Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 1, February 2024, pp. 179-189

DOI: https://doi.org/10.52436/1.jutif.2024.5.1.1567
p-ISSN: 2723-3863
e-ISSN: 2723-3871

STATE OF THE ART ANALYSIS ON BATTERY-RELATED THREATS AND DEFENSES OF IOT DEVICES USING KITCHENHAM

Azka Ghafara Putra Agung[1], Aditya Pradana[*2], Rahmat Budiarto[3]

[1,2]Computer Science Dept., Mathematics and Science Faculty, Universitas Padjadjaran, Indonesia, Indonesia
[3]Computer Science Dept., College of Computing and Information, Al-Baha University, Saudi Arabia
Email: [1]azka20002@mail.unpad.ac.id, [2]aditya.pradana@unpad.ac.id, [3]rahmat@bu.edu.sa

(Article received: December 5, 2023; Revision: January 11, 2024; published: February 13, 2024)

Abstract

The Internet of Things (IoT) keeps growing in size every year, but its growth also companied with threats to its security. This paper centers on the research article that focuses on various attacks on IoT system and devices through power drain techniques targeting IoT devices. This paper discusses various existing attack models, and security model. The main objective is to reveal the state of the art of the security issues of IoT related to attacks to the devices' power. The literature review is performed by implementing Kitchenham method and utilizing Google Scholar and Science Direct databases. 42 publications between 2010 and 2023, fulfilling the selection criteria are selected and comprehensively reviewed. To counteract power drain-induced Denial of Service (DoS) threats, the paper evaluates existing defense mechanisms specifically tailored to mitigate these attacks. These defenses encompass adaptive power management strategies, hardware-level security enhancements, and network-level security measures. The effectiveness, practicality, and trade-offs of these defense mechanisms are examined. The combination of these papers offers comprehensive insights into battery-related security concerns in the IoT landscape, with sleep deprivation attacks, Denial of Service-induced battery drain, and Vampire attack, highlighting the importance of robust security measures in the IoT ecosystem.

Keywords: *Advanced Vampire Attack, Denial of Service, IoT, Kitchenham, Sleep Deprivation Attack.*

1. INTRODUCTION

The realm of Internet of Things (IoT) is marked by the interconnection of a diverse array of devices, such as motion sensors, baby monitors, cameras, smartwatches, and smartphones, utilizing various communication technologies. According to estimates, the IoT landscape is poised to host over 70 billion devices by 2025, with approximately 70% of these being low-power and cost-effective devices. Low Power Wireless (LPW) technologies are emerging as the communication backbone for these IoT devices, promising to connect billions of devices seamlessly [1]. A substantial portion of these devices predominantly relies on batteries as their power source. Market projections indicate a growth in the IoT battery market, surging from USD 9.2 billion in 2020 to USD 159 billion in 2025 [2]. This burgeoning market underscores the importance of devising efficient and optimized solutions for battery utilization in IoT devices.

IoT devices are susceptible to a range of attacks [3] [4]. These devices typically operate software developed by third parties and are connected to the internet, rendering them vulnerable due to inherent limitations in their design, implementation, and resource constraints, notably their reliance on batteries. One well-known form of attack targeting IoT devices involves sleep deprivation [4] [5]. In such attacks, malicious actors employ various means to induce an undesirable spike in battery consumption, preventing the device from entering sleep mode, consequently compromising energy conservation and reducing the device's operational lifespan.

The gravity of sleep deprivation attacks escalates when directed at sensitive devices, such as wearable personal fitness trackers (utilized for personal telemetry) and implantable medical devices (IMDs), as they continuously monitor vital signs, with failures potentially resulting in significant physical harm to users. While defensive strategies against sleep deprivation attacks exist, tailored to these sensitive devices, some necessitate battery replenishment [6], which may not be feasible in all battery-constrained systems. Other techniques rely on external software or hardware to bolster defense mechanisms [7] [8], and some propose detection models rooted in network analysis or network architecture [9] [10]. Furthermore, there have been proposals for Intrusion Detection Systems (IDS) specifically oriented towards identifying battery exhaustion attacks [11] [12], but they fall short in addressing low-powered devices used in IoT settings or providing precise estimations of power consumption.

Fobe et al. [13] introduce a novel technique, grounded in their own attack and security models, designed to manage sleep mode and battery

utilization, effectively mitigating sleep deprivation attacks. This technique ensures an uninterrupted sleep mode, impervious to radio communication or programmable sensor/device interference, while continuously monitoring real-time energy consumption from the battery. Data consumption is meticulously recorded in a moving average array that calculates the average power consumption. Should power consumption surpass a predefined threshold, the device promptly enters sleep mode for the necessary duration to rectify its energy consumption. Notably, unlike related approaches [7] [8] [9] [10] [11] [12], this proposed technique operates directly on low-power sensors, eliminating the reliance on external agents and network architecture to safeguard sensor battery longevity against sleep deprivation attacks.

According to Ioulianou et al. [14], many attacks on IoT devices that have been launched recently exploit the properties of RPL and typically include DoS [15] [16] and routing attacks [17] [18]. Detection of and effective defense against such attacks is currently an open research problem [19], [20]. They examine ContikiOS's RPL implementation, specifically ContikiRPL [21]. Our primary focus centers on two prevalent types of Denial-of-Service attacks, namely "Hello" flooding [16] and version number modification [22] [23]. These attacks have the capability to deplete the batteries of Internet of Things (IoT) devices. To simulate these attacks, Solapure et al. [24] utilized the Cooja simulator, a tool designed for emulating ContikiOS behavior. The study illustrates how these attacks can impact the energy consumption of IoT devices, potentially rendering some devices unreachable. Following the presentation of the simulation findings, the authors delve into potential strategies for defense and detection. Specifically, the authors introduce a modular Intrusion Detection System (IDS) comprising a series of distributed detection modules, complemented by a central detection module within a border router.

