoc Networks, vol. 121, Oct. 2021, doi: 10.1016/j.adhoc.2021.102583.

[4] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," Int J Distrib Sens Netw, vol. 2013, 2013, doi: 10.1155/2013/794326.

[5] A. Raoof, A. Matrawy, and C. H. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," IEEE Communications Surveys and Tutorials, vol. 21, no. 2, pp. 1582–1606, Apr. 2019, doi: 10.1109/COMST.2018.2885894.

[6] C. Pu, "Sybil attack in RPL-based internet of things: Analysis and defenses," IEEE Internet Things J, vol. 7, no. 6, pp. 4937–4949, Jun. 2020, doi: 10.1109/JIOT.2020.2971463.

[7] K. Avila, D. Jabba, and J. Gomez, "A nonlinear robust sliding mode controller with auxiliary dynamic system for the hovering flight of a tilt tri-rotor UAV," Applied Sciences (Switzerland), vol. 10, no. 18. MDPI AG, Sep. 01, 2020. doi: 10.3390/APP10186472.

[8] A. Verma and V. Ranga, "The impact of copycat attack on RPL based 6LoWPAN networks in Internet of Things," Computing, vol. 103, no. 7, pp. 1479–1500, Jul. 2021, doi: 10.1007/s00607-020-00862-1.

[9] A. Verma and V. Ranga, "Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review," IEEE Sens J, vol. 20, no. 11, pp. 5666–5690, Jun. 2020, doi: 10.1109/JSEN.2020.2973677.

[10] A. Verma and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 2, Feb. 2020, doi: 10.1002/ett.3802.

[11] S. A. A. Hakeem, A. A. Hady, and H. W. Kim, "RPL routing protocol performance in smart grid applications based wireless sensors: Experimental and simulated analysis," Electronics (Switzerland), vol. 8, no. 2, Feb. 2019, doi: 10.3390/electronics8020186.

[12] IEEE Communications Society., IEEE Computer Society., and Institute of Electrical and Electronics Engineers, 2019 International Conference on Computing, Networking and Communications (ICNC).

[13] Shram Sadhana Bombay Trust College of Engineering and Technology, IEEE Computer Society, Institute of Electrical and Electronics Engineers. Bombay Section, and Institute of Electrical and Electronics Engineers., ICGTSPICC 2016 : International Conference on Global Trends in Signal Processing, Information Computing and Communication : proceedings : 22-24 December 2016, Jalgaon, Maharashtra, India.

[14] M. Nikravan, A. Movaghar, and M. Hosseinzadeh, "A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks," Wirel Pers Commun, vol. 99, no. 2, pp. 1035–1059, Mar. 2018, doi: 10.1007/s11277-017-5165-4.

[15] J. Rani, A. Dhingra, and V. Sindhu, "A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network," in 2022 International Conference on Communication, Computing and Internet of Things, IC3IoT 2022 - Proceedings, 2022. doi: 10.1109/IC3IOT53935.2022.9768015.

[16] A. Dhingra and V. Sindhu, "A Study of RPL Attacks and Defense Mechanisms in the Internet of Things Network," in Proceedings of International Conference on Computing, Communication, Security.

[17] Nisha, A. Dhingra, and V. Sindhu, "A Review of DIS-Flooding Attacks in RPL based IoT Network," in 2022 International Conference on Communication, Computing and Internet of Things, IC3IoT 2022 - Proceedings, 2022. doi: 10.1109/IC3IOT53935.2022.9767875.