International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

EA-RPL: A Delay-Disruption Tolerant Approach for RPL-based IoT Networks against Inimical Attacks

Anamika Chauhan[1]

Submitted:12/03/2024 **Revised**: 27/04/2024 **Accepted**: 04/05/2024

Abstract: The IETF has introduced a protocol known as the Routing Protocol for Low Power and Lossy Networks (RPL) tailored for Low Power Lossy networks. RPL stands out as a lightweight routing protocol, making it particularly well-suited for IoT sensor networks. However, its lightweight nature leaves it vulnerable to various routing attacks. On the other hand, Delay Tolerant Networks represent another network category primarily focused on providing solutions that cater to delay, fault tolerance, and energy efficiency in resource-constrained environments. This paper provides a concise examination of the vulnerabilities of RPL and recognizes a resemblance in the identification of inactive nodes within a solution inspired by Delay Tolerant Networks. The research introduces a novel approach named EA-RPL, which is developed based on the monitoring of power consumption and statistical outlier analysis for identifying dormant nodes. The study involves the implementation and analysis of Flooding and DODAG Version attacks on RPL, and the simulations conducted in the Contiki OS and Cooja simulator yield promising proof-of-concept results. These results are based on the assessment of performance metrics encompassing radio duty cycle and energy consumption, which enable the successful identification of attackers.

Keywords: *Contiki, Cooja Simulator, DoS, DTN, IoT*

1. Introduction

Low-Power and Lossy Networks (LNN) serve as the foundation for Internet of Things (IoT) networks, playing a pivotal role. However, these networks grapple with several inherent limitations. They predominantly consist of sensor nodes, which operate under numerous constraints such as limited bandwidth, low data transmission rates, high packet loss, frequent topology changes, and the occurrence of link failures. Additionally, these sensor nodes are equipped with constrained on-board processing capabilities, memory, and energy resources.

Routing Protocols for Low Power and Lossy Networks (RPL) was conceived with the primary objective of bridging low-power sensor nodes with IoT networks. RPL's design philosophy centers around simplicity and flexibility, making it compatible with a wide range of resource-constrained devices. Consequently, this empowers a plethora of applications spanning across multi-hop mesh networks, encompassing industrial, urban, and domestic settings. RPL optimizes the utilization of smart device energy, establishes adaptable network topologies, and ensures efficient data routing. ("An efficient intrusion detection scheme for mitigating nodes using data aggregation in delay tolerant network." , September–2015) .

Despite its numerous advantages, RPL faces vulnerability to a variety of attacks, primarily classified into three categories: attacks on resources, traffic, and network topology. Safeguarding the security of RPL-based sensor IoT networks presents a formidable challenge. This research seeks to delve into the existing body of literature pertaining to these attacks and identify gaps in research, particularly in the realm of mitigating the security risks posed by DIS flooding and Version number attacks in IoT applications.

Several solutions including recent ML based techniques have been proposed by researchers, but are computationally extensive and thus not suitable for the LLN.[4][5] Delay Tolerant Networking (DTN) can fill this gap by providing alternative as well as hybrid solutions. Delay tolerant solutions are designed for challenged or infrastructure-lacking environments. A challenged network can be defined as a network with no stable and direct end-to-end path from source to destination. This is caused by such networks being infrastructure less [3,4,5]. It has frequent network disruptions and a lack of resources. The nodes are highly mobile and dynamic. DTN uses this very property of mobility of nodes to form paths opportunistically and deliver messages from one node to another node. The mobile nodes move in different clusters and carry and forward messages across the network to deliver them as destined. These networks initially had ad-hoc applications in areas such as tracking wildlife in difficult terrain using sensor networks, military, and underwater purposes, satellite networks, etc. Thus, they can aid in expansion of the RPL based services in constrained environment. Especially by enabling fault tolerance and enhancing security, by identification & mitigation of attacks.

The following objectives were outlined to achieve in the presented research:

- A detailed study of RPL protocol design and architecture is performed.

• The various attacks in RPL based IoT networks and existing solutions for RPL attacks are discussed.

• •The paper identifies the similarities and use of DTN energy optimizations solution used for one direct attack Flooding & one indirect attack DODAG Version attack on RPL for identification and mitigation.

• A resource (Energy) aware solution based on a delay tolerant routing mechanism is presented for design of an anomaly detection engine for identifying and isolating malicious nodes.

• As case study in a virtual environment with the scenario, implementation, and proof of concept performance evaluation of Robust RPL for Flooding & DODAG Version attacks are simulated

• The results of the simulation are discussed and further theoretical counter measures are also suggested.

2. IoT AND RPL

The realm of the Internet of Things (IoT), especially IP-based sensor networks, is characterized by its diversity and low-power nature [4][5][6]. Within this context, the Routing Protocol for Low-Power and Lossy Networks (RPL) is primarily integrated into the 6LoWPAN protocol stack and serves as a fundamental component for routing when employing IPv6. With IoT networks constantly evolving and incorporating a wide array of hardware and architectural variations to meet market requirements, it has become increasingly challenging to identify routing protocols, operating systems, and security solutions that can cater to all these diverse demands. To illustrate the common network-level architecture of IoT and the protocols employed, refer to Figure 1.