Pu et al. [25] explain due to the RPL lacks security mechanisms for internal attacks [26], Low-Power and Lossy Networks (LLNs) are especially susceptible to a specific DoS attack, which is referred to as the advanced vampire attack (AVA). In contrast to the traditional vampire attack [27], where an adversary merely amplifies the overall network energy consumption, the advanced vampire attack has the capability to not only disrupt immediate service availability but also permanently disable the entire network. This attack not only results in the loss of data packets but also depletes the limited battery energy of nodes. To answer this problem, the authors introduce a novel countermeasure based on the Theil index to detect and mitigate advanced vampire attacks in RPL [28]. Vampire attack is a specific DoS attack, which not only can cause data packet losses, but also drain nodes' limited battery energy. Advanced vampire attacks involve manipulating data packets with fictitious destinations to trick intermediate nodes into dropping tampered packets and responding with error messages. The core concept of the proposed countermeasure involves analyzing the distribution of destination MAC addresses in received data packets using Theil index theory. When an advanced vampire attack is detected, the countermeasure initiates the mitigation procedure to promptly neutralize the threat. The authors employ a customized discrete event-driven simulation framework utilizing OMNeT++ [29] to assess the countermeasure's performance in terms of detection rate and cumulative energy consumption. The authors also reevaluate existing method, a route examination-based mechanism [26] adapting it for the simulation framework for comparative analysis.

IoT network consists of devices that have limited resources. One of them is limitation in battery capacity. Therefore, this battery is very crucial against attacks. Thus, this paper is important for researchers in creating appropriate solutions. The objective of this paper is to to reveal the state of the art of the security issues of IoT related to attacks to the devices' power. The main contributions of this paper are comprehensive insights into battery-related security concerns in the IoT landscape, with sleep deprivation attacks, Denial of Service-induced battery drain, and Vampire attack, highlighting the importance of robust security measures in the IoT ecosystem.

2. METHODOLOGY AND DATASET

This paper uses Kitchenham method for the comprehensive literature review. The flowchart of research process is shown in Figure 1 [30]. The process consists of three phases. The first phase is the Planning the review that involves identifying the objective for a review, specifying the research question(s), and developing a review protocol. The objective of this research is to investigate the state of the art of analysis on battery-related threats and defenses of IoT devices. To select the appropriate literatures, some key questions are required to help refine the criteria and discover new possibilities that have not been investigated before. These questions are related to battery threats and defenses of IoT devices, such as:

Q1–What are the research goals for the battery threats and defenses of IoT devices?

Q2–What techniques are used in defensing the IoT devices from battery-related threats?

Q3–What factors and information are important for developing detection system for IoT devices?

Then, protocols involved in IoT networks are identified.

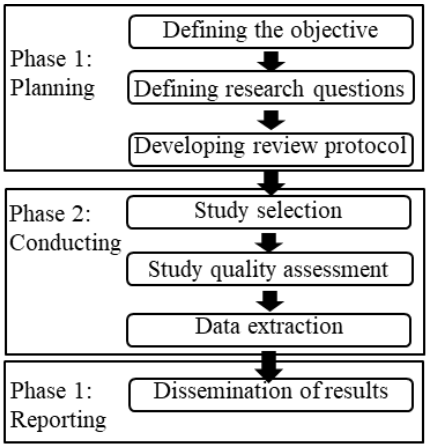

Figure 1.Steps in Kitchenham [30]

The second step is the Conducting the review that involves searching and selecting the relevant literature sources, extracting and synthesizing the data from the studies, and assessing the quality and relevance of the studies. The literatures are selected from Science Direct and Google Scholar databases, published between 2010 and 2023 Table 1 shows the selection criteria, and extracted literatures. Finally, 42 papers are selected manually.

The third step is Reporting the review, which involves presenting and analyzing the results, answering the research question(s), discussing the implications and limitations, and providing a summary and recommendations. The third step's results are presented in Section 3 and Section 4.

Table 1. Selection criteria and extracted literatures

Criteria	Key search	Google Scholar	Science Direct	Total
A	IoT network AND ("IDS" OR "IPS")	215,000	4,868	219,868
B	("DoS" OR "SDA" OR " AVA)	317,300	7,842	325,142
C	("RPL" or "6LoWPAN")	9,900	1,875	11,775
D	A and B	198	78	276
E	D and E	140	47	187

3. ATTACK MODELS

This section summarizes the attack model proposed by each reviewed paper.

3.1. Sleep Deprivation Attack (SDA)

Fobe et al. [13] presented several attack models that will be used to test the proposed method. The following are the attack model given in the paper:

A. The Diamond Sleep Deprivation Attack

Sleep deprivation attack model using the Diamond technique, consist of four primary elements: Adversary, Capability, Infrastructure, and Victim. These elements interact in the following way: the Adversary utilizes Infrastructure to build Capability, the Capability exploits the Victim, and the Infrastructure links to the Victim. In this model, the emphasis lies on the motivation that drives the attack, rather than the specific actions taken.

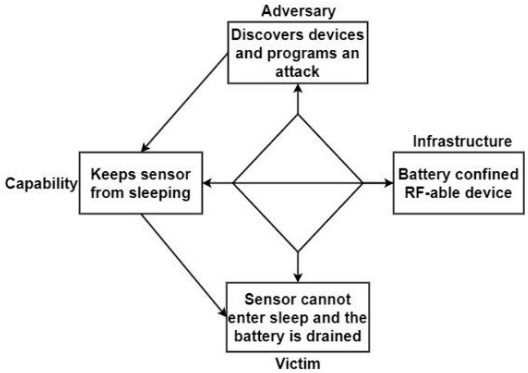

Figure 2. Illustration of the diamond sleep deprivation attack model [13].

