International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

December 2024 | Issue 61 | Volume 16 | Number 4 | Pages 106-119

ENHANCING IOT SECURITY: A COMPREHENSIVE FRAMEWORK FOR ENERGY AND RADIO DATASET GENERATION TO MITIGATE IOT RPL ATTACKS

A. Krari A. Hajami A. Toubi M.A. Said

Laboratory of Research Watch for Emerging Technologies, Faculty of Sciences and Technology, Hassan I University, Settat, Morocco
ayoub.krari@uhp.ac.ma, abdelmajid.hajami@uhp.ac.ma, ayoub.toubi@uhp.ac.ma, ma.aitsaid@uhp.ac.ma

Abstract- The rapid proliferation of IoT networks for critical fields, such as healthcare, industrial automation, and smart cities, brings into sharp focus the urgent need to ensure their security. IoT networks are inherently very vulnerable due to their energy-constrained nature and radio transmission dependence. Such factors make RPL one of the most susceptible protocols to various attacks, directly influencing network reliability and resilience. These include the DIS flood attack, which has grave threats in energy-sensitive applications. This paper, therefore, conceptualizes a systematic methodology in the design of energy and radio datasets to detect attacks in IoT networks, considering one of the critical attacks: the DIS Flood attack in RPL-based networks. The performed simulations of normal and attack scenarios in Cooja, which provides real-time power consumption and radio activity metrics. Our approach will allow for the accurate tracing of power and logging of radio activity, hence providing a dataset that will reflect network behavior both in benign and attack conditions. Our results indicate huge disparities in energy consumption and radio metrics at the instances of attacks, showing critical vulnerabilities in IoT networks. These datasets were then used to develop models for machine learning and deep learning, and the overall efficacy provided by these models in detecting DIS Flood attacks was high. Precisely, some of the deep learning models realized detection accuracies of over 95%, further improving over traditional rule-based approaches. This is an important research area, considering that IoT devices continue to be installed in sensitive applications and that security breaches may lead to disastrous situations. The work presented here contributes to both IoT network resilience and energy efficiency. Thus, this will bring more effective detection systems and contribute to a robust security architecture for the fast-evolving landscape of IoT.

Keywords: IoT Security, RPL Protocol, DIS Flood Attack, Energy Consumption, Radio Metrics, Machine Learning, Deep Learning, Power-Trace, Cooja Simulation, Intrusion Detection System (IDS), Datasets.

1. INTRODUCTION

The exponential increase in IoT achieved unprecedented connectivity regarding smart cities, industrial automation, healthcare, and agriculture. However, this phenomenal increase in networked devices has also caused severe challenges to security, particularly for energy efficiency and radio communications of these networks. This is more relevant to the RPL, which forms the basis of many IoT deployments and stands out as being highly vulnerable against attacks that try to disrupt the stability of the network, increase energy consumption, and degrade its performance.

Power and radio represent two of the most important resources in IoT networks, directly affecting the durability and reliability of distributed systems. Security of these components is highly important in resource-scarce and low-power environments, since attacks can lead to huge deteriorations. The most well-known one is a DODAG Information Solicitation DIS Flood attack, where malicious nodes flood the network with solicitation signals forcing other nodes to uselessly waste their energy. That proves the need for sound security addressing different attack types and scenarios.

Thus, the detection of DIS Flood attacks becomes challenging because they rely on energy drainage and increasing radio activity on resource-constrained nodes. The traditional methods usually fail to recognize these energy-related impacts, and hence early detection becomes hard, which puts network resilience in jeopardy. This work will introduce a new approach based on the comprehensive creation of energy and radio datasets for ML and DL models. Different from existing works focusing on a single attack or certain specific metrics, the proposed framework captures a wide range of network activities both in normal and under-attack status. Integrating power trace data enables the recording of real-time energy and radio metrics, thereby allowing our methodology to develop more accurate detection models. This Approach Contributes Not Only to Early Detection but Also to Long-Term Energy Efficiency and survivability in IoT networks.

Registered: 240705
Reserved: 240916
Article Info: 1905
Accepted: 241126
Available: 241231

This timeliness of the study underpins the increasing deployment of IoT in critical applications where security breaches might have serious implications. Holistic dataset creation may provide a base for developing advanced ML/DL models dealing not only with energy but also with radio metrics. The contribution of this paper is new in providing a comprehensive dataset and an adaptable methodology toward improving resilience and energy efficiency in IoT deployments, considering a significant step forward in IoT security research.

2. RELATED WORKS

Recent years have included significant research efforts aimed at Elevating the security of Internet of Things (IoT), including those that use the (RPL). Multidisciplinary research has investigated multiple aspects of IoT security, encompassing the advancement of IDS, the implementation of machine and deep learning methodologies, and the generation of specialized datasets tailored to specific attack categories. Nevertheless, a prevalent constraint in this research is the insufficient attention given to energy and radio-specific datasets, which are crucial for comprehending the whole consequences of attacks on IoT networks.

Table 1 presents a comprehensive comparison of significant research endeavors in this field, emphasizing the employed methodology, suggested contributions, reported results, and recognized limits. A comparison study highlights the distinct benefit of our proposed work, which fills these gaps by offering a complete framework for creating energy and radio information specifically designed for different attack scenarios in IoT networks.

Table 1. Advancements in RPL IoT datasets generation

Work	Methodology Used	Proposed Work	Results	Limitations
[6]	Developed a data collection framework for IoT IDS, tailored for 6LoWPAN/RPL and CoAP protocols.	Created a dataset tailored to IoT environments to address IDS limitations with existing datasets.	Demonstrated the dataset's applicability to IoT security needs with a focus on specific protocols.	No specific focus on other RPL attacks beyond dataset creation. Lacks emphasis on energy and radio dataset generation, relying on general network datasets with limited captured features.
[7]	Methodical evaluation of machine learning and deep learning techniques for identifying attacks in RPL-based 6LoWPAN Internet of Things networks.	Analyzed existing ML and DL techniques, identified challenges, and proposed future research directions.	Identified gaps in current research and proposed improvements in ML/DL methodologies.	Review-based; lacks practical implementation or experimental results. Does not generate energy and radio datasets, depending on generic network data with a limited scope of captured features.
[8]	Simulated IoT networks to create a comprehensive dataset for sinkhole attacks using COOJA.	Introduced UOS_IOTSH_2024 dataset focusing on sinkhole attacks in RPL-based IoT networks.	Provided a diverse dataset covering multiple attack scenarios, aiding in the development of detection methods.	Focus limited to sinkhole attacks; no exploration of other attack types. Does not address energy and radio-specific datasets, relying on broader network datasets with a restricted range of features.
[9]	Proposed an ANN model for detecting decreased rank attacks using IRAD dataset.	Developed an ANN-based detection framework for RPL-based IoT networks.	Achieved high accuracy in detecting decreased rank attacks in RPL networks.	Limited to decreased rank attacks; did not cover other RPL attack types. Lacks focus on generating energy and radio datasets, utilizing general network datasets with minimal feature capture.
[10]	Developed a hybrid DL-based IDS using IoTR-DS dataset for detecting multiple RPL attacks.	Hybrid DL model combining supervised and semi-supervised learning to detect known and unknown attacks.	Achieved 98% accuracy for known attacks and 95% for unknown attacks in RPL networks	Dependent on dataset quality; performance may vary with different datasets. Does not concentrate on energy and radio data, instead relying on generalized network datasets with a narrow feature set.
Proposed Work	Investigated IoT network security challenges, focusing on energy and radio metrics. Employed a comprehensive framework for dataset generation using power trace data to capture both normal and attack scenarios in RPL-based IoT networks.	Developed a methodology to create energy and radio datasets specifically for IoT environments, enabling the detection and mitigation of various attacks using machine learning and deep learning models.	Showcased the effectiveness of the proposed dataset in identifying and mitigating IoT network attacks, particularly enhancing the detection capabilities for energy-related anomalies and radio disruptions.	

3. METHODOLOGY

3.1. Methodology Description

The proposed methodology as shown in Figure 1 will emulate the normal and attack behaviors in IoT networks by applying the Koja simulator [11]. Simulations to be conducted are those that will serve to produce traffic data in two scenarios: normal traffic and an RPL flood attack scenario. Thus, benign and malicious network traffic data will be collected to have an integral view of network activity under various conditions. This is done by tracing in the simulator, where real-time power consumption and radio communication are observed.