Application Layer	CoAP
Transport Layer	TCP, UDP
Network Layer	IETF RPL, IETF 6LoWPAN
MAC Layer	IEEE 802.15.4e IEEE 802.11 - WiFi Low Power for WLAN
Physical Layer (PHY)	IEEE 802.15.4

Fig. 1. Protocol stack for Low Power Lossy Network Communication

2.1. IoT based Sensor Network Challenges

An IoT based sensor network comprises of sensor nodes, which are devices with low-power, limited storage and processing capacity that work in small neighbourhood. The closely spaced sensors only perform small processing task & data collection to forward that information separately or collectively to a central device via other nodes. The nodes consist a computational and a communication module. The computing module comprises of an embedded processor that control hardware components, an operating System schedules tasks and processes data and memory. Both the modules require a power source to feed the sensor normally with batteries or capacitors. Since these devices are required to operate for long periods of time, they require minimal resource consumption as most sensors have limited power. There are also several characteristics that need consideration due to nature of the devices. The most relevant ones are briefly described in Fig 2.

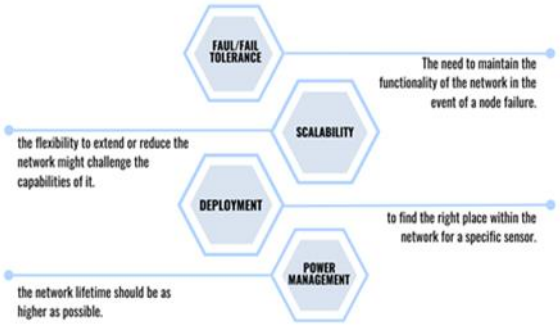

Fig. 2. LLN characteristics

2.2. Routing for Low Power Lossy networks RPL

The Routing Protocol for Low-Power and Lossy Networks (RPL) was developed by the Internet Engineering Task Force (IETF) Routing Over Low Power and Lossy Networks (ROLL) group to fulfil the essential routing requirements for building networks in resource-constrained environments. RPL operates by establishing a destination-oriented Directed Acyclic Graph (DODAG) to facilitate the connection and data dissemination among sensor nodes in a 6LoWPAN network. In this topology, RPL organizes the network into Directed Acyclic Graphs (DAGs), resembling tree-like structures, where each node is directly connected to another node, ensuring that loops are avoided. Loops, in this context, refer to paths that create circular connections within the network.

The DAG maintains default routes among nodes within a Low-Power and Lossy Network (LLN). A DODAG is a specialized type of DAG, with specific nodes within it designated as DAG roots. These root nodes serve as gateways and sinks for other nodes. In a DODAG, only one root exists, and it has no outgoing edges.

The network functions with one or more RPL instances, each comprising one or multiple DODAGs, identified by a unique RPL Instance ID. These RPL instances are logically independent and can run concurrently. Each node in the network can belong to only one DODAG within each instance but may participate in multiple RPL instances. RPL

follows a hierarchical structure, with nodes organized in parent-to-child relationships. However, it also supports a mesh topology to enable routing between sibling nodes.

The process of creating a RPL DODAG endows it with four key features: auto-configuration, self-healing, loop avoidance through detection, and transparency. RPL also permits the construction of multiple DAGs in a RPL network, each having its own root. A node can participate in multiple instances and assume different roles in each one, which enhances high availability and load balancing capabilities. To identify and maintain the network topology, RPL relies on four main values included in RPL control messages, as illustrated in Figure 3.

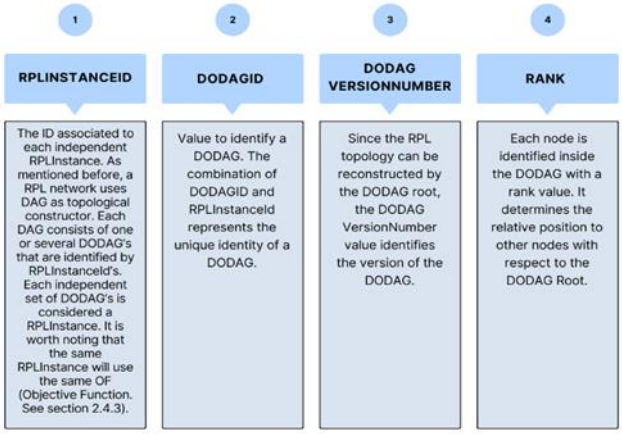

Fig. 3. Four main values within RPL control messages

2.3. RPL Protocol Network model

The following subsections give an overview about some of the key factors that determine the network model followed by RPL such as types of traffic flows, metrics applied to forward data among others.

Factors	Types/Definition
Traffic supported	Multipoint- to-point (MP2P) Point-to-multipoint (P2MP) Point-to-point (P2P).
Nodes	Host Routers Border routers
Rank	Abstract numeric value that provides a scalar representation of the location of a node within the DODAG Version.
Objective function (OF)	The OF determine the way that a node selects and/or enhances routes within a RPL instance.

Fig. 4. Taxonomy of RPL attacks

3. RPL Protocol Attacks

3.1. Attacks on RPL

Attacks on RPL may be divided into three broad categories depending on the mechanism used:

1. Instability and/or unavailability due to extenuation of resources

2. Topology disruptions

3. Traffic anomalies

A detailed taxonomy of the attacks is given in fig 5. This paper focuses on Flooding & DODAG Version attack which is are the two attacks on network resource. [6][7]

Flooding attack is performed by the attacker attempting to make a system asset, generally the server, inaccessible to the client nodes. This disconnects this node virtually and reduces system performance by briefly or indefinitely disrupting services offered by this server. Flooding is typically implemented by flooding the target server with innumerable dummy requests to overload systems, thereby preventing some or all the authentic requests from being fulfilled.