The diamond diagram in Figure 2 illustrates the fundamental aspects of a sleep deprivation attack. The Attack Path suggests that the motivation might lead to other stages in a multi-stage attack, with the current focus on a vulnerable infrastructure as the motivation. Each component has a designated role as follows.

1. Adversary: Orchestrates attacks by using compromised components of a larger system, such as sensors or wearables, to amplify harm or gain control over the Victim. These attacks may not have immediate effects and can unfold over weeks or months.
2. Capability: Sleep deprivation attacks usually occur in close proximity to the target sensors, employing specialized radio messages to prevent them from entering sleep. This attack unfolds gradually over an extended duration.
3. Infrastructure: RF-able devices and their associated networks are crucial for the attack. The Adversary may employ basic network knowledge to manipulate messages and sustain the attack.
4. Victim: Depending on the context, the Victim can be an individual, organization, or service controlling devices like IMDs and Wearables. The targets encompass the company overseeing Infrastructure and the user population.

The model indicates that the attack path can transition from the Victim's sensor to other targets, often involving IoT system infrastructure. Notably, executing such an attack may require only a battery-constrained RF-able sensor.

B. The Kill Chain Sleep Deprivation Attack

The Kill Chain technique outlines a sequence of seven steps that attackers follow to accomplish their goals. These steps include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives. Unlike the Diamond Model, which examines

motives, the Kill Chain focuses on the actual actions taken during an attack. This approach is valuable for disrupting attacks because interrupting any of these steps can thwart the attacker's objectives.

Each step within the Kill Chain, in the context of a sleep deprivation attack, can be described as follows:

1. Reconnaissance: The attacker gathers information about the sensor-owning company, sensor locations, accessibility, and the routines of maintenance teams. For wearable or IMD sensors, the attacker also obtains information about the individual carrying the sensor.
2. Weaponization: The attacker programs devices to emit specialized radio signals continuously, preventing the sensor from entering sleep mode. These devices should outlast their target if battery-constrained.
3. Delivery: The attacker strategically places devices near their targets, requiring no interaction from the victim to initiate the attack. Initially, the victim may not detect the attack.
4. Exploitation: The devices begin to prevent the sensors from entering sleep mode, causing rapid battery depletion. Personnel monitoring the sensor may notice the accelerated battery drain.
5. Installation: The sensor's battery is significantly depleted. The victim's response would typically involve replacing the sensor battery or adapting the system to function without it.
6. Command and Control: In this type of attack, the attacker may not directly control any resources but could disrupt the system integrated with the sensor to trigger an automatic response.
7. Action on Objectives: The victim is compelled to take an action that benefits the attacker, inadvertently creating new attack vectors.

The victim cannot directly observe the attacker's actions during the attack, but analyzing the Kill Chain can help recognize it. Reversing through the chain reveals that the attacker invested time in researching the devices before launching the attack. Identifying the attack allows for understanding the steps and patterns, aiding in detection and prevention.

The Kill Chain provides insight into an attacker's actions, and disrupting any of these steps can prevent a successful attack outcome. Preventing the rapid battery depletion can render the attack ineffective.

C. The Sleep Deprivation Attack Graph

This technique offers an overview of an attack by illustrating the pathways leading to its success. Similar to the Kill Chain, it outlines the necessary steps for executing an attack while providing insights into the relationships among the elements involved. Figure 3 visually represents the attack graph model for the Sleep Deprivation attack, where ovals symbolize targets and arrows depict connections between actors and components represented by rectangles. The attacker's goal is to either harm or exploit the target company's infrastructure or devices. This is achieved by conducting research on the infrastructure related to sensors. The attack on these sensors disrupts their batteries and affects the IoT system. Consequently, this results in damage to the company's infrastructure and triggers a response from the maintenance team, which the attacker may exploit to launch additional attacks, such as intercepting the team's credentials.

In essence, the attack graph illustrates that preventing the rapid battery drain will protect the company's infrastructure and devices from harm or exploitation.

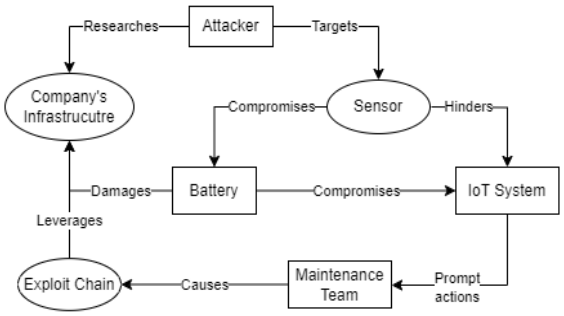

Figure 3. Illustration of the Sleep Deprivation Attack Graph [13].

3.2. DOS Battery Drain Attack Model

Ioulianou et al. [14] present one simple situation, using malicious node as an attack model. The malicious node is attacking the system by flooding the network with DIS control messages and modifying version number every second to keep the neighboring node from power preserving state and draining their power.

To test the attack, the authors perform two separate scenarios. In the first scenario, there are no nodes that have been compromised. Each node is set up to send messages to the server at predefined intervals. These messages include diverse information about the sending node, such as its battery status and temperature.

In the second scenario, one of the nodes has been tampered with and is acting maliciously. It conducts DoS attacks by sending a large volume of DIS messages to neighboring nodes. Furthermore, it alters the DODAG version number, triggering global repair processes.

The server (Sky 1) functions as the recipient for all network messages, and therefore, it remains operational continuously. The benign nodes transmit data to the server and are set to send a DIS message every 60 seconds until they successfully join the network. On the other hand, the malicious node conducts a "Hello" flooding attack by broadcasting 80 DIS messages every second.