This change in code was implemented on Koja by applying the power trace functions necessary for the simulator to generate the power and radio metrics accordingly. From these collected metrics, twelve special features are extracted, related to energy and radio, the datasets are then prepared as benign and as malicious datasets. These last datasets have been additionally preprocessed to be made ready for machine learning and deep learning models' implementations. The proposed framework avails an overall technique for developing newer datasets that can contribute toward a more secure and energy-efficient development in IoT networks.

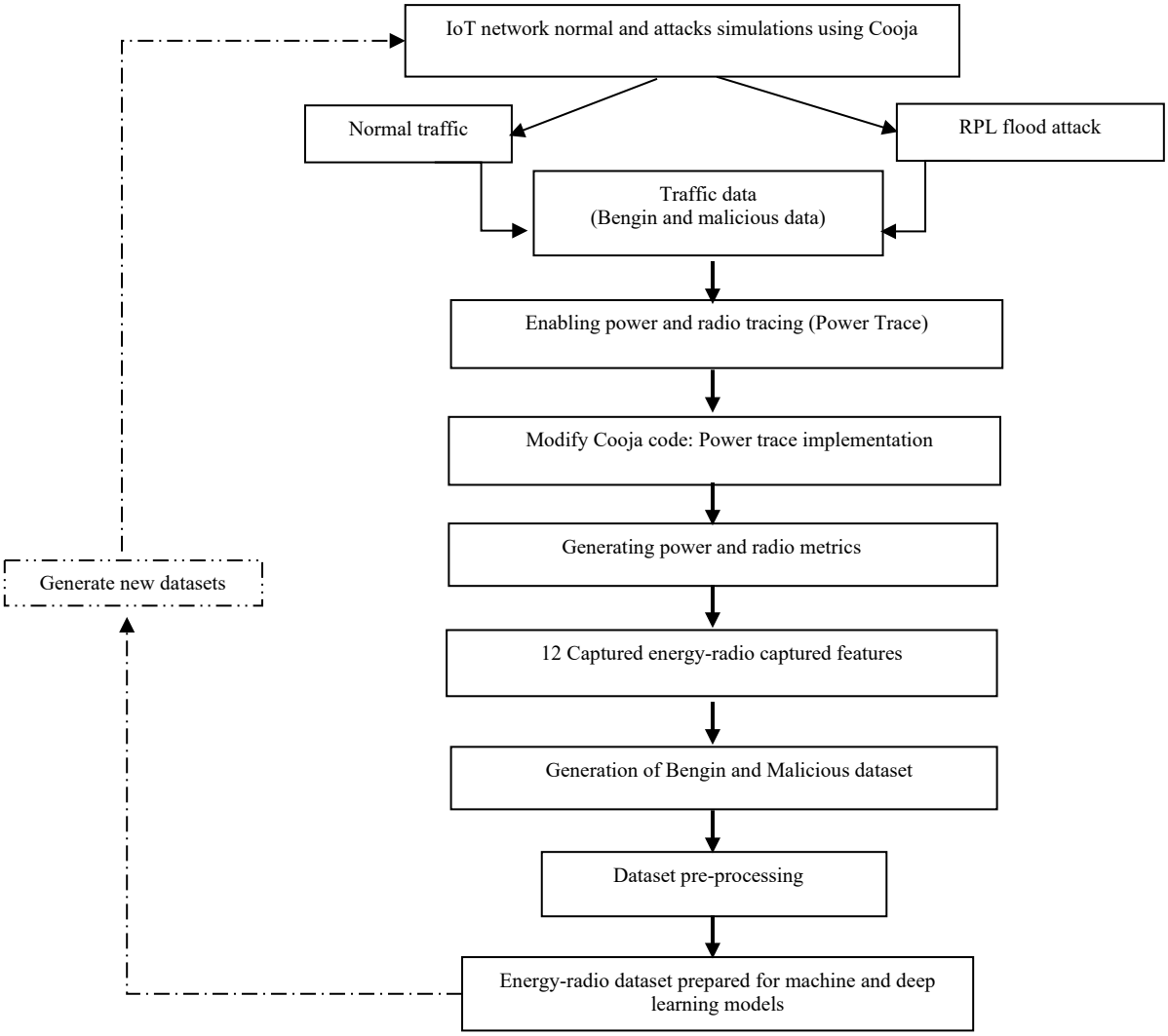

Figure 1. Proposed approach

4. SIMULATIONS PHASE

4.1. Simulations Phase

To accurately evaluate the effects of the DIS Flood attack on an IoT network, two separate scenarios as shown in Figures 2 and 3 were created and tested, a normal functioning scenario and an attack scenario. The purpose of these scenarios was to measure the fluctuations in energy usage and radio activity metrics across various network situations.

Standard Scenario, Under typical circumstances, the IoT network functions without any malicious behavior. The network topology has numerous nodes, with each node being depicted as a purple circle, and a root node represented by a green circle (Node 1). Nodes communicate via established RPL routes, which are shown by blue arrows representing the flow of data between nodes [12, 13]. Every node carries out basic operations such as transmitting and receiving data packets at regular intervals. The red circles surrounding the nodes depict the communication range of each individual node. In this scenario, power and radio measurements are gathered to establish a reference point for energy usage and network activity in a typical, undisturbed condition [14, 15]. The acquired data encompasses the duration of CPU activity, low power mode (LPM) duration, transmission duration, and listening duration, offering a full perspective on the network's typical operational state.

In the attack scenario, a malicious node (Node 22) is introduced to simulate a flood attack known as DIS (DODAG Information Solicitation) Flood. The attacker node, depicted as a yellow circle, persistently transmits an excessive number of DIS messages to its adjacent nodes (Nodes 15, 16, 18, 19, 20, and 21) [16], as seen by the blue arrows. These messages inundate the network with control traffic, leading to the impacted nodes expending resources on processing superfluous control packets and regularly updating their routing tables.

The attack results in substantial disturbances in the network's functioning, resulting in elevated energy consumption and intensified radioactivity in the nodes located near the attacker. This scenario demonstrates the effects of the DIS Flood attack on the stability of the network, the efficiency of energy usage, and the reliability of communication. The gathered data offers valuable understanding of the unusual patterns that arise during the attack, assisting in the formulation of efficient detection and mitigation techniques.

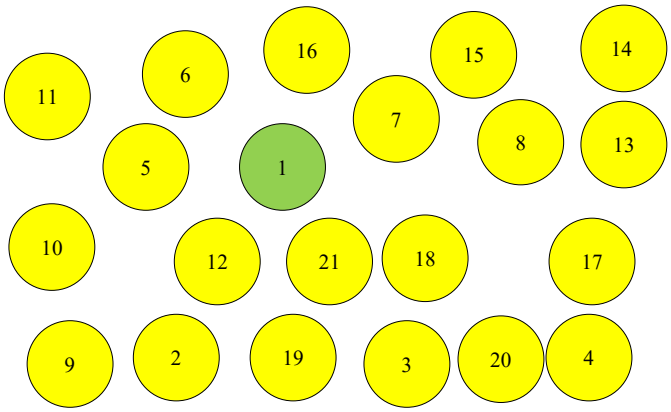

Figure 2. Normal simulation map

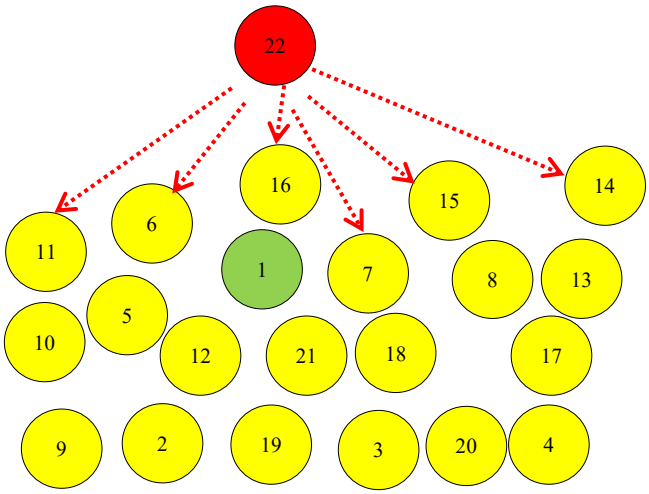

Figure 3. Flooding attack simulation map

5. RESULTS AND ANALYSIS

5.1. CPU Evolution

The graphs displayed in the following, that is, Image 4 and Image 5, show the utilization of the CPU at a particular time during normal and attacker instigated conditions, respectively. As an axis, the Y-axis represents the tick of the CPU utilization and, as the X-axis it is plotted for time in seconds. For this case study in the normal behavior, that is, for Figure 4, the CPU load also increases in phase with time i.e. we see a consistent increase for all nodes involved in the network. The X-axis region is 0 to 1800 seconds when the Y-axis direction is almost 450000 ticks. The CPU utilization increases in rate as the time progresses at a steady rate, signifies an operation with no any packet drops and no delays for this timeline.

