PASSIVE RULE-BASED APPROACH TO DETECT SINKHOLE ATTACK IN 6LoWPAN RPL BASED INTERNET OF THINGS NETWORKS

AL SARAWI SHADI MUSTAFA SUBH

UNIVERSITI SAINS MALAYSIA

2024

PASSIVE RULE-BASED APPROACH TO DETECT SINKHOLE ATTACK IN 6LoWPAN RPL BASED INTERNET OF THINGS NETWORKS

by

AL SARAWI SHADI MUSTAFA SUBH

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

February 2024

ACKNOWLEDGEMENT

{يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ}

[المجادلة: 11]

All praise and thanks are due to ALLAH SUBHANH WA TAALA, the Lord of the world, for giving me the health, strength, knowledge, and patience to complete this Thesis.

Since the Prophet, MOHAMMED “Peace be Upon Him,” said: 'Whoever does not thank people (for their favors) has not thanked Allah (properly)’. Therefore, I would like to express my deep gratitude to my primary supervisor, Dr. Mohammed Anbar, for his encouragement, innovative suggestions, and invaluable help. Additionally, my appreciation and sincere gratitude go to the co-supervisor, Prof. Rosni Abdullah, for support and guidance. I am honored to be under the supervision of these supervisors during the Ph.D. research years.

I would like to express my most sincere and deepest gratitude to those close to my heart, my dearest mother Malak Al Kurdi, and my beloved wife Samar Orabi for their care, love, du'a, and for allowing me to be as ambitious as I wished. I would also like to express my gratitude and thanks to all NAv6 center members, my colleagues, technicians, and administrative staff.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
ARP	Address Resolution Protocol
CAGR	Compound Annual Growth Rate
CIA	Confidentiality Integrity and Availability
DAG	Directed Acyclic Graph
DAO	Destination Advertisement Object
DDoS	Distributed Denial -of -Service
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DNS	Domain Name System
DODAG	Destination Oriented Directed Acyclic Graph
ICT	Information Communication Technology
IDC	International Data Corporation
IETF	Internet Engineering Task Force
INTI	Intrusion detection of Sinkhole attack on 6LoWPAN for IoT
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ITU	International Telecommunications Union
LoWPANs	Low power Wireless Personal Area Networks
MP2P	Multipoint-to-point
P2MP	Point-to-multipoint
P2P	Point-to-point
PRBA	Passive Rule-Based Approach
QoS	Quality of Services
ROLL	Routing over Low Power and Lossy Links
RPL	Routing Protocol for Low-Power and Lossy Network
WSNs	Wireless Sensor Networks

LIST OF APPENDICES

PENDEKATAN PERATURAN PASIF UNTUK MENGESAN SERANGAN LUBANG BENAM DALAM RANGKAIAN INTERNET BENDA BERDASARKAN RPL 6LOWPAN

ABSTRAK

Internet Benda (IoT) yang berkembang pesat merentasi pelbagai aplikasi memungkinkan berbilion peranti, manusia, dan perkhidmatan bertukar maklumat dan berhubung antara satu sama lain. Oleh kerana banyaknya maklumat sulit yang terkandung dalam data yang dikongsi, keselamatan maklumat merupakan kebimbangan utama yang mesti dipertimbangkan. Kebanyakan ancaman terhadap keselamatan IoT pada masa ini tertumpu pada lapisan rangkaian, yang diwakili oleh protokol penghalaan untuk rangkaian berkuasa rendah dan hilang (RPL). RPL terdedah kepada pelbagai serangan yang boleh menyebabkan gangguan rangkaian. Serangan lubang benam ialah salah satu serangan yang mengeksploitasi kelemahan RPL dan menarik trafik yang banyak dengan mengiklankan maklumat palsu yang mengubah keutamaan penghalaan bagi nod-nod lain. Matlamat tesis ini adalah untuk mencadangkan Pendekatan Berasaskan Peraturan Pasif yang dinamakan PRBA untuk mengesan serangan lubang benam dalam rangkaian IoT berasaskan RPL 6LoWPAN, yang terdiri daripada empat peringkat untuk mencapai empat objektif penyelidikan, iaitu: (1) Peringkat Pengumpulan dan Pra-pemprosesan Data yang memenuhi objektif untuk mentransformasi nilai penggunaan kuasa yang dikumpul dan trafik rangkaian ICMPv6 yang ditangkap ke dalam format yang bermakna; (2) Peringkat Pemilihan Ciri yang memenuhi objektif untuk mengurangkan saiz ciri dengan memilih ciri paling ketara yang menyumbang kepada pengesanan serangan lubang benam; (3) Peringkat Petunjuk Tingkah Laku yang memenuhi objektif untuk mengenal pasti tingkah laku