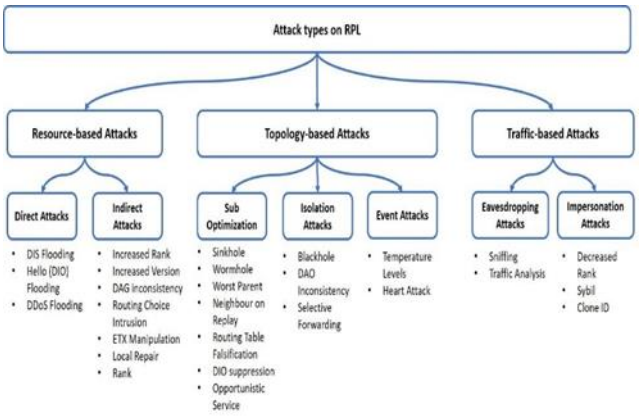

Fig. 5. Taxonomy of RPL attacks

3.2. Related work

As mentioned in Study, most real world IoT solutions use sensor devices in physical layer. These devices are resource constrained devices and if they can be depleted of resources, connectivity and availability will be denied. Flooding is one of the most common attacks; it has been a major concern in the RPL security.

RPL is lightweight in its design and the fact that nodes connected via Internet can be globally accessed makes them much more susceptible to such attacks. An attacker aims at overloading the target node with a huge amount of traffic using RPL-UDP pair. As UDP is connection-less in nature, absence of handshake tends to increase in the number of IP address spoofing attacks. This may easily lead to launch of Flooding attacks on LLN by attackers.[5][6][7]

At the network layer DIS can be launched by selective

forwarding. Thus, the conclusion is that IoT and Flooding together is a dangerous mix.

The RFC 7416 in its section 7.3.2 suggests countermeasures for mitigating Flooding by creating limit on the traffic that a node may send referred to as quotas, variation in traffic when nodes that exceed that quota or allow only data may be used to block such nodes. Another study suggests including a system that can provide authentication method for identity verification of the nodes, and integrity of the data. Despite several countermeasures being put in place, message being transmitted consume energy of the receiver used in rejecting, dropping, or accepting the packet. Consequently, the above-mentioned mechanisms would not be able to provide any solution to this problem. Hence, it can be said that, mitigation of Flooding attack by means of authentication or encryption may consume energy or resources but cannot offer security. Therefore, IDS (Intrusion detection system) that can help to detect intruders would be more suitable in detecting and preventing such attacks.

Having seen the impact that this attack has regarding nodes power consumption and based on published related work a solution to detect this type of attack is described. This works does further research on power consumption as a feature for attack identification.

4. DTN And IoT Interdependency

DTN & IOT During the same period as IoT another class of networks the Delay/Disruption Tolerant Networks (DTN), sometimes also referred to as Opportunistic Networks (ON) was developed for providing routing in a challenged network where no stable end-to-end path is available [4]. A challenged network can be defined as a network with no stable and direct end-to-end path from source to destination. This is caused by such networks being infrastructure-less [3,4,5]. It has frequent network disruptions and a lack of resources. The nodes are highly mobile and dynamic. DTN uses this very property of mobility of nodes to form paths opportunistically and deliver messages from one node to another node. The mobile nodes move in different clusters and carry and forward messages across the network to deliver them as destined. These networks initially had ad-hoc applications in areas such as tracking wildlife in difficult terrain using sensor networks, military, and underwater purposes, satellite networks, etc.

The reason for DTN successfully working in this application is that it overcomes the difficulty of accessing the network continuously, even in remote or dynamic environments where there is no guarantee of the availability of a complete and stable path from source to destination. The traditional infrastructure-based routing protocols quite naturally due to the nature of their design fail to deliver in such a challenging environment.

Literature analysis shows several similarities between the design issues, node/ traffic behavior and resource constraints, and performance metrics of DTN and IoT. This has led to an array of solutions being designed with hybrid mechanisms. The DTN-enabled IoT network solutions enable smart objects to effectively communicate with more efficiency even in the presence of frequent disruptions. This also addresses the much larger issue of lifetime constraints. Recent studies have shown that DTN within the IoT framework provides the most suitable and satisfactory results.

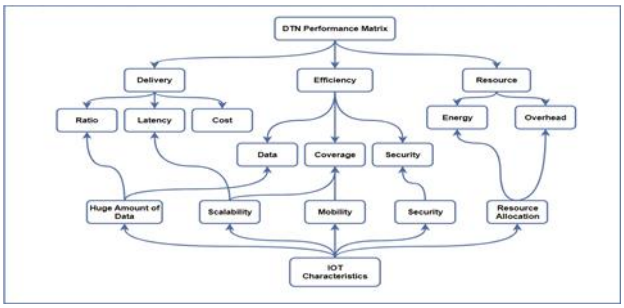

Fig. 6. Interdependency of DTN and IoT

5. Proposed Framework

The proposed EA-RPL approach consists of two conceptual modules:

A.Part A for the calculation of rate of drain of energy by residual energy measurement which is DTN inspired Dead Node identification method and then

B.Part B for anomaly detection based on outlier analysis to identify intrusion for mitigation of attack. The features of EA-RPL specifications are used to check for the power consumption pattern and detect anomaly.[2]

5.1. Energy efficient Dead node identification in DTN

DTN are resource constrained and messages must be transmitted to nodes having high encountering ability, for maximising efficiency and lifetime. Hence, any message transmission to a destination which is about to be dead, causes wastage of network resources because any messages destined to or passing via dead/nearly dead node will never reach destinations. Also, any Node with high battery drainage will die early. The delay tolerant network transmits multiple copies of each message that lead to higher resource consumption.