It illustrates normal operation of a network in which the CPU does not reach its maximum utilization owing to the fact that all applications share the CPU load fairly. In Figure 5 that represents the attack scenario the trend deviates significantly beyond the normal trend. The scenario also implies very unexpected behavior in the attack since the time ranges from 0 to 1800 seconds and the vertical line goes up to 856000 ticks which shows remarkable increase in CPU due to the attack.

During attack the values of average CPU usage increases faster due to more compute power demanded by the DIS flood attack. This is an attack that overloads the network with cycles of continuous DIS messages and according to the result some nodes end up having way too much subletting than usual. Nonuniform distribution of consumption of CPU in the background of normal scenario is observed to be different in the attack condition. This happens because of maximum employment of resources that leads to great increase in CPU usage and has a direct effect on overall network performance, specifically its power tariffs and scheduling. Processing power is also required very much, and these circumstances will cause huge impact of the DIS flood attack on the network.

The evaluation of normal and attack situations reveals the negative outcomes of DIS flood attacks on Internet-of-Things (IoT) networks. In normal conditions the network functions well with CPU consumption stopping at about 450,000 ticks at the end of the simulation. In turn, during the attack, the higher level of the CPU consumption is around 856,000 ticks, which further highlights the resources and the energy consumption of the network under the attack.

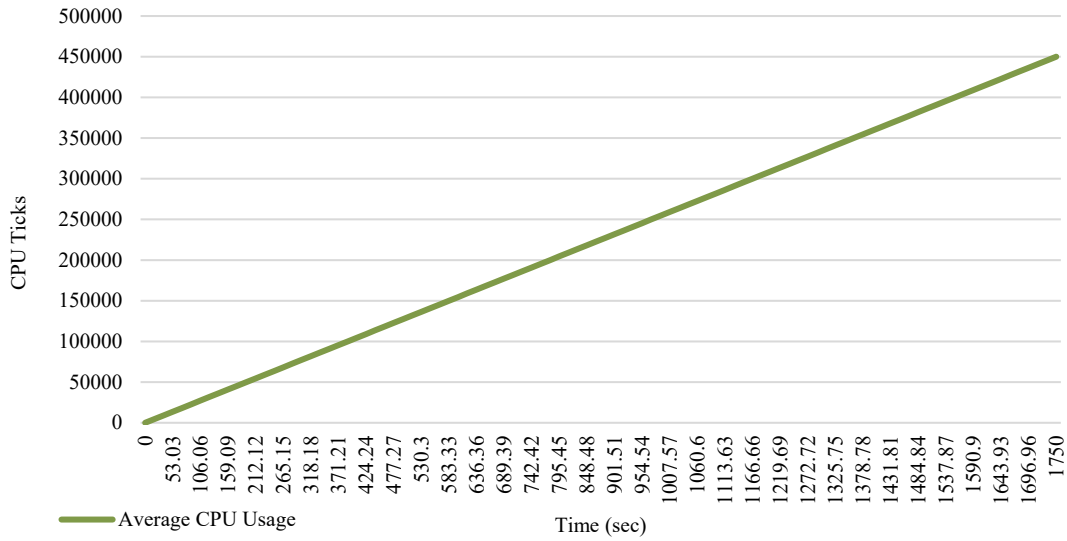

Figure 4. Average CPU over time during normal simulation

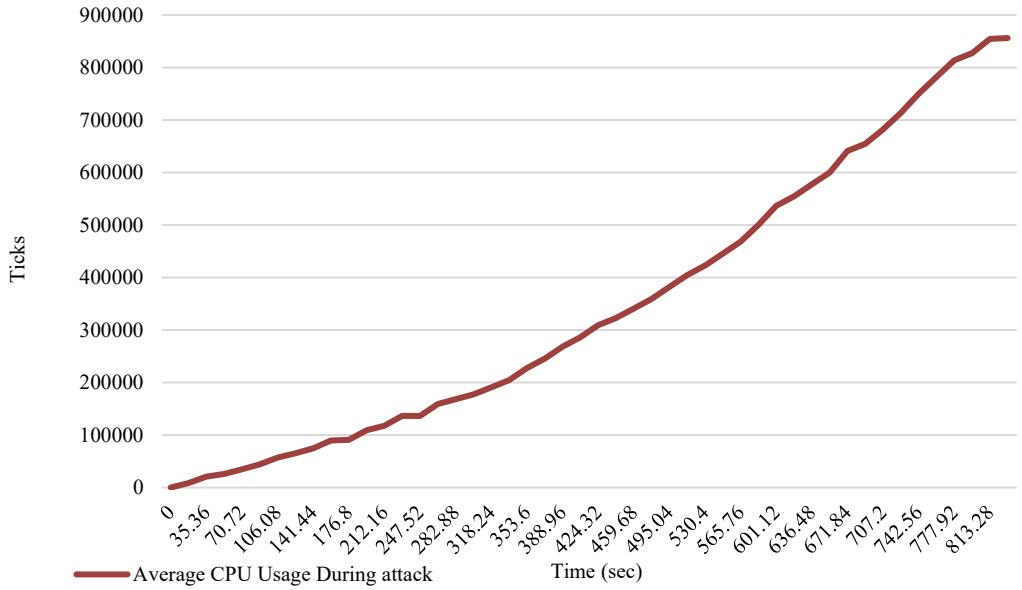

Figure 5. Average CPU over time during attack simulation

5.2. LPM Evolution

Figures 6 and 7 represent the average LPM utilization across time under normal and attack conditions. LPM Utilization in this case, on both Figures 6 and 7 means how much time in clock cycles a device in the network spent or went about in the low power modes. It's a critical parameter for energy efficiency as it tracks the time during which a certain node is in the low power states and there is no communication activity [17, 18]. The X-axis represents the time covered in the specified span seconds.

During the normal simulation however i.e. as shown in Figure 6, the average LPM usage experiences an upward trend with time, peaks at slightly under 69,000 ticks before coming to a halt as the simulation period ends. That enables us to start with the reaction to the network by the able-bodied units, and reference to the gradual rise on the graph particularly in the range of the first 250 seconds it will be followed by stabilization of LPM usage. The increase in LPM usage however shows nodes use low-power mode often when there is no communication going on active range, a measure for energy saving [19]. The controlled LPM usage across the network is an indication that the use of the network is evenly distributed and there is no overload or strange activities.

On the other hand, the DoS scenario in Figure 7 was characterized by very low average LPM usage, with the maximum values being about 35,000 ticks. By contrast, the drop is more pronounced during the latter half of the simulation conveying the heavy damages caused by the attack. While the attack in itself does not drain the network, it is discovered that the active prevention of the intended frame increases traffic, making nodes respond more frequently to the heightened traffic thereby decreasing LPM usage. This behavior has a profound impact on energy conservation, leading to higher net energy outlay.

The comparison of Figures 6 and 7 points out the increasing amount of energy that the attack wastes in the operation of the network. Where the normal scenario makes better efficiency when it comes to energy saving, the attack alternative makes the utilization of LPM variable explaining the higher energy consumption due to the network. This analysis strengthens the evaluation of the importance of appropriate defense systems which are essential in reducing these attacks energy costs which affect the performance of the network.

5.3. Transmit Evolution

Figures 8 and 9 illustrate the average Transmit (TX) time across all normal and attack scenarios. The Y-axis of these graphs corresponds to TX time in ticks, where ticks refer to the number of clock cycles taken by a node to send data [20]. This value is indicative of the activity and congestion of the network as well as the data management capacity of the nodes in the network. The x axis indicates time represented in seconds of the simulation.