abnormal serangan lubang benam menggunakan ciri-ciri ICMPv6 dan penggunaan kuasa dari peringkat sebelumnya; dan (4) Peringkat Pengesanan Serangan Lubang Benam yang memenuhi objektif untuk memutuskan sama ada terdapat serangan lubang benam dalam dua langkah. Langah Pertama adalah Berasaskan Peraturan dan Langkah Kedua adalah Kaedah Undian Tanpa Wajaran. Pendekatan PRBA yang dicadangkan telah dilaksanakan dan dinilai menggunakan simulator COOJA dan kemudian dibandingkan dengan pendekatan sedia ada lain, termasuk pendekatan ELNIDS dan teknik NPMT. Dari segi ketepatan pengesanan, hasil simulasi menunjukkan bahawa Kadar Ketepatan pendekatan PRBA adalah 100% dengan kaedah undian tanpa wajaran, dan Kadar Ketepatan pendekatan PRBA ialah 90% dan kadar positif palsu ialah 0.2% tanpa kaedah undian tanpa wajaran. Dari segi penggunaan kuasa, pendekatan yang dicadangkan memenuhi keperluan nod terkekang tanpa mengakibatkan peningkatan dalam penggunaan kuasa disebabkan oleh reka bentuk penggunaan.Tambahan pula, keputusan simulasi menunjukkan bahawa menggunakan lima penunjuk tingkah laku utama dengan ketara meningkatkan ketepatan pengesanan, yang disokong oleh kaedah undian tidak wajar. "Oleh itu, ini akan mencapai objektif utama penyelidikan ini, iaitu untuk mencadangkan pendekatan berasaskan peraturan untuk mengesan serangan lubang benam dengan ketepatan yang tinggi." Di samping itu, beberapa ciri baharu menyumbang kepada penyelidikan.

PASSIVE RULE-BASED APPROACH TO DETECT SINKHOLE ATTACK IN 6LOWPAN RPL BASED INTERNET OF THINGS NETWORKS

ABSTRACT

The Internet of Things (IoT) is growing rapidly across a wide range of applications that enable billions of devices, people, and services to exchange information and connect with one another. Due to the large amount of confidential information contained in the shared data, information security is a key concern that must be considered. Most existing security challenges in IoT are focused on the network layer, which is represented by its routing protocol for low-power and lossy networks (RPL). The RPL exposes to various attacks that may lead to network disruption. A sinkhole attack is one of the attacks that utilize the vulnerabilities in RPL and attracts considerable traffic by advertising falsified information data that change the routing preference for other nodes. The aim of this thesis is to propose a Passive Rule-Based Approach named PRBA to detect sinkhole attacks in 6LoWPAN RPL-based IoT Networks, which consists of four stages to achieve four research objectives, which are: (1) Data collection and preprocessing stage that fulfills the objective to transform the collected power consumption values and the captured ICMPv6 network traffic into a meaningful format; (2) Feature Selection stage that fulfills the objective to decrease the size of the features by selecting the most significant features that contribute to detecting sinkhole attacks; (3) Behavioral Indicators stage that fulfills the objective to identify abnormal behavior of sinkhole attacks using the features of the ICMPv6 and power consumption from the previous stage; and (4) Sinkhole Attack Detection stage that fulfills the objective to decide whether there is a sinkhole attack in two steps. Step One is Rule-based, and Step Two is an Unweighted Voting Method.

The proposed approach PRBA is implemented and evaluated using the COOJA simulator and then compared with other existing approaches, including the ELNIDS approach and NPMT technique. In terms of detection accuracy, the simulation results show that the PRBA approach Accuracy Rate is 100% with an unweighted voting method, and PRBA Approach Accuracy Rate is 90%, and the False-positive rate is 0.2% without an unweighted voting method. In terms of power consumption, the proposed approach meets the requirements of the constrained nodes without causing an increase in power consumption due to the deployment design. Furthermore, the simulation results show that using the five major behavior indicators significantly improves detection accuracy, which is supported by unweighted voting methods. “Consequently, this will achieve this research’s primary objective, which is to propose a rule-based approach for detecting sinkhole attacks with high accuracy.” In addition, several new features contribute to the research.