The objective function for DTN is optimised and controlled by forwarding the messages via nodes with high encountering ability. This will ensure intermediate nodes lose energy only in transmission and reception. This requires that for Energy Efficiency messages must avoid inactive and dead nodes. Dead node will not be able to forward any messages to their destinations. [2]

Authors propose an anomaly detection mechanism based on

a routing protocol for Delay Tolerant Network based on Optimising the Objective Function based on Destination to Dead node, which is a function of connectivity and delay in encounter time. The same principle may be applied to server nodes under attack the delay in processing is the Objective function of CPU power and Transmission Power.

5.2. Anomaly detection engine-based Outlier analysis

The methodology introduced comprises several key elements, including hypothesis formation, testing, observation, and drawing conclusions. The initial hypothesis posits that in a network employing RPL, nodes may exhibit abnormal power consumption patterns when subjected to attacks. Such nodes will display a distinctive power drainage behaviour that significantly deviates from typical observations, raising suspicions of a distinct underlying cause. These exceptional observations are commonly referred to as outliers, representing data points that appear inconsistent with the rest of the dataset [7].

Depending on the information scope considered for outlier detection, outliers can be categorized as either global or local. In the experimental results that follow, the anomalies are revealed to be local outliers. Detecting and eliminating local outliers help reduce the communication overhead, subsequently leading to a reduction in overall energy consumption.

It is worth noting that outliers can stem from various sources, including noise, errors, and other events, not just malicious attacks. However, this research primarily focuses on outliers induced by malicious attacks, specifically concerning network security.

Statistical-based methods offer a straightforward approach to handle outlier detection. These techniques are model-based and prove particularly effective in sensor-based networks and Low-Power and Lossy Networks (LLN) due to their minimal overhead. In this context, the Mean and Standard Deviation Method serves as the predictor. The detection of DIS Flooding attacks and Version Attacks is accomplished using statistical outlier analysis. This process involves the simulation of the EA-RPL Protocol, the collection of power-related data, and the computation of Power Consumption and Radio Duty Cycle percentages for different nodes. The calculations for both parameters adhere to the following formulas:

Energy consumption (Power in mW) represented as E may be defined as given in equation 1

$$E = \frac{Energest\_Value \times Current \times Voltage}{RTIMER\_SECOND \times Runtime} \quad \text{…. Equation 1}$$

Radio Duty Cycle% of node represented as **R** is defined as

$$R = \frac{Energest\_TX + Energest\_RX}{Energest\_CPU + Energest\_LPM} \quad \text{…. Equation 2}$$

Architectural flow for proposed method is given in Fig. 7.

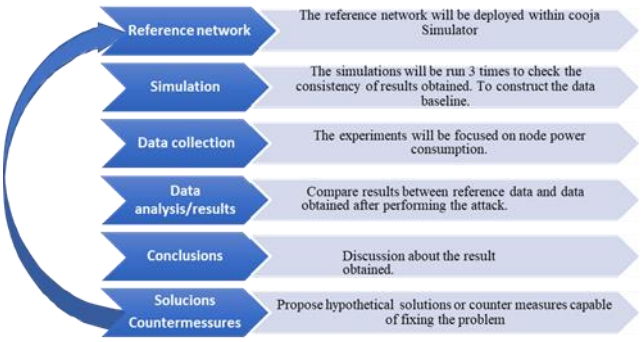

Fig. 7. Architectural flow for proposed method

6. Implementation

To simulate the impact of an attack on the lower three layers of the UDP/IP/RPL protocol stack, TCP implementation is carried out using the Contiki-Cooja pair. These layers are particularly vulnerable in resource-constrained IoT nodes. Contiki OS, in conjunction with the Cooja simulator, is chosen due to its minimalist feature set that is well-suited for a complete TCP/UDP/IP/RPL stack [1].

Contiki, an operating system designed for memory-constrained and networked environments, is tailored for low-power wireless devices. The Collect View application, an integrated power profiler in Contiki OS, is employed for power parameter measurements. The required parameters include transmission time, receiving time, LPM power, and CPU power. Utilizing relevant formulas, the Power Consumption and Radio Duty Cycle percentages are calculated, and graphical representations are generated. Subsequently, an Outlier Analysis is conducted to identify both attackers and victim nodes.

The IoT scenario simulation utilizes RPL as the routing protocol for various network topologies. Power Consumption and Radio Duty Cycle percentages are computed for all nodes. The implementation methodology involves a comparison between the network under attack and a baseline reference network. Hence, it begins with the deployment of a reference network, followed by the deployment of different malicious nodes to simulate attacks. To achieve the simulation attacks, RPL configuration files are modified, resulting in changes in node behavior.

The values of the reference network are measured through the Cooja GUI, and the power consumption data from the nodes is collected. Each attack is then deployed to demonstrate how nodes may experience altered power consumption in the presence of an attack. The reference network consists of two types of motes: a sink node, which functions as a Low power and Lossy Network Border Router (LBR) and DODAG router, and leaf motes, serving as wireless sensor collectors [Fig 2].