During the normal simulation (Figure 8), there is a gradual rise in the TX time for all the nodes and after the 1800 seconds simulation it reaches a little less than 320000 ticks. Such steady growth means that the nodes are transmitting data outwards evenly to all directions without much congestion or abnormality. The slight variations in the TX time cause the behavior in the network to be made up of nodes being in some usually congested mode with respect to data transmission, where the nodes are performing simple tasks of suppressing and forwarding data and sending control messages from time to time. Wrong science fiction movies spoil the whole implausibility quite well, however, the consistency of the TX time across nodes in normal conditions indicates that the network is functioning optimally without any congestion.

However, in an attack scenario (Figure 9), TX time goes to another level, with the nodes bearing the brunt of the DIS Flood attack displaying the most dramatic increase. The Y-Axis is now up to 700,000 ticks, much larger than 320,000 ticks in the case without an attack.

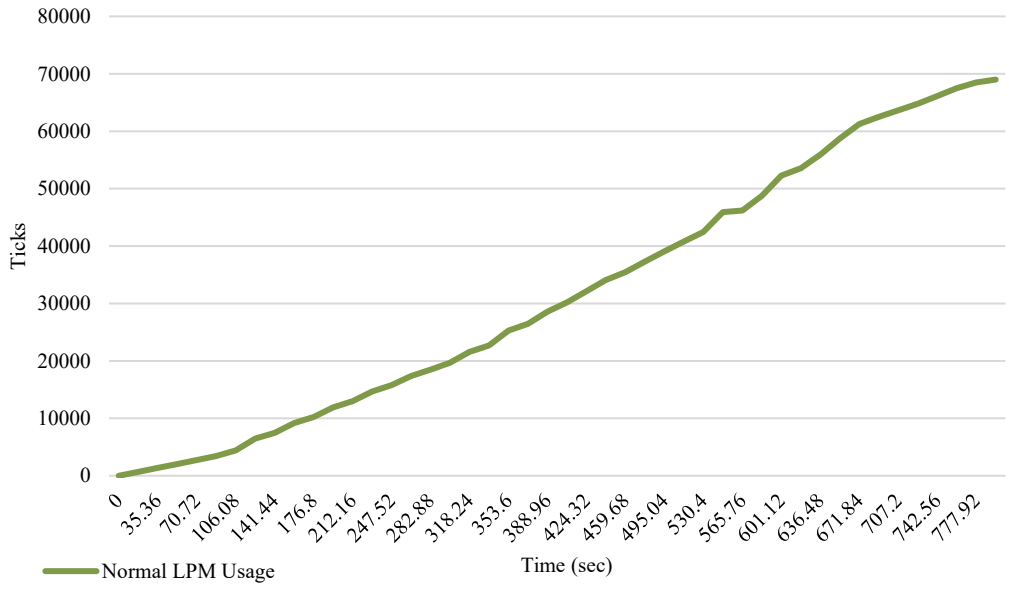

Figure 6. Average LPM over time during normal simulation

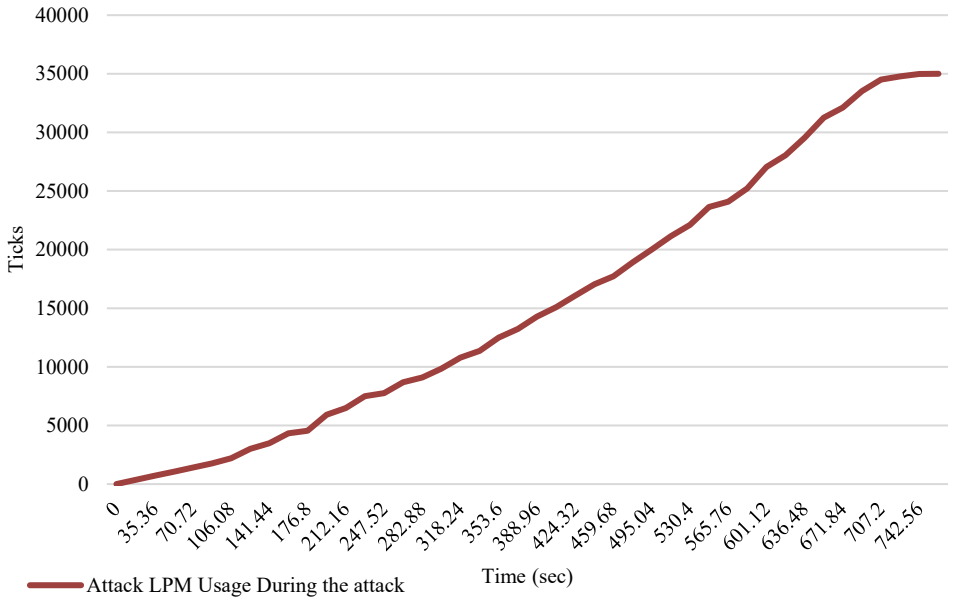

Figure 7. Average LPM over time during attack simulation

Such steep growth means that there is an escalation in transmitting volume considering the nodes that are being inhibited are the very ones being bombarded with DIS speeches. Correspondingly, these particular nodes endure longer TX times, with some reaching performing semblance of up to 700,000 ticks. Such an impact is predictable as the network has been attacked by high volumes of control messages, making some of the nodes transmit data for a longer period than normal.

The situation of the target scenario moreover showcases a traffic distribution distortion, meaning that some parts of the network get saturated while the others remain virtually calm. Such results show that there was a high increase in TX time experienced by the affected nodes while the unaffected nodes kept their TX time quite steady and low which suggest that the attack tends to put most of the network traffic to some specific nodes. This results in high congestion and more transmission delays for the nodes under attack and conversely for other nodes the situation remains normal.

The difference between 'normal' and 'attack based' scenarios is very significant and straightforward with respect to the usage of the network in the case of DIS Flood attack. The network is operationally functional in the normal situation and the nodes are able to adhere to designated times for the relay of the packets. But in the attack situation the system gets choked up and some of the nodes are made to bear an unreasonable amount of load in terms of transmissions resulting to increased power usage and processing latencies.