CHAPTER 1

INTRODUCTION

1.1 Overview

The Internet of Things (IoT) contains many constraints, such as limited processing capability, low storage, short power life, and limited transmission range. Therefore, a successful implementation of IoT relies on the existing Internet Protocol (IP) infrastructure to optimally utilize readily available resources while benefiting from the vast address space of Internet Protocol Version 6 (IPv6) (Ghaleb et al., 2018).

The International Data Corporation (IDC) estimated that there will be 55.7 billion connected IoT devices by 2025. IDC also reported that by 2025, IoT devices would generate 73.1 zettabytes of data, triple the amount generated in 2019 (18.3 zettabytes) (Gaber et al., 2022). In addition, 70% of breaches, according to IDC, originate at endpoints, despite increased IT spending on this threat surface. Also, Columbus (2020) forecasted that the global security market would grow from $167.1 billion in 2019 to $248.26 billion by 2023, growing at a 10.4% Compound Annual Growth Rate (CAGR). Additionally, the COVID-19 pandemic has increased security needs, becoming the most urgent of all priorities since nearly every company has employees working from home. Furthermore, Statista (2021) forecasted end-user spending on IoT solutions to increase steadily globally from 2017 to 2025, as shown in Figure 1.1.

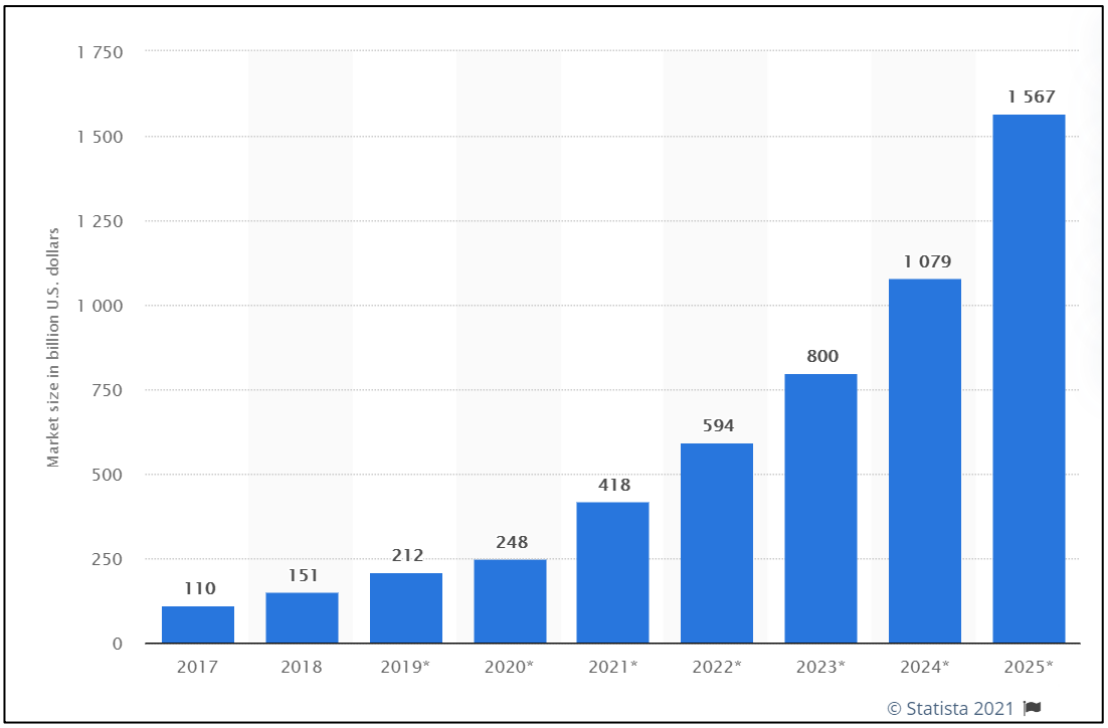

Figure 1.1 Forecast on global spending of end-user on IoT (Statista, 2021)

IoT provides the opportunity for wearable devices, home appliances, and systems to exchange information to provide services to end-users. Consequently, IoT enables billions of devices to exchange information and connect with services and people. Due to the substantial amount of personal and confidential information in the shared data, information security is a crucial concern that must be considered. Additionally, hardcoded credentials are easily compromised due to reused passwords. The primary goal of IoT security is to maintain the confidentiality and privacy of users by ensuring the security of devices, data, and infrastructures within the IoT ecosystem and guaranteeing service availability (Hassan, W. H., 2019; Zhang et al., 2014)