To maintain a realistic simulation environment, a 100x100-

meter area with randomly distributed motes is used. This ensures that the simulation closely mimics real-world conditions.

The primary objective when simulating an attack is to modify the behavior of a mote or motes without altering the normal behavior of the rest of the network members. Doing so, it can be assessed how the network reacts to unusual situations.

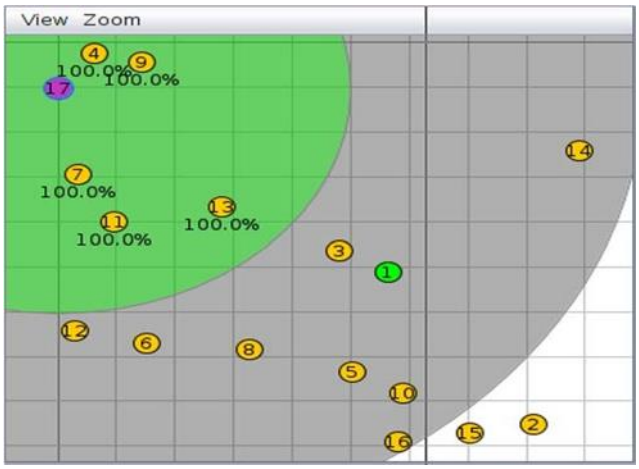

Fig. 8. Reference Network with a Malicious Mote

The method used to achieve that approach can be accomplished by following the steps below:

- Duplicate the Contiki folder to create a new Contiki O.S. instance.
- Modify the correspondent files according to the attack.
- Create and add new malicious mote(s) compiling the node firmware within the new Contiki instance, to the reference network.
- Run the network

The simulation parameters for testing EA-RPL are given in Table 4.

Table 1. Simulation Parameters

Simulation Parameters	
Simulation tool	Contiki 3.0 Cooja simulator
Mote type	Sky mote
Source code motes	Contiki/examples/ipv6/rpl-collect
Source code malicious	ContikiX/examples/ipv6/rpl-collect
Simulation run time	600 seconds
Number of leaf nodes	16
Total number of modes with malicious	17
Sink node	1
Legitimate nodes	15
Malicious	1
Radio Medium	UDGM6: Distance Loss
Transmission range	50m
Interference range	100m
Mote start delay	1,000
Random seed	123,456
Positioning	Random positioning

Table 2. Parameters obtained under DIS Flooding Attack

Node	CPU Power	LPM Power	Listen Power	Transmitting Power	Total Power
2	0.529437	0.14747	1.164172	1.216901	3.05798
3	0.519456	0.147772	1.342622	0.804244	2.814094
4	1.862863	0.107097	20.62037	2.087472	24.6778
5	0.558204	0.146599	1.208506	1.067168	2.980477
6	0.669933	0.143216	1.941257	1.653602	4.408008
7	2.055413	0.101267	21.08135	2.653331	25.89136
8	0.658032	0.143576	1.804332	1.607205	4.213146
9	2.249478	0.095391	24.84559	2.339792	29.53025
10	0.536049	0.14727	1.319688	1.183416	3.186423
11	1.94192	0.104703	21.68966	1.578212	25.3145
12	1.911479	0.105625	22.16001	1.839849	26.01696
13	2.081404	0.10048	22.60831	1.082049	25.87225
14	0.401297	0.15135	0.628189	0.652141	1.832977
15	0.438142	0.150234	0.977078	0.628442	2.193896
16	0.324334	0.15368	1.311769	0.451707	2.241489

Table 3. Parameters obtained under Version Attack

Node	CPU Power	LPM Power	Listen Power	Transmitting Power	Total Power
2	0.602729	0.145251	1.143023	1.293798	3.1848
3	0.726128	0.141514	1.665977	1.35384	3.88746
4	0.774497	0.14005	1.898859	2.45655	5.269957
5	0.693996	0.142487	1.528769	1.260165	3.625417
6	0.739039	0.141124	1.929971	1.379761	4.189893
7	0.686793	0.142705	1.444965	1.531812	3.806276
8	0.755925	0.140612	1.932812	1.304027	4.133376
9	0.712355	0.141931	1.636302	2.112633	4.60322
10	0.655797	0.143644	1.401083	1.232513	3.433037

11	0.741452	0.14105	1.803722	1.699925	4.386149
12	0.710229	0.141996	1.534094	1.963687	4.350006
13	0.847708	0.137833	2.26769	1.801375	5.054605
14	0.665057	0.143364	1.328748	2.127283	4.264451
15	0.634679	0.144283	1.300595	1.192799	3.272357
16	0.658718	0.14355	1.3268	1.365794	3.494948

7. Results and Analysis

A DIS attack is a direct assault targeting network resources, characterized as a flooding attack designed to overwhelm nodes and links by generating a significant volume of traffic. The objective of simulating this attack is to comprehend the impact on power consumption experienced by leaf nodes when a malicious node initiates a DIS attack in a wireless sensor network. Subsequently, the results will inform the exploration of potential theoretical solutions or, if feasible, the implementation of countermeasures against this specific attack.