Table 2. First Scenario Power Consumption [14]

Node	Radio ON	Radio TX	Radio RX
Sky 1	99.82%	0.11%	0.18%
Sky 2	1.93%	0.87%	0.05%

Sky 3	1.94%	0.87%	0.06%
Sky 4	1.16%	0.24%	0.06%
Sky 5	1.25%	0.35%	0.07%
Sky 6	1.20%	0.30%	0.04%
Sky 7	1.29%	0.39%	0.06%
Average	15.34%	0.45%	0.07%

In the first scenario, everything operates as intended, with nodes joining the network one by one, and the server occasionally sending repair signals to adjust the topology as new nodes join. The power consumption for the first scenario is presented in Table 2. Using the same node configurations, the second scenario involving a malicious node was replicated. In this case, the power consumption of the nodes is impacted by the presence of the malicious node, as depicted in Table 3. Although the nodes are supposed to be in sleep mode most of the time, they are active for 50% of the time, which also applies to the server. The disparity compared to the normal scenario is approximately 35%, which is a substantial difference. The reason for this behavior is caused by the fact that the malicious node broadcasts DIS messages requiring a DIO reply from its neighbors, and because the malicious node keeps changing the DODAG version number therefore the node never appeared in the network and no information is sent to the server.

Table 3. Second Scenario Power Consumption [14].

Node	Radio on	Radio TX	Radio RX
Sky 1	100.00%	0.07%	0.24%
Sky 2	3.78%	2.08%	0.19%
Sky 3	59.37%	2.20%	35.70%
Sky 4	4.28%	2.60%	0.03%
Sky 5	59.60%	1.99%	36.06%
Sky 6	60.17%	2.42%	36.08%
Sky 7	63.98%	47.33%	0.94%
Average	50.17%	0.45%	15.61%

3.3. Advanced Vampire Attack Model

Pu et al.[25] propose one attack model in their paper, which attack the Routing Protocol on IPv6 that uses Lossy Network that widely known as RPL. RPL possess distinct characteristics like limited memory, computing resources, low data rates, and unreliable wireless connections.

RPL lacks security features, making it vulnerable to advanced vampire attacks. These attacks aim to make legitimate intermediate nodes drop data packets and respond with error messages to the LLN Border Router (LBR). This disruption has two significant consequences: it hampers service availability by causing many dropped data packets, and it can permanently disable the network by draining nodes' battery energy as each intermediate node forwards numerous error messages to the LBR.

In the normal scenario, energy consumption increases gradually and linearly as simulation time passes, due to intermediate nodes along the forwarding path regularly handle a small amount of data packets, leading to a steady energy increase. However, in the advanced vampire attack scenario, energy usage spikes. The attack begins at around 450 seconds, and from that point on, the cumulative energy consumption significantly rises with time. When the simulation concludes, the attack scenario's total energy consumption is approximately three times that of the normal scenario, due to a large number of tampered data packets with fictitious destination MAC addresses, causing intermediate nodes to generate and forward numerous error messages, resulting in a substantial energy drain.

4. SECURITY MODELS

In this section we summarize the security model proposed by each reviewed paper.

4.1. Sleep Deprivation Security Model

Following the understanding of the attack model, the next step involves crafting a security model. This security model is designed to enforce a policy that governs the usage of battery resources. The policy sets a specific power consumption threshold that the device must not exceed. Should consumption surpass this threshold, the device recalculates and enters a sleep period to conserve power.

The model strikes a balance between availability, power consumption, and sleep. The device is required to remain available for communication during defined intervals, although it won't be continuously available due to sleep cycles. The device communicates these availability periods to the larger system it belongs to. Additionally, there's a policy-mandated limit on the amount of energy the device can consume within a specified timeframe. If consumption exceeds this limit, the device activates the sleep mode to reduce consumption. Before entering sleep mode, the device communicates the duration of its sleep cycle to allow the larger system to manage its temporary unavailability.

The security model devised to counter sleep deprivation attacks can be translated into an algorithm that the device executes to control its sleep cycles based on energy consumption. This algorithm manages the sleep cycle to ensure that power consumption remains below the threshold defined in the security policy. Several variables, predetermined by the policy and device specifications, play roles in policy management. These variables include MAS (moving average size), SAMPLING PERIOD (measurement collection interval), POLICY PERIOD (duration until policy check), POLICY POWER (consumption threshold), and SLEEP POWER (power usage in sleep mode). The algorithm works by collecting power measurements, updating average power values, and comparing them to POLICY POWER. When the average power exceeds this threshold, the device adjusts its sleep time to reduce consumption and then enters sleep mode. This

algorithm ensures that the device conserves battery life as dictated by the policy.

4.2. DOS Battery Drain Intrusion Detection System

1. Architecture and Components

The proposed architecture for IoT network security comprises traditional sensor nodes along with two new device types: IDS routers and IDS detectors.

- IDS Routers: These routers have a dual role, serving as the network's border router (BR) while hosting both a detection module and a firewall. As the BR, they manage communication between devices within the network and external servers. The detection module utilizes specific algorithms to identify malicious nodes within the network, while the firewall generates and enforces rules to block any malicious traffic attempting to enter the network.
- IDS Detectors: These sensor-like devices, referred to as IDS detectors, are strategically positioned near sensor nodes. They actively monitor network traffic and transmit any suspicious data to the IDS router for further analysis. In the event of internal network disruptions caused by malicious devices, detectors log the packets involved. If a node's behavior aligns with a known attack pattern, relevant information is promptly communicated to the IDS router.

2. Mitigating Attacks

The primary objective of this IDS system is to detect and prevent various types of attacks commonly encountered in IoT networks. This includes safeguarding against DoS attacks that could deplete sensor node batteries. Additionally, the system addresses routing attacks, which often exploit the Routing Protocol for Low-Power and Lossy Networks (RPL), a commonly used routing protocol in IoT sensor networks.