Among routing attacks, the sinkhole attack is the type of attack under the Denial of Service (DoS) category and one of the most destructive for IoT environments. Additionally, it is more destructive when combined with other attacks and may cause significant damage. There is a risk that this attack may cause

information loss and packets not being delivered to the base station if it goes undetected and disconnects the nodes from the internet. Additionally, a sinkhole attack increases network overhead and reduces the network's lifespan (as a result of elevated energy consumption), leading to network destruction (Padmanabhan et al., 2022; An & Cho, 2022; Mehta et al., 2022; Rehman et al., 2019; Cervantes et al., 2015)

According to Abd Halim et al. (2021), the most prevalent DDoS attack in agriculture is sinkhole attacks that fool sensor nodes into using a fake fastest route information, forcing the nodes to send their traffic to the malicious sinkhole node.

1.2 Introduction

This section presents an introduction to the IoT, Routing Protocol for Low-Power and Lossy Networks (RPL), and IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN), security issues, and different types of attacks that threaten IoT networks as shown in Sections 1.2.1, 1.2.2, 1.2.3 and 1.2.4, respectively.

1.2.1 IoT

IoT architecture includes various internet-connected sensors and end devices, such as smart cars, appliances, and homes. Devices are set up and strategically placed to allow communication with users over the Internet through gateway nodes that receive and send data, as shown in Figure 1.2 (Pundir et al., 2020). The IPv6's potentially unlimited address space allows billions or trillions of these devices to be connected to the internet. The introduction of IPv6 on LoWPAN networks (6LoWPAN) by the Internet Engineering Task Force (IETF) extends these intelligent devices on the Internet and integrates IPv6 into Wireless Sensor Networks (WSN). 6LoWPAN uses the RPL to route the data. However, RPL is susceptible to various

routing attacks, which can cause network damage (MelancyMascarenhas and Vineet Jain, 2018).

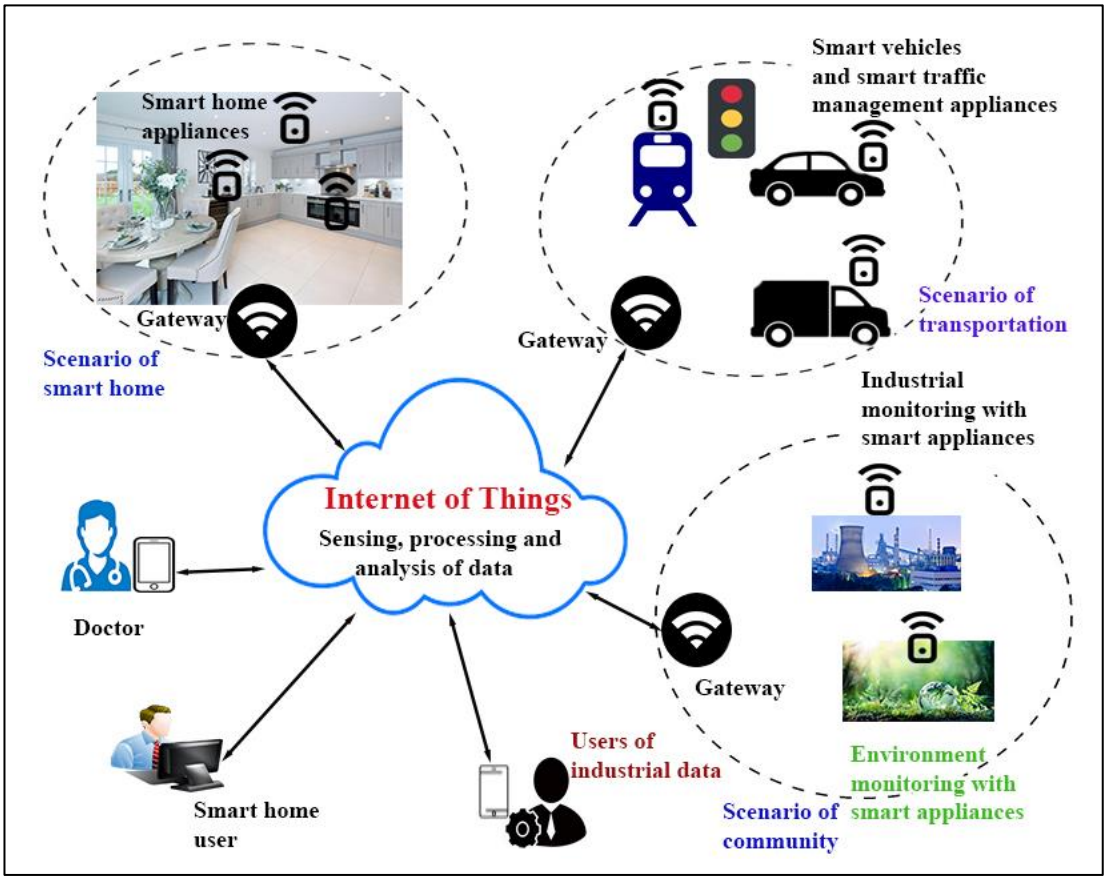

Figure 1.2 Generic IoT architecture (Pundir et al., 2020)