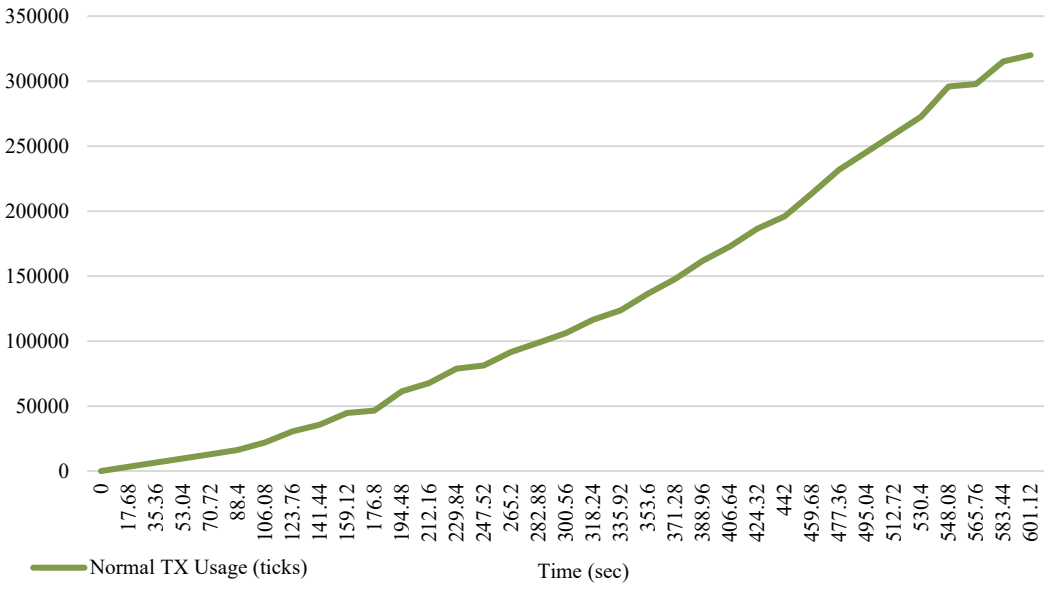

Figure 8. Average transmit (TX) over time during normal simulation

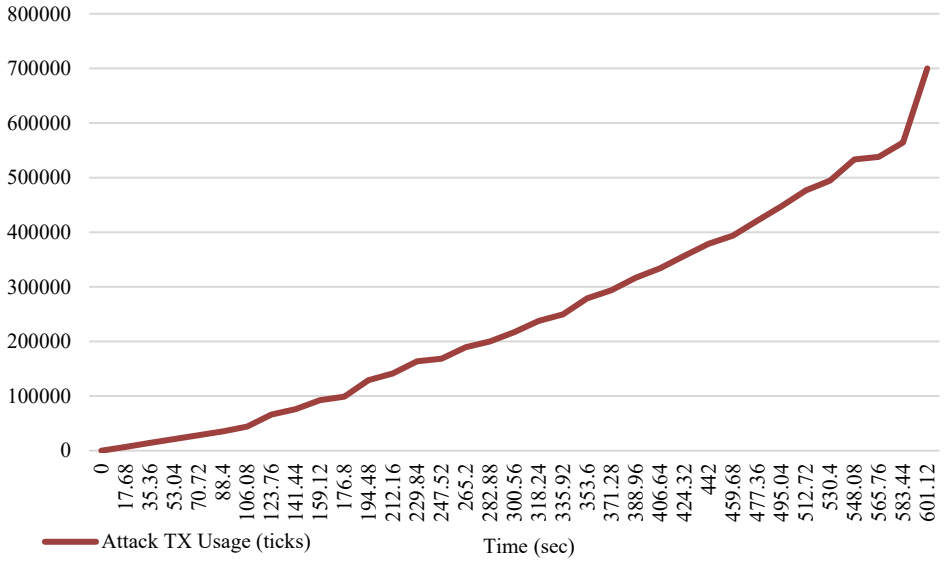

Figure 9. Average (TX) over time during attack simulation

5.5. Radio Activity Evolution

Figures 10 and 11 depict the mean representation of the radio activity utilization of nodes over a certain period during both attack and normal states. Both graphs have Y-axis as the percentage of radio activity signifying the period spent by a node's radio 'on', as either 'transmit' or 'received' over the overall duration of the simulation with the X-axis being time in seconds of the simulation [21]. In normal conditions simulation (refer to Figure 10), the average radio activity is observed to be on the following low values, between 0% and going up to approximately 7% towards the end of the 1800 seconds duration simulation. Such a low radio activity means that the nodes perform quite well in terms of communication by spending most of the time, not engaged in any communication activity, but rather in idle state or even in a low power mode [22]. The slight changes in the levels of the radio energy are typical, as in a normal network, some nodes will be energized to send/receive data while most of the time, they will be off with no energy wastage. In general, the network is active and communicates very well without excessive use of radio for all nodes.

On the other hand, the attack scenario (Figure 11) reveals high levels of radio activity with a specific focus on the nodes affected by the DIS Flood attack. The Y-axis rises as far as 86.7%, which is extremely higher than the statistics in the normal case study. This increase shows that the affected nodes in question have their radios on either receiving or sending information and even active communication allows for up to 86.7 % of the members active at a given moment. The nodes are attacked, and so instead of a dialogue there is a barrage of DIS messages that these nodes have to process resulting in increased radio activity with respect to time and energy costs.

This difference in the normal and attack scenarios illustrates the element of communication disruption with regards to the DIS Flood attack. Normal scenario indicated that radio activity would be low signifying low energy communication. In the attack scenario on the other hand, radio activity increased significantly for the nodes under attack causing higher energy costs and extra explanation costs. Nodes that were not affected, on the other hand, had a fairly low and stable level of radio activity which demonstrates the effect of the attack on the distribution of network traffic. This part shows the severe effects of recent DIS Flood attacks on overall network performance with emphasis on efficiency of communication and energy consumption. Attacks cause those nodes to radiate more understanding that they are trying to perform additional communication which throws everything out of balance.

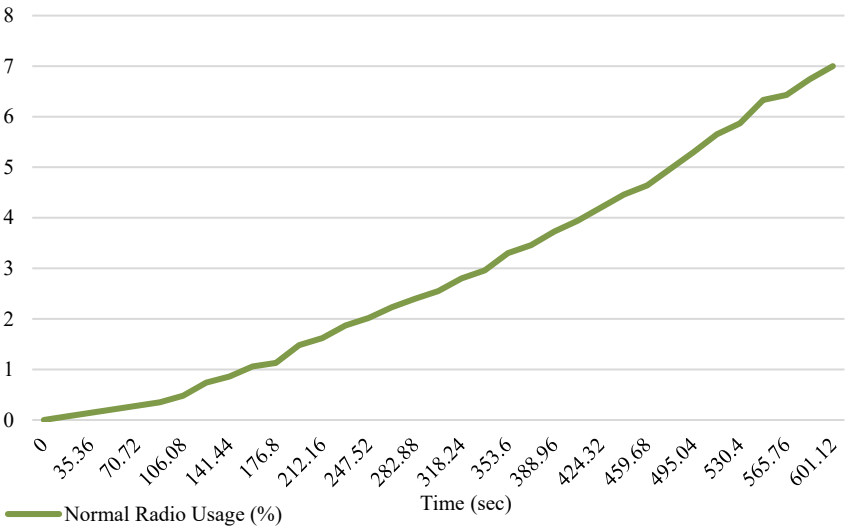

Figure 10. Average radio activity over time during normal simulation

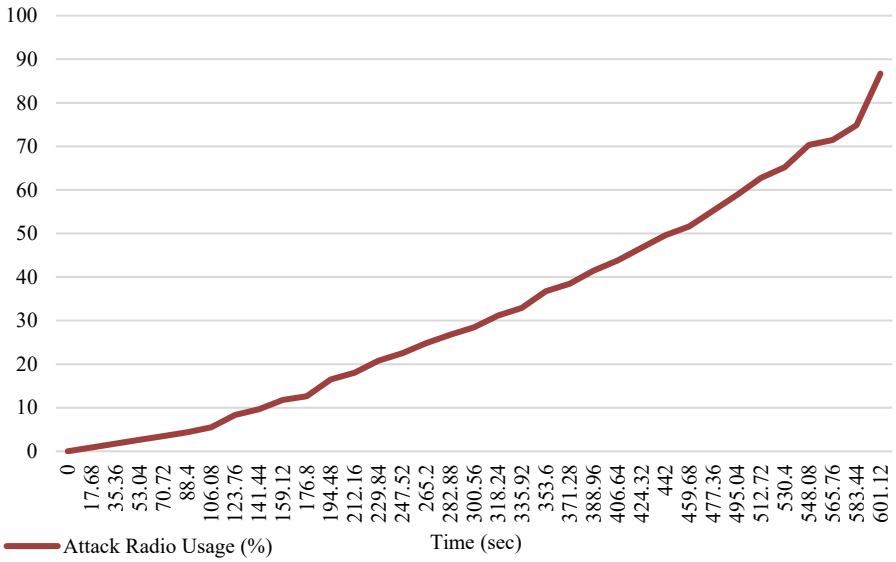

Figure 11. Average radio activity over time during attack simulation

6. ENERGY-RADIO DATASETS GENERATION

6.1. Mote Output

The Table 2 below showcases a sample of the "Mote output" window from the Contiki Cooja simulator. This window offers comprehensive real-time logs of different parameters and metrics for each node (mote) in the simulated IoT network [23]. The output is crucial for monitoring and analyzing the behavior of each mote during the simulation, especially in scenarios that involve network attacks.

Every row in the output corresponds to a particular moment in the simulation, indicated by:

- The Time column (for example, "00:51.306" represents 51 seconds and 306 milliseconds).
- The Mote column specifies the particular node, such as "ID:12" for the node with ID 12.
- The Message column records different metrics related to that node at the specified time.

The recorded metrics in the Message column encompass:

• P (label): Represents a distinct identification or label linked to the message.
• The numbers "All CPU," "All LPM," "All Transmit," and "All Listen" represent the aggregate energy consumption metrics for CPU, Low Power Mode (LPM), transmission, and listening activities up to the current point in the simulation, measured in ticks.

The Figures "1225722", "26393", "4054", and "0" correspond to the cumulative energy consumption of CPU, LPM, transmit, and listen, respectively.

• The values CPU, LPM, Transmit, and Listen represent the energy usage for the current cycle for CPU, Low Power Mode (LPM), transmission, and listening operations, respectively. The cycle-specific measurements offer detailed information on the immediate energy use at every time interval.

• Rime Address (e.g., 6405): Represents the distinct identifier of the mote inside the network, enabling the recognition of communication patterns and data transmission between nodes.

The extensive logging allows for a thorough examination of the network's energy usage and operating effectiveness. Researchers can use it to precisely identify the specific instances when nodes depart from their usual behavior, particularly when they are under attack. The detailed data collected in the "Mote output" is essential for verifying the simulation findings, creating precise energy consumption models, and improving the detection skills of machine learning algorithms for IoT network security.