- Detection Metrics: The IDS system employs specific metrics to identify malicious nodes. One such metric is the packet sending rate, as normal smart devices typically do not exchange numerous packets. Abnormal behavior, such as sending an excessive number of packets, may indicate a malicious node. Another metric considers packet intervals, as each device communicates at specific time intervals. Malicious nodes may exploit this by sending requests too frequently. By comparing a node's behavior to established thresholds, the IDS can identify and flag malicious activity.
- Scalability: The IDS is designed to be efficient in large-scale networks. It only forwards suspicious traffic from detectors to the router, minimizing unnecessary communication overhead. The router gains a holistic view of the network and can take action against suspicious nodes effectively.

3. Detection Module and Firewall

The detection module within the router plays a crucial role in identifying potential threats within the network. It makes decisions based on collected data for each individual device. For instance, devices that excessively send packets at a high rate or exhibit an abnormal Received Signal Strength (RSS) value may be considered malicious. The detection module can take actions such as removing a malicious device from the network, blacklisting its IP address, generating firewall rules, and notifying network administrators.

- Firewall: The IDS system incorporates a firewall as an additional layer of protection. The firewall blocks the IP addresses of known malicious nodes based on stored firewall rules. If the detection module identifies malicious behavior, it can create a new firewall rule to halt traffic between the malicious node and the internet.
- Placement Strategy: The IDS employs a hybrid approach to IDS module placement, combining network-based and host-based methods. Centralized detection occurs at the router, which analyzes traffic and detects sensor or internet attacks. Decentralized nodes, the IDS detectors, perform lightweight tasks like monitoring and forwarding suspicious packets to the router. This strategic placement ensures efficient detection and mitigation of attacks from various network segments.

This comprehensive approach to IoT network security helps protect against a wide range of potential threats, ensuring the integrity and reliability of IoT sensor networks.

4.3. Advanced Vampire Security Model

The Theil index-based countermeasure presents a comprehensive method for identifying and addressing advanced vampire attacks within networked systems. This security technique relies on nodes within the network recording the destination MAC addresses of received data packets and evaluating the evenness or randomness of their distribution using Theil index theory. The Theil index measures the distribution's evenness, with a higher index indicating a more uniform distribution, while a lower value suggests uneven distribution.

In the context of an advanced vampire attack, adversaries introduce fictitious and unreachable destination MAC addresses, resulting in a significant increase in the evenness or randomness of the distribution of destination MAC addresses in data packets. This abnormal increase in the Theil index value is a key indicator of the presence of such an attack.

To implement this countermeasure, each intermediate node first records destination MAC

addresses within a specific window. Once the window concludes, the node calculates the Theil index value of these addresses based on the data recorded. The entire MAC address space is equally divided into groups, and various parameters, such as the share of destination MAC addresses in each group, are calculated to determine the Theil index values for each group. The node then compares the calculated Theil index value of the current window with the value from the previous window to identify any significant deviations.

When an advanced vampire attack is detected, the countermeasure triggers an attack mitigation procedure at the intermediate node, which is the next hop for the suspected adversary. This procedure reduces the number of accepted data packets from the adversary. To adapt to changing network states and varying attack patterns, an adaptive acceptance rate of data packets is employed. The acceptance rate depends on system parameters and the accumulated detection rate of advanced vampire attacks.

In summary, the Theil index-based countermeasure is a robust and adaptable approach for detecting and mitigating advanced vampire attacks in networked environments. By efficiently assessing the distribution of data and dynamically adjusting the acceptance rate for data packets, it contributes to enhancing network security and protecting against sophisticated attacks.

5. DISCUSSION

The three main papers[13][14][25] that are currently being reviewed offer insightful information on how to handle security issues related to battery or power draining. By presenting unique attack models and security techniques, each papers advances our knowledge of IoT security. In this section we go over the cause of the research each paper and the papers related to their works.

1. Sleep Deprivation Attack

Fobe et al. [13] introduce a light-weight security model that aims to prolong the operational lifespan of IoT devices under sleep deprivation attacks. By emphasizing strategies to keep devices active during attacks, the proposed model exhibits promise in maintaining device functionality without going over power consumption threshold. While there are already some security models that aim to handle this type of attack, model made by the authors aims to improve and fix some issues that present on previous works. The difference compared to previous works are:

- Abdullah et al. [7] proposed a blockchain-based solution to address issues on multiple layer including network layer issues, such as Sybil Attack, Sleep Deprivation, Denial of Service, Malicious Code Injection, and Man-in-the-Middle. While their work shares the concern of sleep deprivation attacks in the network layer, Fobe et al propose a solution that can be run locally instead of running it on blockchain.
- Monnet et al. [10] suggest a clustered WSN (Wireless Sensor Network) with trusted traffic monitoring agents to detect potential attackers, emphasizing a fair election process. But their works did not focus on mitigating the attack and required an external program to help on those detection.
- Hei et al. [8] examine a resource depletion attack on Implantable Medical Devices (IMD) and proposed a machine learning-based solution for detection. Their approach shifts the authentication process to an external device, achieving over 90% detection rate. However, similar to work by Monnet et al., their proposal didn't focus on mitigating the attack and relies on additional device.
- Alampalayam et al. [9] present an adaptive security scheme against denial of service threats in mobile agent systems, providing continuous monitoring and protection. But, their Adaptive Security Model (ASM) only focuses on detection.
- Nash et al. [11] use the relation between energy consumption and system load, while Jacoby and Davis [12] introduce a battery-based intrusion detection system (B-bid). Both approaches, however, are criticized for imprecise estimations and not considering low-powered devices. Fobe et al. [13] work aims to fix that issue by making a program that low-power friendly and having more precise power consumption estimation by using specialized method.

Fobe et al. experimental results show the model was able to detect and carry out its mitigation method. By putting the device to deep sleep, the device can preserve its battery and increase battery life time by 51.2% compared to attacked device without any security model.