Conversely, a version attack is an indirect offensive tactic in which a malicious node introduces a higher version number for a DODAG tree. Nodes receiving DIO messages with the new version number begin to establish a new DODAG tree. This attack disrupts the network by introducing inconsistencies and inefficiencies into its topology. The simulation aims to elucidate the consequences of leaf nodes repeatedly receiving DIO messages with higher versions and their impact on mote energy consumption. Furthermore, this investigation will explore potential theoretical solutions or, where feasible, practical implementations to mitigate this particular attack.

The graphical representation in Figures 7 and 8 illustrates the disparity between the average parameters of unaffected nodes and attacker nodes. The data clearly reveals that the radio duty cycle percentage for nodes under attack or acting as attackers is significantly higher than that of regular nodes. This outcome aligns with the initial theoretical hypothesis upon which the experimentation was based.

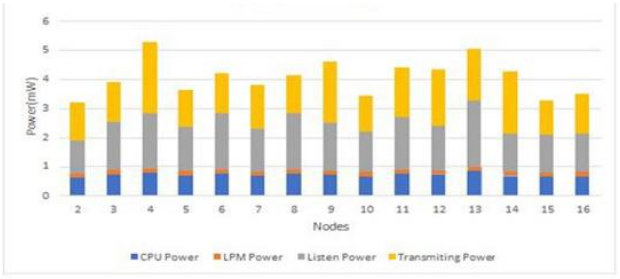

Fig. 9. Nodes Consumption by CPU, LPM, Listen and Transmitting Power – DIS Flooding Attack

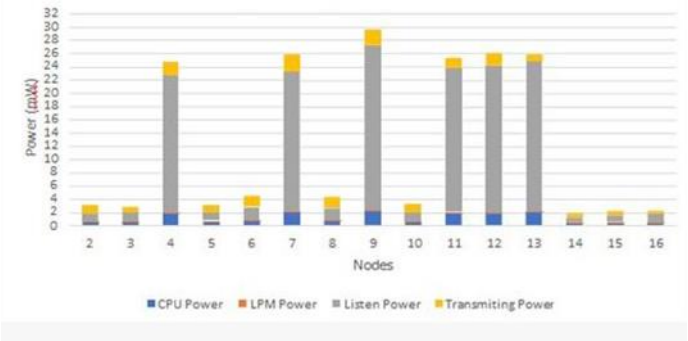

Fig. 10. Nodes Consumption by CPU, LPM, Listen and Transmitting Power –Version Attack

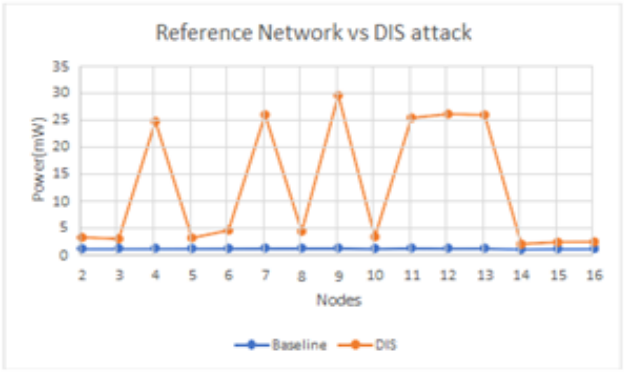

Fig. 11. Power Consumption Difference Between Reference Network and DIS Attack

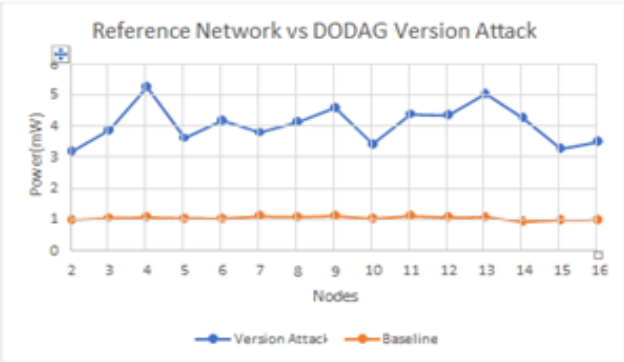

Fig. 12. Power Consumption Difference Between Reference Network and Version Attack

Table 4. Consumption Differences Between Reference Network and DIS Attack in Percentage

Node	CPU Power	LPM Power	Listen Power	Transmitting Power	Total Power
2	50.73%	-3.53%	175.34%	1686.32%	207.32%
3	28.91%	-2.33%	201.99%	1380.74%	167.20%
4	439.65%	-30.02%	4464.80%	1552.05%	2192.78%
5	42.77%	-3.34%	173.21%	1553.23%	183.98%
6	71.76%	-5.59%	329.44%	3100.63%	321.65%
7	457.53%	-33.52%	4400.12%	2094.64%	2231.79%
8	61.41%	-5.01%	284.91%	2505.18%	286.77%
9	536.20%	-37.57%	5289.45%	1391.67%	2526.70%
10	40.46%	-3.08%	201.52%	1747.37%	207.77%
11	400.11%	-31.00%	4514.19%	1290.59%	2152.99%
12	442.29%	-30.89%	4810.18%	1503.86%	2328.46%
13	411.89%	-33.54%	4714.20%	1714.25%	2280.02%
14	26.76%	-1.67%	54.57%	1120.36%	97.02%
15	19.23%	-1.40%	129.45%	1189.26%	120.62%
16	-11.67%	0.85%	205.87%	732.94%	123.55%

Table 5. Consumption Differences Between Reference Network and Version Attack in Percentage