Through the analysis of the results, researchers can gain a deeper understanding of how network attacks Impact the energy usage of particular nodes and the overall performance of the network. This knowledge is crucial for the development of stronger and more resilient security solutions for the IoT.

Table 2. Sample of Data collection using power trace

Time	Mote	P	All-CPU	All-LPM	All-Transmit	All-Listen	CPU	LPM	Transmit energy	Listen energy
00:41.306	ID:12	0.18	85369	1225722	26393	40514	28456	29452	22935	5511
00:50.353	ID:19	0.18	124722	1513925	50848	31403	22028	31051	32155	4661
00:50.355	ID:12	0.18	120545	1518137	29570	37702	17436	32528	21392	5786
00:50.469	ID:12	0.18	118816	1518471	46253	48750	30857	30257	46253	7764
00:50.470	ID:12	0.18	126032	1465419	60194	46603	23901	27684	25282	4122
00:50.544	ID:12	0.18	196959	1453970	91063	91063	46361	46061	46061	3763
00:50.684	ID:12	0.18	197500	1440154	98090	80920	12578	26825	18732	5229
00:50.717	ID:19	0.18	223507	1407747	107380	77392	23890	28516	29305	5421
00:50.717	ID:12	0.18	94964	1496464	40224	33335	19498	20144	20914	5297
00:50.791	ID:5	0.18	66221	1463712	21116	22935	14537	31178	13178	2901
00:50.795	ID:9	0.18	82900	1493834	44220	24177	22597	37380	15377	3903
00:51.014	ID:5	0.18	85316	1557974	26163	31980	13724	30034	31980	3249
00:51.273	ID:4	0.18	125844	1512737	50546	40662	30836	28879	21881	4397
00:51.306	ID:12	0.18	114783	1523860	50657	48765	33270	29411	32981	6874

6.2. Captured Features

In order to properly observe and analyze the energy usage trends of IoT nodes in our simulations, we employed the "power trace" plugin in the Contiki operating system. Table 3 presents an exhaustive list of the different characteristics recorded by the "power trace" plugin.

This plugin is essential to measuring the performance and energy efficiency of each node, whether it is operating normally or under attack. This analysis offers a comprehensive understanding of how power is used by each node in various operational modes [24, 25].

Table 3. Energy and radio captured features

Index	Feature	Description
1	Simulation Time	Total duration of the simulation.
2	Clock Time	Measured in ticks per second (default is 128 ticks/second).
3	Mote ID	Unique identifier for each mote in the network.
4	Label	Assigned label for the mote.
5	Rime Address	Network address of the mote in the Rime protocol.
6	Sequence Number	Sequence number associated with data packets.
7	Total CPU Energy	Cumulative CPU energy consumption.
8	Total LPM Energy	Cumulative energy consumption in Low Power Mode (LPM).
9	Total Transmit Energy	Cumulative energy used for data transmission.
10	Total Listen Energy	Cumulative energy consumed while listening for data.
11	Total Idle Transmit Energy	Energy consumption during idle transmission states.
12	Total Idle Listen Energy	Energy consumption during idle listening states.
13	CPU Energy (Cycle)	CPU energy consumption for the current cycle.
14	LPM Energy (Cycle)	LPM energy consumption for the current cycle.
15	Transmit Energy (Cycle)	Energy used for data transmission in the current cycle.
16	Listen Energy (Cycle)	Energy consumed while listening in the current cycle.
17	Idle Transmit Energy (Cycle)	Idle transmission energy for the current cycle.
18	Idle Listen Energy (Cycle)	Idle listening energy for the current cycle.

Through the analysis of these characteristics, we can evaluate the effects of various attack scenarios on the energy consumption and operational efficiency of IoT nodes. Usage metrics such as all-CPU, all-lpm, all-transmit, and all-listen provide data on the overall energy use for the whole simulation duration. On the other hand, cycle-specific metrics like CPU, lpm, transmit, and listen help us identify changes in energy consumption at smaller time intervals.

6.3. Sample of the Prepared Dataset

The Table 4 below provided displays a sample of the Energy-Radio dataset that has been selectively compiled to record the fundamental energy usage and radio activity measurements of IoT nodes during regular operation.

This dataset is an essential element of our research, specifically created to establish a thorough foundation for comprehending the fundamental characteristics of IoT devices in relation to energy efficiency and communication patterns, Through the systematic recording of metrics like as CPU duty cycle, low power mode utilization, transmission and reception counts, and associated energy expenditures, this dataset enables a comprehensive examination of how each node manages processing tasks and conserves energy. Radio activity percentages provide a measure of the communication overhead encountered by the network, indicating the level of participation of each node in transmitting and receiving data.

Table 4. Sample of the prepared dataset (DIS and Hello Flooding attacks)

Time	ID	Seqno	CPU Duty Cycle	Low Power Mode	TX Count	RX Count	TX Bytes	RX Bytes	CPU Energy	Low Power Energy	Low Power Energy	Radio
00:10.4	8	1285	0.18	0	3866	324631	0	3337	20541	3113	3113	1.01%
00:10.5	11	1285	0.18	0	14151	314323	3955	4174	20563	2393	2393	2.47%
00:10.6	2	1285	0.18	0	14811	313658	5602	3497	45210	2661	2661	2.77%
00:10.6	6	1285	0.18	0	21502	307040	7207	4979	52100	2681	2681	3.70%
00:10.7	18	1285	0.18	0	9044	319429	3041	3982	56234	2465	2465	2.13%
00:10.7	4	1285	0.18	0	9353	319147	3040	4339	52398	2404	2404	2.24%
00:10.7	7	1285	0.18	0	12505	315972	3152	4629	25874	2984	2984	2.36%
00:10.8	14	1285	0.18	0	12964	315518	3229	4145	96523	2568	2568	2.24%
00:10.8	15	1285	0.18	0	14350	314126	5367	5573	52411	2736	2736	3.33%
00:10.8	20	1285	0.18	0	7982	320516	1921	2949	36592	2866	2866	1.48%

Table 5. Testing the methodology on other routing attacks

Attack Type	Description	Impact on IoT Network	Affected Metrics	Potential Detection with Proposed Framework	Number of Dataset Rows Generated
DIS Flood Attack	Malicious nodes flood the network with DODAG Information Solicitation messages, causing resource exhaustion.	Increased CPU utilization, reduced Low Power Mode (LPM), and heightened radio activity near attacker nodes.	CPU energy, LPM energy, transmit and listen times, radio activity.	High detection accuracy due to noticeable deviations in energy and radio metrics.	103,478 rows
Sinkhole Attack	An attacker node falsely advertises itself as having the best route, attracting and dropping packets.	High radio activity due to incorrect routing, increased energy consumption in affected nodes.	Radio activity, transmit time, increased energy consumption at affected nodes.	Detectable through abnormal radio and energy metrics as affected nodes transmit excessively.	94,621 rows
Wormhole Attack	Two malicious nodes create a tunnel to relay packets, bypassing legitimate routing paths.	Increased transmission delays and uneven energy distribution across network nodes.	Transmission delays, uneven CPU and energy consumption across nodes, abnormal transmit and listen times.	Can detect increased transmission and listening times, especially in nodes near the wormhole tunnel.	98,905 rows
Version Number Attack	An attacker increments the RPL version number, forcing nodes to rejoin the network unnecessarily.	Increased control traffic, heightened energy usage, and reduced network stability.	Increased transmit and listen times, CPU energy spikes due to unnecessary network reconvergence.	Detectable through spikes in energy consumption and control traffic patterns.	87,254 rows
Selective Forwarding Attack	Malicious nodes selectively drop packets, disrupting network communication.	Reduced packet delivery rates, leading to retransmissions and higher energy usage in surrounding nodes.	Radio activity, increased retransmission attempts, energy consumption in transmitting nodes.	Detectable through radio activity and retransmission anomalies.	82,789 rows

7. GENERALIZATION OF THE FRAMEWORK TO MULTIPLE IOT ATTACKS

Having considered the configuration of the proposed framework with various IoT breach scenarios, Table 5 represents a detailed paradigm of conditions related to the suitableness of the proposed framework for given IoT attack scenarios. For each attack type, the table identifies the most salient features, the impact on the IoT network, the energy as well as radio parameters, and the how well again considering in this side the framework can be applied with respect to detection of attacks. Furthermore, data relating to the number of rows in the dataset produced as a result of each attack within the experiments, stressing the expanse and grasp of the research data.