2. DoS Battery Drain Attack

Ioulianou et al. [14] focuse on countering battery-draining attacks through a security model centered around intrusion detection systems (IDS). While there is already a few technique on IOT-based IDS already developed, Ioulianou et al. claims that current solution have their own constraint. The authors mentioned Kalis, which necessitates the deployment of detection modules specifically tailored to the attack type, potentially leading to a complex network setup and diminished detection performance. Moreover, Kalis utilizes Wi-Fi for communication, posing a risk of interference between smart sensors and Kalis nodes in close proximity.

Other solution they mention is Svelte, being a host-based IDS, requires modification of the sensor's software, a challenging task for larger networks commonly found in many IoT application domains. Additionally, Svelte is noted for its high false

detection rate, as demonstrated by Matsunaga et al. [31], who proposed a scheme to mitigate this issue. However, Ioulianou et al. notes that further experiments are essential to validate the robustness and scalability of the proposed solution by Matsunaga et al.

3. Advanced Vampire Attack

Pu et al. [25] introduce an security model that identifies and mitigates advanced vampire attacks by limiting the activity of infected nodes. Their model aims to improve on various previously developed models which will be listed below.

- Ghaleb et al. [30] propose countermeasure addresses a Destination Advertisement Object (DAO) insider attack in RPL by associating a counter with each child node in a sub-DODAG. However, its limitation lies in its inefficiency to detect a dynamic DAO insider attacker who manipulates malicious traffic patterns or mimics realistic DAO traffic to evade detection.
- Moving on to Aris et al. [32], the authors delve into RPL version number attacks, offering lightweight mitigation techniques. The first technique targets malicious version number updates from powerful attacking positions, while the second incorporates a trust mechanism. Despite their promise, these techniques may falter in the presence of adversaries executing bad-mouthing attacks in neighboring nodes.
- In the paper by Chang et al.[33], a unique approach of power-positive networking is introduced to counter energy DoS threats. This lightweight strategy leverages wireless charging signals for communication, replenishing energy at the receiving node and thwarting energy DoS attacks.
- Addressing privacy concerns, Nizzi et al. [34] propose an address shuffling algorithm integrated with a keyed-hash message authentication code for IoT devices. This algorithm ensures controlled and collision-free MAC address shuffling, preventing adversaries from inferring network topology or node functionalities.
- For LPWAN IoT networks, Bidgoly and Bidgoly [35] introduce a key synchronizing algorithm involving a random number generator and hashing method. It aims to enhance security through key regeneration. Meanwhile, Murali and Jamalipour [36] model the sybil attacks using an artificial bee colony algorithm and proposes an intrusion detection algorithm. This approach introduces three new variables—nonce ID, control message counter, and timestamps—into the DODAG Information Object (DIO) control message to detect sybil attacks.
- In the context of RPL-based LLNs, Pu et al. [37] put forth a misbehavior-aware detection scheme against energy depletion attacks, offering a tailored defense mechanism. Zeitz et al. [38] introduce micro moving target IPv6 defense as a security mechanism for low-power IoT devices, focusing on IPv6 address rotation for enhanced security.
- Considering energy harvesting networks, Pu et al. [39] investigate stealthy collision attacks, shedding light on potential threats in such environments. A survey by Vasudeva and Sood [40] reviews promising techniques to defend ad hoc networks from sybil attacks. Additionally, Raoof et al. [41] provide an overview of routing attacks and mitigation techniques specific to RPL-based IoT.

Despite the various of countermeasures Pu et al. [39] explore in these studies, as of their latest knowledge, there is an identified gap in comprehensive detection and mitigation strategies specifically designed for the advanced vampire attack.

While each security models have their own way to deal with these power draining threats, there is potential for synergy among these security models. Combining elements of the sleep deprivation model, DoS intrusion detection, and advanced vampire attack may result in a comprehensive security framework. However, it is crucial to acknowledge that the effectiveness of these models was primarily tested on specific systems and need more testing on other system and threats.Table 4 lists some similarities and differences on the security model that has been reviewed.

Table 4. Security Model Characteristics

Attack type	Tested system	Security type	Implementation
Sleep Deprivation [13]	ESP32	Damage control	Additional program on every nodes
DoS Drain[14]	IPv6 Routing Protocol (RPL)	Detection and flagging	Additional program on routers
Advanced Vampire [20]	IPv6 Routing Protocol (RPL)	Detection and counter-measure	Additional program on adversary nodes

The literature analysis result of this paper is compared with other similar literature reviews in [9], [11], and [42] as summarized in Table 5.

Table 5. Comparison with other literature review works

Reference	Method	Thought
[9]	Conventional literature review	The main contributions of this work: 1. A classification of different IoT applications and specific security and privacy issues related to those applications. 2. A detailed explanation of different threat sources in different layers of IoT.

		3. Detailed and realistic recommendations to improve the IoT infrastructure to facilitate secure communications. 4. Review on the proposed countermeasures to the security issues in IoT. 5. An assessment of the open issues, challenges and future research directions for developing secure IoT applications.
[11]	Conventional literature review	A review on Deep Learning (DL) approaches used for IoT anomaly-based attacks detection and their effectiveness in conquering the security challenges in IoT environment. In addition, a comparative study is presented to highlight the performance indicators and architecture of each DL technique. Several DL models are used to detect malicious attacks in different IoT areas. Implementing DL methods with relevant vast datasets can significantly resist different security and privacy concerns.
[42]	Conventional literature review	The main contributions are a new taxonomy of the threats against IoT-based systems, identify what threats can be effectively mitigated by integrating IoT with blockchain technology, the challenges faced by the blockchain-enabled IoT-based systems, and the likely approaches to overcoming these challenges.
This paper	Kitchenham method	The research explored in this paper review has shed light on a critical concern within the realm of Internet of Things (IoT) security, the vulnerability of IoT devices to battery-draining attacks.