Node	CPU Power	LPM Power	Listen Power	Transmitting Power	Total Power
2	71.59%	-4.98%	170.34%	1799.20%	220.06%
3	80.20%	-6.47%	274.73%	2392.62%	269.12%
4	124.36%	-8.49%	320.36%	1844.15%	389.62%
5	77.50%	-6.05%	245.61%	1852.21%	245.43%
6	89.48%	-6.97%	326.94%	2570.59%	300.78%
7	86.29%	-6.32%	208.45%	1167.00%	242.80%
8	85.42%	-6.98%	312.32%	2013.74%	279.45%
9	101.47%	-7.11%	254.94%	1246.85%	309.45%
10	71.84%	-5.46%	220.11%	1824.01%	231.59%
11	90.95%	-7.05%	283.72%	1397.83%	290.37%
12	101.49%	-7.09%	239.92%	1611.81%	306.04%
13	108.48%	-8.83%	382.88%	2920.33%	364.98%
14	110.08%	-6.86%	226.96%	3880.81%	358.38%
15	72.72%	-5.31%	205.43%	2347.04%	229.07%
16	79.39%	-5.79%	209.39%	2418.50%	248.56%

As can be seen in the Fig. 8. when an attacker is present or the server is under attack its duty cycle % is approximately 100%. This is an indication that it is active all the time during the simulation. The case for nodes far away is visibly different. The other node's duty cycle is falling in a much lower range. It is Firstly affecting the nodes in its range then all other nodes deployed in the region. This is due to request packets being generated in high number causing the flooding attack. It can also be concluded confidently from the above Fig 6 that the power consumption measured in Mw is also comparatively higher than the other nodes excluding server. So, the rate of battery drainage rate for attacker is also much higher that rate of battery drainage for other nodes.

8. Conclusion

Based on the results derived from the implementation of the proposed approach, it is conclusively established that the initially assumed hypothesis is indeed valid. The simulations conducted within the Contiki-OS Cooja simulator confirm the alignment of deductions with the original hypothesis. This approach serves as a proof-of-concept identification method and offers a computationally efficient alternative for analysing network parameters to detect and prevent various threats to the network. The significance of deriving this solution from delay-tolerant routing, despite its resource constraints, introduces several notable advantages:

1. Implementation does not necessitate the introduction of new parameters or fields. It relies on predefined patterns, such as the mode of operation of RPL or anomaly-based triggers (e.g., alerting when power consumption exceeds a specific threshold or when certain message types exceed normal behaviour).

2. In terms of scalability and energy efficiency, the implementation is straightforward.

3. It can function as a Network-based Intrusion Detection System, allowing for the seamless addition of new nodes to the network without the need to install a new host-based IDS on each node.

4. This approach also mitigates potential incompatibilities (e.g., operating systems, firmware) since it requires no hardware modifications.

5. Moreover, this solution doesn't impact the performance or power consumption of nodes, eliminating the need for constant power supplies and avoiding added complexity due to encryption or authentication mechanisms, making it a lightweight and practical solution.

9. References

（"An efficient intrusion detection scheme for mitigating nodes using data aggregation in delay tolerant network." , September–2015, ）

[1] A. Conta, Deering, S., M. Gupta, E. (2006). RFC 4443:Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. RFC 4443, 53(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

[2] Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. Journal of Network and Computer Applications, 66, 198–213. https://doi.org/10.1016/j.jnca.2016.03.006

[3] （Wireless sensor networks: a survey. Computer Networks, , (2002). , ）Chen, Y., Chanet, J.-P., Hou, K.-M., Shi, H., & De Sousa, G. (2015). A Scalable Context-Aware Objective Function (SCAOF) of Routing Protocol for Agricultural Low-Power and Lossy Networks (RPAL). Sensors, 15, 19507–19540. https://doi.org/10.3390/s150819507

[4] D'Hondt, A., Bahmad, H., & Vanhee, J. (2016). RPL Attacks Framework. Retrieved from https://github.com/dhondta/rpl-attacks/blob/master/doc/report.pdf

[5] Dodig-crnkovic, G. (2002). Scientific Methods in Computer Science. Computer (Long.

[6] Beach. Calif)., 126–130. Retrieved from http://poincare.math.rs/~vladaf/Courses/Matf MNSR/Literatura/Scientific Methods in Computer Science.pdf

[7] Dodis, Y., Kiltz, E., Pietrzak, K., & Wichs, D. (2012). Message Authentication, Revisited (pp. 355–374). https://doi.org/10.1007/978-3-642-29011-4_22

[8] Dohler, M., Daza, C. V, & Lozano, A. (2012). draft-ietf-roll-security-framework-07 - A Security Framework for Routing over Low Power and Lossy Networks.

[9] Dohler CTTC Daza A Lozano Universitat Pompeu

Fabra M Richardson, M. V. (2015).

[10] RFC 7416 - A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks …RPLs—.

[11] Dunkels, A., Schmidt, O., Finne, N., Eriksson, J., Österlind, F., & Durvy, N. T. M. (2011). The Contiki OS: The Operating System for the Internet of Things.

[12] Online], at Http://www. Contikios. Org.

[13] Dvir, A., Holczer, T., & Buttyan, L. (2011). VeRA - Version number and rank authentication in RPL. Proceedings - 8th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, MASS 2011, 709–714.