The scope of these attack scenarios encompasses the generic and frequent RPL based IoT attacks where they include the DIS Flood, Sinkhole, Wormhole, Version Number and Selective Forwarding predominant in the

discrete event robustness attacks. Such attacks relate to energy consumed by nodes in the network, network topology, usage of resources and more importantly, the extent of communication. It is evident from the table that the DIS Flood detection frame, which was designed for that specific attack, explains why it is able to detect other attacks as it is based on the efficiencies of energy and radio metrics. Further study was proposed to increase the number of attack scenarios and developed larger datasets for better training and testing of the model.

8. THE USAGE OF DATASETS FOR MACHINE LEARNING MODELS

The scheme is represented in the Figure 12 below, showing the overall procedure of utilizing the energy and radio data prepared for training and testing machine learning models against the Internet of Things (IoT) attacks. Explanation of items on each particular stage of the process is given below. First, the preprocessing is accomplished by fairly balancing the dataset according to the normal and attack instances. Afterward, the data is transformed which results in consistent feature values through multiple scales. Features of interest are selected that will undergo Principal Components Analysis (PCA) for even more fine-grained selection and ensured reduction of the model training phase to the significant features only.

Here, the models are classified and trained using adjustable back-propagation rules with Adam, an optimizer, such that the model can learn from both good and malicious cases. In addition, the steps comprise setting the model to have the right number of hidden layers with non-linearity to be able to capture the more complicated behaviors of the attacks. Testing the trained model for generalization using unseen samples is performed and others aids the way the model was built, models its performance by performing K-Fold cross validation on many sub-blocks of the dataset.

Finally, these models are used to detect attacks. For this purpose, it assigns the end devices in the IoT network as either normal or attacker. When a deviation in energy and radio metrics is observed, abnormal or rogue nodes are recognized. A structured approach, starting from the dataset consolidation till the very end of the model validation, effectively detects IoT security issues.

9. CONCLUSION

This work introduces an innovative approach to creation of a thorough energy-radio dataset specifically designed for the investigation of IoT network security. The DIS Flood attack is used as a case study for this purpose. Utilizing power trace metrics, the proposed system captures comprehensive energy consumption and radio activity patterns across all nodes. This framework establishes a strong basis for the development of machine learning and deep learning models that target the detection and mitigation of different IoT network attacks.

Our study reveals statistically significant differences in energy usage and radio activity, especially for nodes located near the attacker, when comparing normal and attack circumstances. The mentioned variations emphasize the decisive influence of DIS Flood attacks on the performance and energy efficiency of networks, therefore emphasizing the necessity for efficient methods of detection and response. The dataset produced not only enables the detection of anomalous activities linked to security risks but also assists in the development of energy-efficient IoT networks by uncovering possibilities for enhancing power efficient utilization.

The pressing nature of this research is motivated by the escalating use of IoT devices and the rising complexity of network assaults that exploit their weaknesses. This study makes a significant contribution to the area by addressing the difficult characteristics of energy and radio metrics in IoT security. It enables the development of more effective and efficient security solutions. Subsequent research will broaden this approach to encompass other categories of attacks, therefore augmenting the dataset's comprehensiveness and its efficacy in training more sophisticated models.

Furthermore, it will be crucial to include actual IoT deployment data in order to verify the suggested models and guarantee their suitability in various and ever-changing settings. In result, this study establishes the foundation for developing IoT networks that are more robust, energy-efficient, and secure, capable of enduring ever-changing cyber risks.

ACKNOWLEDGEMENTS

Firstly, the authors extend their profound appreciation to God, for providing me with the fortitude and resilience to overcome all challenges encountered during this research. Secondly, the authors extend their sincere appreciation to the members of the Laboratory of Research Watch for Emerging Technologies (VETE), Faculty of Sciences and Technology, Hassan I University, Settat, Morocco whose contributions, both direct and indirect, have been indispensable to completion of this manuscript.

REFERENCES

[1] H. Allioui, Y. Mourdi, "Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey", Sensors, Vol. 23, No. 19, p. 8015, 2023.

[2] L. Xing, "Reliability in Internet of Things: Current Status and Future Perspectives", IEEE Internet of Things Journal, Vol. 7, No. 8, pp. 6704-6721, August 2020.

[3] S. Bagchi, T.F. Abdel Zaher, R. Govindan, P. Shenoy, A. Atrey, P. Ghosh, R. Xu, "New Frontiers in IoT: Networking, Systems, Reliability, and Security Challenges", IEEE Internet of Things Journal, Vol. 7, No. 12, pp. 11330-11346, December 2020.

[4] A. Krari, A. Hajami, E. Jarmouni, K. Errakha, "Neural Network-Based Detection Mechanism Against RPL DIS Flooding Attacks in IoT Networks", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 59, Vol. 16, No. 2, pp. 175-184, June 2024.

[5] J. Tournier, F. Lesueur, F. Le Mouel, L. Guyon, H. Ben Hassine, "A Survey of IoT Protocols and Their Security Issues Through the Lens of a Generic IoT Stack", Internet of Things, Vol. 2020, pp. 100-264, 2020.

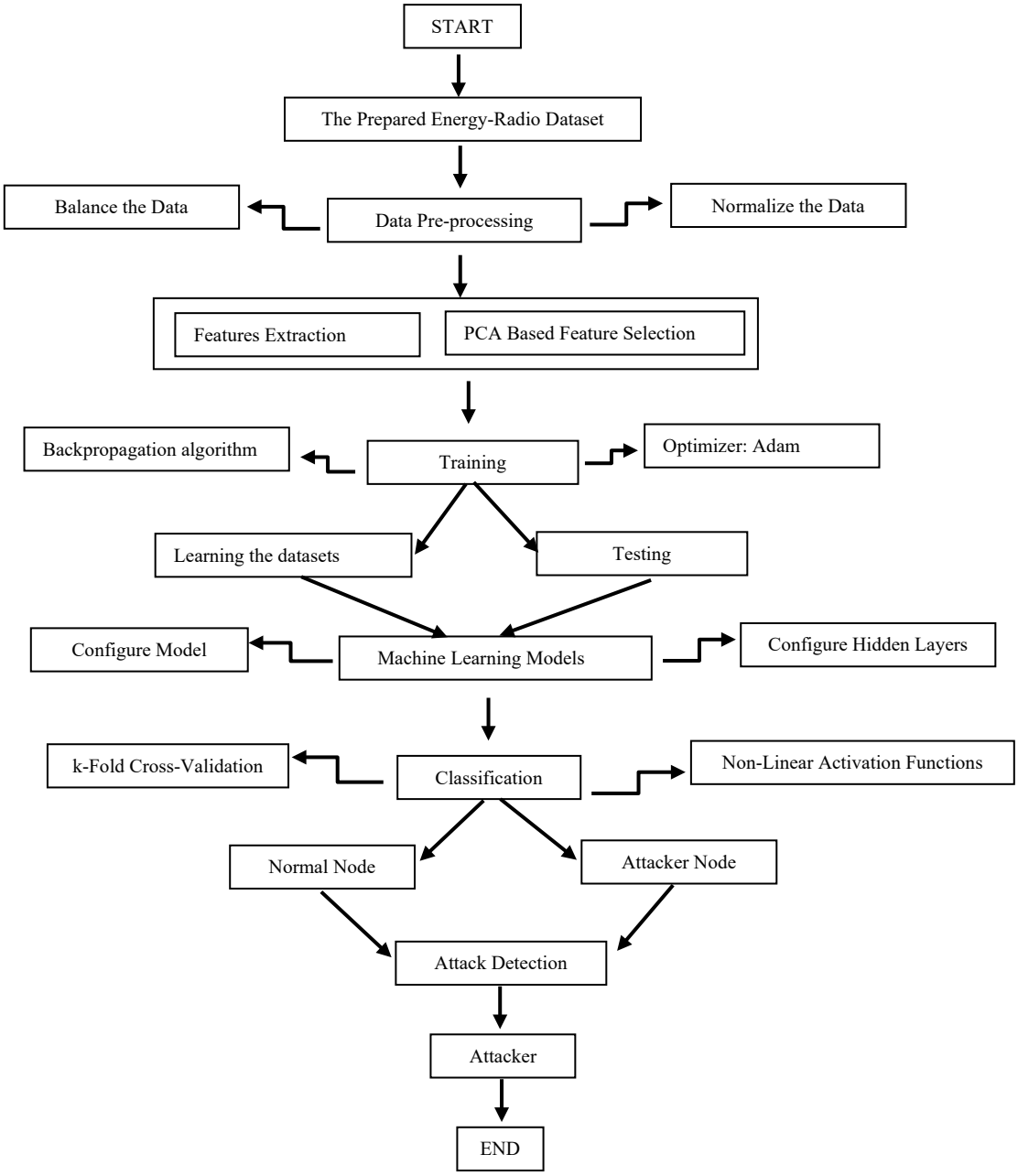

Figure 12. Usage of datasets for machine learning models

[6] S. Sharma, V. Kumar, K. Dutta, "Multi-Objective Optimization Algorithms for Intrusion Detection in IoT Networks: A Systematic Review", Internet of Things and Cyber-Physical Systems, Issue 1, Vol. 4, pp. 258-267, 2024.