6. CONCLUSION AND FUTURE WORKS

The research explored in this paper review has shed light on a critical concern within the realm of Internet of Things (IoT) security, the vulnerability of IoT devices to battery-draining attacks. Three seminal papers, "A New Defensive Technique against Sleep Deprivation Attacks Driven by Battery Usage", "Battery Drain Denial-of-Service Attacks and Defenses in the Internet of Things", and “A Theil Index-Based Countermeasure Against Advanced Vampire Attack in Internet of Things” have independently delved into the challenges posed by attacks focused in battery drainage in the IoT landscape. Each of the reviewed studies have offered innovative solutions and defensive techniques to mitigate the adverse effects of these attacks. Notably, their common focus on addressing battery drain issues presents a unique opportunity for synergistic collaboration.

The convergence of ideas from these papers opens the door to a promising avenue for future research. By combining the insights and techniques presented in all three papers, we have the potential to develop a holistic and robust defense mechanism against battery-draining attacks in IoT environments. This collaborative approach could yield a comprehensive solution that not only prolongs the lifespan of IoT devices but also fortifies the security posture of IoT networks. As the IoT landscape continues to evolve, this synthesis of ideas may pave the way for more resilient and efficient IoT ecosystems, ultimately enhancing the reliability and longevity of IoT devices in an increasingly interconnected world. However, each of the proposed models need further testing on different devices and system before doing more research on combining their functionality.

Future research can also utilize these security techniques to delve deeper into more IoT domains. One of the areas that this research can explore is IoVT (Internet of Vehicle Things) or VANET (Vehicular Ad Hoc Network). With self-driving cars becoming increasingly common as technology evolves, attacks on the nodes of self-driving vehicles, such as navigation, detection, or cameras, can result in catastrophic accidents if proper security countermeasures are not in place.

REFERENCES

[1] Statista, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030," 2022. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Accessed 09/23/2023).

[2] Markets and Markets, "Battery market for IoT by type, rechargeability, end-use application, and geography - Global Forecast to 2025," 2020. https://www.marketsandmarkets.com/Market-Reports/battery-iot-market-153084557.htm (Accessed 09/23/2023).

[3] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The effect of IoT new features on security and privacy: new threats, existing Solutions, and Challenges Yet to Be Solved," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606-1616, April 2019, doi: 10.1109/JIOT.2018.2847733.

[4] L. G. A. Rodriguez and D. M. Batista. “Program-Aware Fuzzing for MQTT Applications,” *in Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis*, pp. 582–586, 2020.

[5] R. Kumar, S. Kumar and P. Arjariya, "A Comprehensive Survey of Security Challenges and Threats in Internet of Things," *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, 2021, pp. 1-5, doi: 10.1109/ISCON52037.2021.9702368..

[6] M.A. Siddiqi, W.A. Serdijn & C. Strydis, "Zero-power defense done right: shielding IMDs from battery-depletion attacks," *J. Sign Process Syst 93*, pp. 421 - 437, 2021. https://doi.org/10.1007/s11265-020-01530-5.

[7] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala and S. Elkhediri, "CyberSecurity: A review of Internet of Things (IoT) security issues, challenges and techniques," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019*, pp. 1-6, doi: 10.1109/CAIS.2019.8769560.

[8] X. Hei, X. Du, J. Wu and F. Hu, "Defending resource depletion attacks on implantable medical devices," *2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL*, USA, 2010, pp. 1-5, doi: 10.1109/GLOCOM.2010.5685228.

[9] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," in *IEEE Access*, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[10] Q. Monnet, Y. Hammal, L. Mokdad and J. Ben-Othman, "Fair election of monitoring nodes in WSNs," *2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, 2015, pp. 1-6, doi: 10.1109/GLOCOM.2015.7417091.

[11] H. Ismaeel and W. Elmedany, "Anomaly-based detection technique using deep learning for Internet of Things: A Survey," *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sakheer, Bahrain, 2022, pp. 278-284, doi: 10.1109/3ICT56508.2022.9990632.

[12] J. Fobe, M. Nogueira, and D. Batista. "A new defensive technique against sleep deprivation attacks driven by battery usage", in *Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, Santa Maria, 2022, pp. 85-96. doi: https://doi.org/10.5753/sbseg.2022.224911.

[13] J. Fobe, M. Nogueira, and D. Batista. "A new defensive technique against sleep deprivation attacks driven by battery usage", in *Proceedings of the 22nd Brazilian Symposium on Information and Computational Systems Security*, Santa Maria, 2022, pp. 85-96, doi: https://doi.org/10.5753/sbseg.2022.224911.

[14] P. P. Ioulianou, V. G. Vassilakis, and M. D. Logothetis, "Battery drain denial-of-service attacks and defenses in the Internet of Things", *JTIT*, no. 2, pp. 37–45, Jun. 2019, doi: 10.26636/jtit.2019.131919.

[15] C. Pu and T. Song, "Hatchetman attack: A denial of service attack against routing in low power and lossy networks," *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, Shanghai, China, 2018, pp. 12-17, doi: 10.1109/CSCloud/EdgeCom.2018.00012.

[16] P. Kasinathan, C. Pastrone, M. A. Spirito and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Lyon, France, 2013, pp. 600-607, doi: 10.1109/WiMOB.2013.6673419.

[17] Wallgren L, Raza S, Voigt T. "Routing attacks and countermeasures in the rpl-based Internet of Things," *International Journal of Distributed Sensor Networks*. 2013;9(8). doi:10.1155/2013/794326.

[18] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based internet of things, "*HAL (Le Centre Pour La Communication Scientifique Directe)*, May 2016, doi: 10.6633/ijns.201605.18(3).07.

[19] H. -S. Kim, J. Ko, D. E. Culler and J. Paek, "Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2502-2525, Fourthquarter 2017, doi: 10.1109/COMST.2017.2751617.