1.2.2 6LoWPAN

The WSN is the core of IoT technology because it allows various sensor applications to be part of intelligent ecosystems. The most challenging aspects of this system are power consumption or network lifetime and security. The IETF developed the 6LoWPAN standard in the RFC4944 document to address the challenges in a WSN, a low throughput wireless network with low-powered and resource-constrained nodes to enable communication via IPv6 among low-cost and low-power devices. Furthermore, the compatibility of the MAC and physical layers with the IEEE 802.15.4

standard allows it to run IPv6 (Ahmad et al., 2022; Melancy Mascarenhas and Vineet Jain, 2018)

One of the most popular protocols for managing WSN is 6LoWPAN, which uses RPL to build the network topology to route data to and from the Access Point (Ahmad et al., 2022; Verma et al., 2022).

1.2.3 RPL

The RPL protocol was designed for the 6LoWPAN to realize the IoT concept. RPL has many means for routing messages, such as DIS (DODAG Information Solicitation), DAO (DODAG Destination Advertisement Object), and DIO (DODAG Information Object). RPL has better overhead, delay, and power than others, such as LOADng and Ad-hoc On-demand Distance Vector Protocol (AODV) (La et al., 2013; Kathuria et al., 2013). The major drawbacks of RPL are the weak physical protection of nodes and the low capabilities of nodes to provide strong cryptography (Le et al., 2016).

The IETF standardized the RPL protocol in RFC4919 and RFC6550 documents (Kushalnagar et al., 2007; Winter et al., 2012) that focus on IP for LLNs by employing IPv6 over 6LoWPAN, leading to standardizing IPv6 in IEEE 802.15.4 networks. Subsequently, the IETF formed the Routing over Low Power and Lossy Links (ROLL) group to specify RPL. RPL is now a standard routing protocol for IPv6 connected to IoT, and the RPL's objective function selects an optimal route. Each node is assigned an ID centered on the rank and IPv6 address. Nodes exchange graph-related information with other nodes using three RPL-specific Internet Control Message Protocol version 6 (ICMPv6) messages: DIS, DAO, and DIO, as shown in Figure 1.3 (Liscio, 2016).

Routing protocols allow routers to establish routes between nodes by exchanging route details. However, networks could be vulnerable to attacks if these route details are leaked (Airehrour, 2017).