[7] W.A.H.M. Ghanem, S.A.A. Ghaleb, A. Jantan, et al., "Cyber Intrusion Detection System Based on a Multi-Objective Binary Bat Algorithm for Feature Selection and Enhanced Bat Algorithm for Parameter Optimization in Neural Networks", Sensors, Issue 9, Vol. 22, pp. 3400-3420, 2022.

[8] D. Sutanto, M.A. Andryani, M. Hilman, et al., "Enhanced Dataset for IoT Device Identification Using Low-level Network Traffic Data", Data in Brief, Issue 1, Vol. 54, pp. 10617-10625, 2024.

[9] A. Roy, S. Sharma, S. Kumar, "Artificial Neural Network Model for Decreased Rank Attack Detection in RPL Based on IoT Networks", Vol. 1, Issue 1, pp. 1-15, 2021.

[10] R. Zietlow, A. Chanda, A. Jhumka, "Blockchain-Based Trust Establishment for IoT Edge Devices Using Decentralized Trust", Journal of Cybersecurity and Privacy, Vol. 12, No. 2, pp. 1-16, 2023.

[11] A. Krari, A. Hajami, E. Jarmouni, "Study and Analysis of RPL Performance Routing Protocol Under Various Attacks", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 49, Vol. 13, No. 4, pp. 152-161, Set tat, Morocco, December 2021.

[12] A. Hasan, M.A. Khan, B. Shabir, A. Munir, A.W. Malik, Z. Anwar, J. Ahmad, "Forensic Analysis of

Blackhole Attack in Wireless Sensor Networks/Internet of Things", Applied Sciences, Issue 22, Vol. 12, pp. 1-20, Switzerland, November 2022.
[13] M. Islam, Z. Kwak, S. Kim, "Analysis of Black Hole Attacks in RPL-Based Low-Power and Lossy Networks", Sensors, Issue 2, Vol. 21, pp. 1-20, Switzerland, January 2021.
[14] E. Rastogi, M.K. Maheshwari, A. Roy, N. Saxena, D.R. Shin, "Energy Efficiency Analysis of Narrowband Internet of Things with Auxiliary Active Cycles for Small Data Transmission", Transactions on Emerging Telecommunications Technologies, Issue 4376, Vol. 33, pp. 1-12, London, UK, October 2021.
[15] T. Kamal, E. Helmy, S. Fahmy, M.H. Abd El Azeem, "Detecting and Preventing for Performance Assessment of IoT Devices Under Dodge Information Solicitation (DIS) Attacks", 2023 40th National Radio Science Conference (NRSC), Cairo, Egypt, May 2023.
[16] F. Siddiqui, J. Beley, S. Zeadally, G. Braught, "Secure and Lightweight Communication in Heterogeneous IoT Environments", Internet of Things, Issue 6, Vol. 14, p. 100093, September 2019.
[17] A. Haj Hassan, Y. Imine, A. Gallais, B. Quoitin, "Consensus-Based Mutual Authentication Scheme for Industrial IoT", Ad Hoc Networks, Issue C, Vol. 145, pp. 103-162, June 2023.
[18] Y. Yilmaz, B. Halak, "TIGHTEN: A Two-Flight Mutual Authentication Protocol for Energy-Constrained Devices", Authentication of Embedded Devices, Technologies, Protocols and Emerging Applications, pp. 89-112, Springer, January 2021.
[19] A.K. Jaiswal, "DoS Attack Network Traffic Monitoring in Software Defined Networking Using Mininet and RYU Controller", Preprint, November 2022.
[20] A. Hkiri, M. Karmani, O. Ben Bahri, A.M. Murayr, F. H. Alasmari, M. Machhout, "RPL-Based IoT Networks Under Decreased Rank Attack: Performance Analysis in Static and Mobile Environments", Computers, Materials and Continua, Vol. 78, No. 1, pp. 227-247, January 2024.
[21] A. Seyfollahi, A. Ghaffari, "A Review of Intrusion Detection Systems in RPL Routing Protocol Based on Machine Learning for Internet of Things Applications", Wireless Communications and Mobile Computing, August 2021.
[22] A. Asaduzzaman, "CoAP Message Delivery Scheme Using MQTT in Wireless Sensor Network for IoT", Diva, 2023.
[23] U. Kulau, S. Muller, S. Schildt, F. Busching, L. Wolf, "Investigation and Mitigation of the Energy Efficiency Impact of Node Resets in RPL", Ad Hoc Networks, Vol. 114, p. 102417, April 2021.
[24] G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J.C. Ribeiro, J. Rodriguez, "An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks", Electronics, Vol. 10, No. 21, p. 2562, October 2021.

BIOGRAPHIES

Name: **Ayoub**
Surname: **Krari**
Birthday: 10.08.1996
Birthplace: Settat, Morocco
Bachelor: Network and Technologies of Telecommunications, Department of Mathematics and Computer Science, Faculty of Science and Technology, Hassan I University, Settat, Morocco, 2017
Master: Telecommunications System and Network Engineering, University of Sultan Moulay Slimane, Beni Mellal, Morocco, Since 2019
Doctorate: Student, Internet of Things Routing Security, VETE Laboratory, Faculty of Science and Technologies, Hassan I University, Settat, Morocco, Since 2019
The Last Scientific Position: Systems and Security Engineer, Ministry of National Education, Morocco, Since 2020
Research Interests: Internet of Things, Security, AI
Scientific Publications: 9 Papers

Name: **Abdelmajid**
Surname: **Hajami**
Birthday: 26.04.1975
Birthplace: Errachidia, Morocco
Bachelor: Informatics, Mathematic and Informatics Department, Faculty of Sciences and Technology, Hassan I University, Settat, Morocco, 2004
Master: Networks, Telecommunications and Multimedia, Department of Networks and Telecoms, National Higher School of Computer Science and Systems Analysis, Mohamed V University, Rabat, Morocco, 2006
Doctorate: Networks, Telecommunications and Multimedia, Department of Networks and Telecoms, National Higher School of Computer Science and Systems Analysis, Mohamed V University, Rabat, Morocco, 2011
The Last Scientific Position: Prof., Department of Applied Physics, Faculty of Sciences and Technology, Hassan I University, Settat, Morocco, Since 2011
Research Interests: Security, Networks, Bio-Informatics
Scientific Publications: 65 Papers, 2 Books, 2 Projects, 3 Theses

Name: **Ayoub**
Surname: **Toubi**
Birthday: 19.05.1994
Birthplace: Rabat, Morocco Technology Settat, Morocco, 2015
Master: Information Systems Security, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, 2018
Doctorate: Student, Routing Protocols for Multimedia in IOT, LAVETE Laboratory, Faculty of Science and Technology, Hassan I University, Settat, Morocco, Since 2021
Research Interests: WSN Routing Protocol, Cyber Security, and Smart Sensor Memory Issues
Scientific Publications: 5 Papers, 1 Poster

Name: **Marouane**
Surname: **Ait Said**
Birthday: 27.06.1993
Birthplace: Agadir, Morocco
Bachelor: Telecommunication Networks and Technologies, Faculty of Science and Technology, Ibn Zohr University, Agadir, Morocco, 2014
Master: Software Engineering, Computer Science, National School of Applied Sciences, Tetouan, Morocco, 2016
Doctorate: Telecommunications, Department of Mathematics and Computer Science, Faculty of Science and Technology, Hassan I University, Settat, Morocco, Since 2019
Research Interests: Payment Systems, Fraud Detection, Security
Scientific Publications: 2 Papers