[14] https://doi.org/10.1109/MASS.2011.76

[15] Evans, D. (2011). The Internet of Things - How the Next Evolution of the Internet is Changing Everything. CISCO White Paper, (April), 1–11. https://doi.org/10.1109/IEEESTD.2007.373646

[16] Farooq, M. U., Waseem, M., & Khairi, A. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111(7).

[17] Gaddour, O., & Koubâa, A. (2012). RPL in a nutshell: A survey. Computer Networks, 56(14), 3163–3178. https://doi.org/10.1016/j.comnet.2012.06.016

[18] Kelsey, R. (2015). 7/17/2015 RFC 6550 - RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, 1–314. https://doi.org/10.17487/rfc6550

[19] Kirichek, R., & Koucheryavy, A. (2016). Internet of Things Laboratory Test Bed. In Wireless Communications, Networking and Applications, Wcna 2014. https://doi.org/10.1007/978-81-322-2580-5_44

[20] Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sensors Journal, 13(10), 3685–3692. https://doi.org/10.1109/JSEN.2013.2266399

[21] Levis, P., Clausen, T., Hui, J., Gnawali, O., & Ko, J. (2011). RFC 6206 - The Trickle Algorithm. Internet Requests for Comments. https://doi.org/10.1017/CBO9781107415324.004

[22] Marco, P. D. I. (2008). Protocol Design and Implementation for Wireless Sensor Networks. Piergiuseppe Di Marco, (April). Retrieved from https://www.diva-portal.org/smash/get/diva2:572787/FULLTEXT01.pdf

[23] Mayzaud, A., Badonnel, R., & Chrisment, I. (2016). A Taxonomy of Attacks in RPL- based Internet of Things. International Journal of Network Security IJNS, 18(3), 459–473. Retrieved from https://hal.inria.fr/hal-01207859

[24] Moteiv. (2006). T-Mote Sky Datasheet. Electronics, 1–28.

[25] Nataf, E., & Festor, O. (2012). Online Estimation of Battery Lifetime for Wireless Sensor Network, (September), 28. Retrieved from https://arxiv.org/pdf/1209.2234.pdf

[26] Perrey, H., Landsmann, M., Ugus, O., Schmidt, T. C., & Wählisch, M. (2013). TRAIL: Topology Authentication in RPL. 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 73–74.

[27] https://doi.org/10.1109/INFCOMW.2013.6970745

[28] Pongle, P., & Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. In 2015 International Conference on Pervasive Computing (ICPC) (pp. 1–6). IEEE. https://doi.org/10.1109/PERVASIVE.2015.7087034

[29] RGHIOUI, A., KHANNOUS, A., & BOUHORMA, M. (2014). Denial-of-Service attacks on 6LoWPAN-RPL networks: Issues and practical solutions. Journal of Advanced Computer Science & Technology, 3(2), 143. https://doi.org/10.14419/jacst.v3i2.3321

[30] Ruckebusch, P., Devloo, J., Carels, D., De Poorter, E., & Moerman, I. (n.d.). An evaluation of link estimation algorithms for RPL in dynamic wireless sensor networks. Retrieved from http://www.wishful-project.eu/sites/default/files/scube_2015.pdf

[31] Sharma, D., Assistant, S., Mishra, I., & Jain, S. (n.d.). ISSN: 2454-132X Impact factor: 4.295 A Detailed Classification of Routing Attacks against RPL in Internet of Things. International Journal of Advance Research Ideas and Innovations in Technology. Retrieved from https://www.ijariit.com/manuscripts/v3i1/V3I1-1257.pdf

[32] Shukla, P., & Professor, A. (2007). Comparative Analysis of Distance Vector Routing & Link State Protocols. International Journal of Innovative Research in Computer and Communication Engineering (An ISO Certified Organization), 3297(10). https://doi.org/10.15680/IJIRCCE.2015

[33] Sunshine, C. A. (1977). Source routing in computer networks. ACM SIGCOMM Computer Communication Review, 7(1), 29–33. https://doi.org/10.1145/1024853.1024855

[34] Thomson, C. (2016). Cooja Simulator Manual, (C), 2015–2016. https://doi.org/10.13140/RG.2.1.4274.8408

[35] Thubert, P. (2012). RFC 6552 - Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL). Internet Requests for Comments, 1–14. https://doi.org/10.1017/CBO9781107415324.004

[36] Vasseur, J.-P., & Dunkels, A. (2010). RPL Routing in Smart Object Networks. Interconnecting Smart Objects with IP. https://doi.org/10.1016/B978-0-12-375165-2.00017-X

[37] Vasseur, J., Fellow, C., Systems, C., Agarwal, N., Leader, T., & Hui, J. (2011). RPL: The IP routing protocol designed for low power and lossy networks Internet Protocol for Smart Objects (IPSO) Alliance.

[38] Vijayarani, S., Maria, M., S, S., & Professor, A. (2015). INTRUSION DETECTION SYSTEM – A STUDY. International Journal of Security, Privacy and Trust Management, 4(1). https://doi.org/10.5121/ijsptm.2015.4104

[39] Wang, Q., & Balasingham, I. (n.d.). Wireless Sensor Networks -An Introduction 1 0 Wireless Sensor Networks -An Introduction. Retrieved from http://cdn.intechweb.org/pdfs/12464.pdf

[40] "An efficient intrusion detection scheme for mitigating nodes using data aggregation in delay tolerant network." . NavazASSyed, J. Antony Daniel Rex, and P. Anjala MarySeptember–2015, . International Journal of Scientific & Engineering Research, Vol No-6.