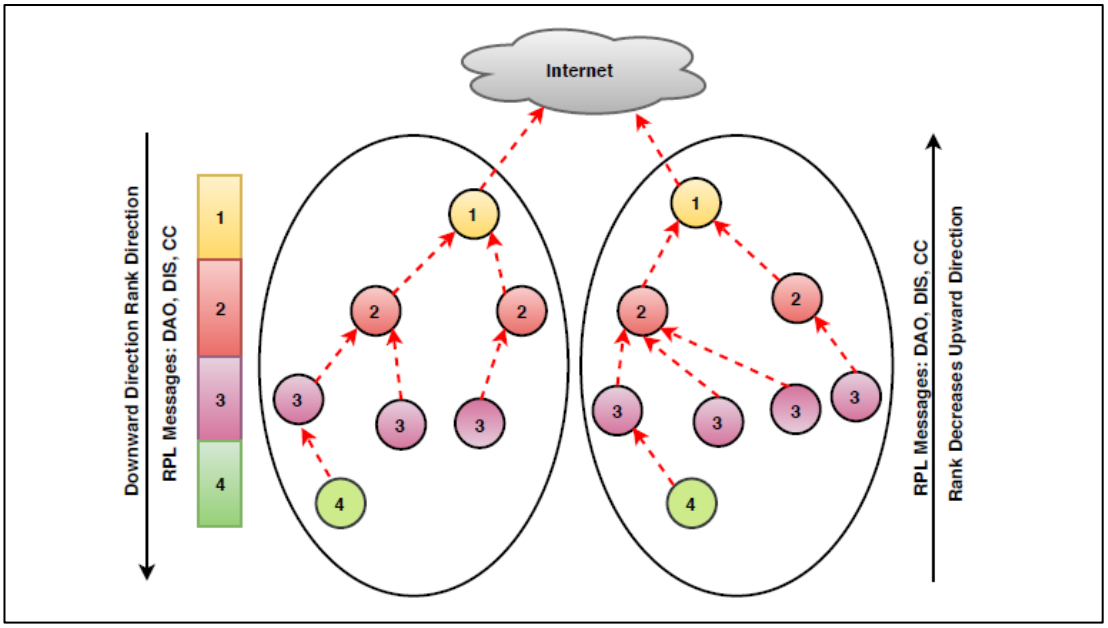

Figure 1.3 RPL Topology (Bhale et al., 2020)

1.2.4 RPL Security

The RPL protocol is susceptible to many vulnerabilities due to the characteristics of LoWPANs, such as low power consumption. In some environments, 6LoWPAN-connected devices may sleep for extended time to conserve power and may not be able to communicate during these sleep periods. In addition, it is expected that many devices will be deployed. This constraint forces the need for a large address, which is well covered by IPv6 capacity addressing. The RPL protocol defines many approaches to secure its protocol, such as integrating local and global repair approaches and loop avoidance and detection approaches (Arshad et al., 2020; Ech-Chaitami et al., 2011)

The RPL-based network is vulnerable to different attacks and one of the most destructive is the sinkhole attack that could affect and destroy the RPL network

topology (An & Cho, 2022; Thavamani et al., 2022; Padmanabhan et al., 2022). For example, a sinkhole attack can create energy holes in the network by draining the surrounding nodes' energy. In addition, it can spread false advertisements, resulting in potentially dangerous or inappropriate responses (Chahid et al., 2017).

1.3 Research Motivation

Technology has become an indispensable part of human life, and one of the revolutionizing technologies is the IoT. Since numerous things are interconnected, there is a possibility of security breaches. Deploying billions of IoT devices will raise critical management, scalability, reliability, availability, and security issues. Therefore, researchers must focus on securing the networks and system from vulnerabilities and weaknesses, especially severe threats to IoT that aim to degrade network performance, drain device batteries, exhaust the storage, and cause packet loss and delay (Ganchev et al., 2018)

The routing protocols on IoT networks have many vulnerabilities that expose the network to threats, such as Sybil, sinkhole, blackhole, and HELLO flood attacks. The sinkhole attack is a serious threat to IoT networks, and its attack severity multiplied when combined with other attacks (Arshad et al., 2020; Yadollahzadeh et al., 2021).

Statista (2020) statistics indicate that attacks on routing protocols make up 20% of threats worldwide, and the number is forecasted to rise to 23% by 2021. Moreover, compromised IoT devices compose 13% of threats worldwide and are predicted to rise to 21% by 2021.

The statistics also projected that the global expenditure related to IoT security will reach $36.6 billion by 2025, at 23.9% CAGR within the forecasted time. The

major reasons that push the IoT security market growth are the increase in ransomware attack incidents on IoT devices, security concerns for critical infrastructure, data risks in IoT networks, and growing IoT security regulations (Statista, 2021).

According to Kaspersky Lab's IoT report, IoT devices experienced more than 120,000 malware attacks in the first six months of 2018, triple the amount in all of 2017. At the same time, 2017 also saw a 10-times increase in smart device malware compared to 2016 (Kaspersky, 2018). IBM reported that the combined IoT attacks were 400 percent higher between October 2019 and June 2020 compared to the previous two years, as shown in Figure 1.4 (IBM, 2021).