[20] E. Garcia Ribera, B. Martinez Alvarez, C. Samuel, P.P. Ioulianou, V.G. Vassilakis, "An intrusion detection system for RPL-based IoT networks", *Electronics* 2022, *11*, 4041. https://doi.org/10.3390/electronics11234041.

[21] A. Alazab, A. Khraisat, S. Singh, S. Bevinakoppa, O.A. Mahdi, "Routing attacks detection in 6LoWPAN-Based Internet of Things", *Electronics* 2023, *12*, 1320. https://doi.org/10.3390/electronics12061320.

[22] A. Dvir, T. Holczer and L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL," *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia*, Spain, 2011, pp. 709-714, doi: 10.1109/MASS.2011.76.

[23] G. Simoglou, G. Violettas, S. Petridou, L. Mamatas, "Intrusion detection systems for RPL Security: A comparative analysis", *Computers & Security*, vol. 104, 2021, 102219. https://doi.org/10.1016/j.cose.2021.102219.

[24] S.S. Solapure, H.H. Kenchannavar, K.P. Sarode, "Issues faced during RPL protocol analysis in Contiki-2.7". In: Tuba, M.,

Akashe, S., Joshi, A. (eds) ICT Systems and Sustainability. Advances in Intelligent Systems and Computing, vol 1077. Springer, Singapore, 2020. https://doi.org/10.1007/978-981-15-0936-0_51

[25] C. Pu, J. Brown and L. Carpenter, "A theil index-based countermeasure against advanced vampire attack in Internet of Things," 2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR), Newark, NJ, USA, 2020, pp. 1-6, doi: 10.1109/HPSR48589.2020.9098987.

[26] C. Pu, "Spam DIS attack against routing protocol in the Internet of Things," 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2019, pp. 73-77, doi: 10.1109/ICCNC.2019.8685628.

[27] E. Y. Vasserman and N. Hopper, "Vampire attacks: draining life from wireless ad hoc sensor networks," in IEEE Transactions on Mobile Computing, vol. 12, no. 2, pp. 318-332, Feb. 2013, doi: 10.1109/TMC.2011.274.

[28] R. Kanbur and A. Snell, "Inequality indices as tests of fairness, " *The Economic Journal*, vol. 129, no. 621, pp. 2216–2239, Jan. 2019, doi: 10.1111/ecoj.12637.

[29] A. Varga, OMNeT++, 2014, http://www.omnetpp.org/ (Accessed 9/10/2023).

[30] Y.D. Prabowo, A. I. Kristijantoro, H.L.H.S. Warnars, W. Budiharto, "Systematic literature review on abstractive text summarization using Kitchenham method," *ICIC Express Letters*, Part B: Applications 21852766, ICIC International, 2021, 12, 1, 1075. https://cir.nii.ac.jp/crid/1390009225965346944

[31] T. Matsunaga, K. Toyoda and I. Sasase, "Low false alarm rate RPL network monitoring system by considering timing inconstancy between the rank measurements," 2014 11th International Symposium on Wireless Communications Systems (ISWCS), Barcelona, Spain, 2014, pp. 427-431, doi: 10.1109/ISWCS.2014.6933391.

[32] A. Arış, S. B. Ö. Yalçın, and S. Oktuğ, "New lightweight mitigation techniques for RPL version number attacks," *Ad Hoc Networks*, vol. 85, pp. 81–91, Mar. 2019, doi: 10.1016/j.adhoc.2018.10.022.

[33] S. Chang, S. L. S. Kumar, Y.-C. Hu, and Y. Park, "Power-Positive networking, " *ACM Transactions on Sensor Networks*, vol. 15, no. 3, pp. 1–25, May 2019, doi: 10.1145/3317686.

[34] F. Nizzi, T. Pecorella, F. Esposito, L. Pierucci and R. Fantacci, "IoT security via address shuffling: the easy way," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3764-3774, April 2019, doi: 10.1109/JIOT.2019.2892003.

[35] A. Jalaly Bidgoly and H. Jalaly Bidgoly, "A novel chaining encryption algorithm for LPWAN IoT network," in IEEE Sensors Journal, vol. 19, no. 16, pp. 7027-7034, 15 Aug.15, 2019, doi: 10.1109/JSEN.2019.2910850.

[36] S. Murali and A. Jamalipour, "A Lightweight Intrusion Detection for Sybil Attack Under Mobile RPL in the Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 379-388, Jan. 2020, doi: 10.1109/JIOT.2019.2948149.

[37] C. Pu and B. Groves, "Energy Depletion Attack in Low Power and Lossy Networks: Analysis and Defenses," 2019 2nd International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 2019, pp. 14-21, doi: 10.1109/ICDIS.2019.00010.

[38] K. Zeitz, M. Cantrell, R. Marchany and J. Tront, "Changing the game: A micro moving target IPv6 defense for the Internet of Things," in IEEE Wireless Communications Letters, vol. 7, no. 4, pp. 578-581, Aug. 2018, doi: 10.1109/LWC.2018.2797916.

[39] C. Pu, S. Lim, B. Jung and M. Min, "Mitigating stealthy collision attack in energy harvesting motivated networks," MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 2017, pp. 539-544, doi: 10.1109/MILCOM.2017.8170779.

[40] A. Vasudeva and M. Sood, "Survey on sybil attack defense mechanisms in wireless ad hoc networks, " *Journal of Network and Computer Applications*, vol. 120, pp. 78–118, Oct. 2018, doi: 10.1016/j.jnca.2018.07.006.

[41] A. Raoof, A. Matrawy and C. -H. Lung, "Routing attacks and mitigation methods for RPL-based Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1582-1606, Secondquarter 2019, doi: 10.1109/COMST.2018.2885894.

[42] W. Zhao, S. Yang and X. Luo, "On Threat Analysis of IoT-Based Systems: A Survey," 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 2020, pp. 205-212, doi: 10.1109/SmartIoT49966.2020.00038.