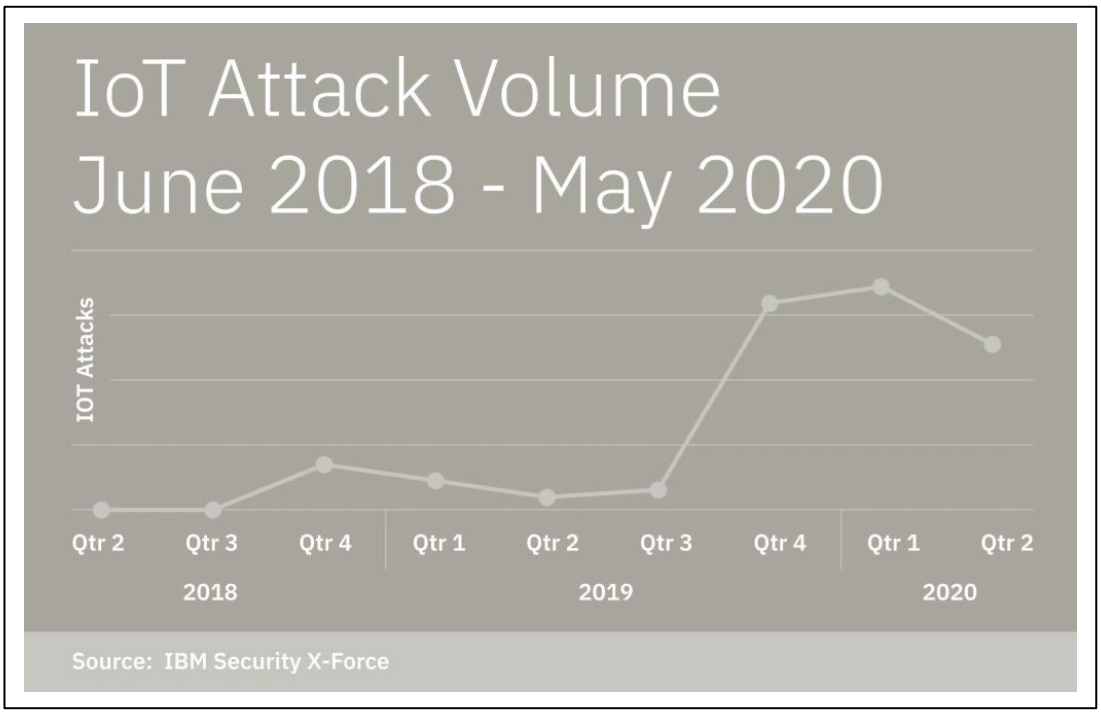

Figure 1.4 IoT Attack Volume between 2018 and 2020 (IBM, 2021)

Undetected attacks may have significant consequences since they could involve millions of internet-connected devices, and many applications and services that rely on sensors use the RPL protocol. An attack may result in information loss and endanger human life in the worst-case scenario. For example, suppose an intelligent medical device that monitors a human’s heart rate is disconnected from the internet

due to attacks on the RPL protocol. In that case, the data from the heart monitor cannot reach the monitoring system at the hospital, preventing the user from receiving timely medical attention in case of an emergency. Similarly, an attack on a hospital could result in fatalities due to disrupted services. For example, in September 2020, a hospital in Germany was the target of a DoS attack, resulting in the death of a patient after the health service halted due to the attack (Jalali et al., 2021).

1.4 Problem Statement

IoT is connecting with heterogeneous devices and communicating to transfer data over a network without requiring human-to-human or human-to-computer interaction. These devices are deployed in an open place. However, IoT devices are constrained due to limited power, storage, and energy. The intruder launches different routing attacks due to constrained devices. In the existing system, the proposed approaches did not fulfill the security solution. Therefore, the nodes can be compromised, and the attacker can capture sensor nodes and obtain all critical information, data, and code stored on the node, which was previously a legitimate member of the network (Stephen et al., 2017).

Due to the constrained nature of the RPL network, many attacks can damage the IoT network. A Sinkhole attack is one of the most stringent routing attacks. It creates nodes with misleading routing information, removes packets, overrides data, or transfers selected data. Additionally, it can cause energy in the surrounding nodes, causing energy gaps in the network (Arshad et al.,2020; An & Cho,2022; Waoo et al., 2021; Rehman et al.,2019). Therefore, several approaches have been proposed to detect sinkhole attacks in the RPL network.

Bhale et al. (2020) stated that the most common and efficient sinkhole attack detection approaches in 6LoWPAN RPL networks are distributed IDSs, such as SVELTE (Raza et al., 2013) and INTI (Cervantes et al., 2015). However, both approaches consume significant power and have low detection accuracy. The high-power consumption is due to the heavy processing and inappropriate deployment design, which shortens nodes' battery life. The moderate detection accuracy and high false-positive rate (between 4% and 10%) of the IDSs are due to two factors. First, inappropriate features selection that does not contribute to the attack detection, and second, inadequately studied behavioral characteristics or indicators that contribute to sinkhole attack detection that negatively affects the IDS's detection accuracy (Kenji et al., 2015; Bhale et al., 2020).

Mahmood et al. (2018) attempted to overcome the drawbacks of SVELTE and INTI in detecting sinkhole attacks in RPL-based networks by proposing the Neighbor Passive Monitoring Technique (NPMT). However, the results showed that although the detection accuracy improved slightly due to the features used to detect sinkhole attacks, the behavioral characteristics contributing to the detection of sinkhole attacks are not well studied. In addition, the power consumption slightly increased due to the inappropriate deployment design.

The existing mechanisms for detecting Sinkhole attack suffer from several problems that can be summarized as follows:

- The existing approaches to detecting sinkhole attacks do not consider the significant features and behavioral characteristics that contribute to accurately detecting the attacks.
- The existing approaches to detecting sinkhole attacks suffer from high power consumption due to deployment design that can increase network overhead and

drain the surrounding nodes' energy, creating energy gaps and reducing the network's lifespan.

Hence a better solution is needed to detect sinkhole attacks with low power consumption and high accuracy.

1.5 Research Objectives

This thesis's primary goal is to propose a passive rule-based approach for detecting sinkhole attacks in RPL-based 6LoWPAN IoT networks that consume low power and have high detection accuracy. The following objectives are fundamental to achieving the research's primary goal:

- To propose a set of features to distinguish nodes exhibiting abnormal behavior in RPL networks.
- To propose a set of behavioral indicators contributing to the detection of sinkhole attacks in RPL-based networks. The indicators are (i) Bi-Directional, (ii) Bi-Directional Frequency, (iii) DIO Transmission Frequency, (iv) Rank Harmony, and (v) Power Consumption.
- To propose a rule-based mechanism to detect sinkhole attacks based on the features and behavioral indicators from the first and second objectives.

1.6 Research Scope

The scope of the proposed approach is limited to sinkhole attack detection in RPL-based networks and does not consider the mobility and mitigation phase, which could be future work. The dataset used to evaluate and test the Passive Rule-Based

Approach (PRBA) is self-generated using simulated traffic comprising actual sinkhole attacks. Table 1.1 lists the research scope and limitations.

Table 1.1 Research Scope and Limitations

Items	Scope of Research
WSN Operating System	Contiki
Sensor simulator	COOJA
Performance metrics	Power consumption and detection accuracy
Detection Approach	Anomaly-based Approach
IoT Application	Smart home
Network Target	6LoWPAN
Routing Protocol	RPL
Protocol Type	ICMPv6
Target Layer	Network layer
Attack Type	Sinkhole attack
Dataset	Simulated traffic dataset
Router	Fixed location inside the network without energy limitations.
Placement of the proposed approach	Installed on a PC or Laptop to analyze the data and identify suspicious nodes

1.7 Research Contribution

The main contribution of this research is a high-level approach for sinkhole attack detection in 6LoWPAN RPL-based IoT networks with low power consumption and high accuracy, called PRBA. Moreover, the passive node in this approach consumes sufficient power to perform data analysis and processing without affecting other constrained nodes in the network. Furthermore, the passive node is connected via a wired network to ensure it will not interfere with the normal node's power. In addition, having the passive node connected via a wired network will keep it

functioning even if the jamming attack targets the communication channels of IoT nodes. The rest of the research contributions are as follows:

- A set of new features derived from basic features that allow distinguishing nodes exhibiting abnormal behavior. It can be used to develop an efficient approach for classifying and detecting sinkhole attacks in RPL-based networks.
- A set of behaviors to be considered an indicator of a sinkhole attack in an RPL-based network. The indicators are (i) Bi-Directional, (ii) Bi-Directional Frequency, (iii) DIO Transmission Frequency, (iv) Rank Harmony, and (v) Power Consumption.
- A rule-based mechanism with a predefined threshold value for detecting sinkhole attacks based on the features and behavioral indicators proposed in the first and second objectives to maximize detection accuracy and minimize power consumption.

1.8 Research Steps

The following steps are followed while conducting this research:

First Step - Literature Review. This step presents the background of IoT, RPL, and 6LoWPAN. It also studies the accuracy of the existing related work to detect sinkhole attacks on the RPL networks for IoT.

Second Step - Literature Analysis. This step analyzes the existing IDS and identifies their advantages and limitations. A thorough analysis provides a better understanding of the existing solutions, research problems, limitations, and research scope, providing a solid basis for the proposed approach.

Third Step - Design and Modeling. This step discusses the proposed approach, PRBA, by setting a new rule and selecting the appropriate feature to enhance the detection approach.

Fourth Step - Implementation and Evaluation. This step involves implementing and evaluating the proposed approach. Analysis of the evaluation result shows that the dataset generated from an actual network resulted in different rules and behavioral indicators that can be used to evaluate the proposed approach regarding power consumption and detection accuracy.

Fifth Step - Conclusion. The last step summarizes this research work by highlighting its contributions and limitations and suggesting potential future work; Figure 1.5

shows the research steps.

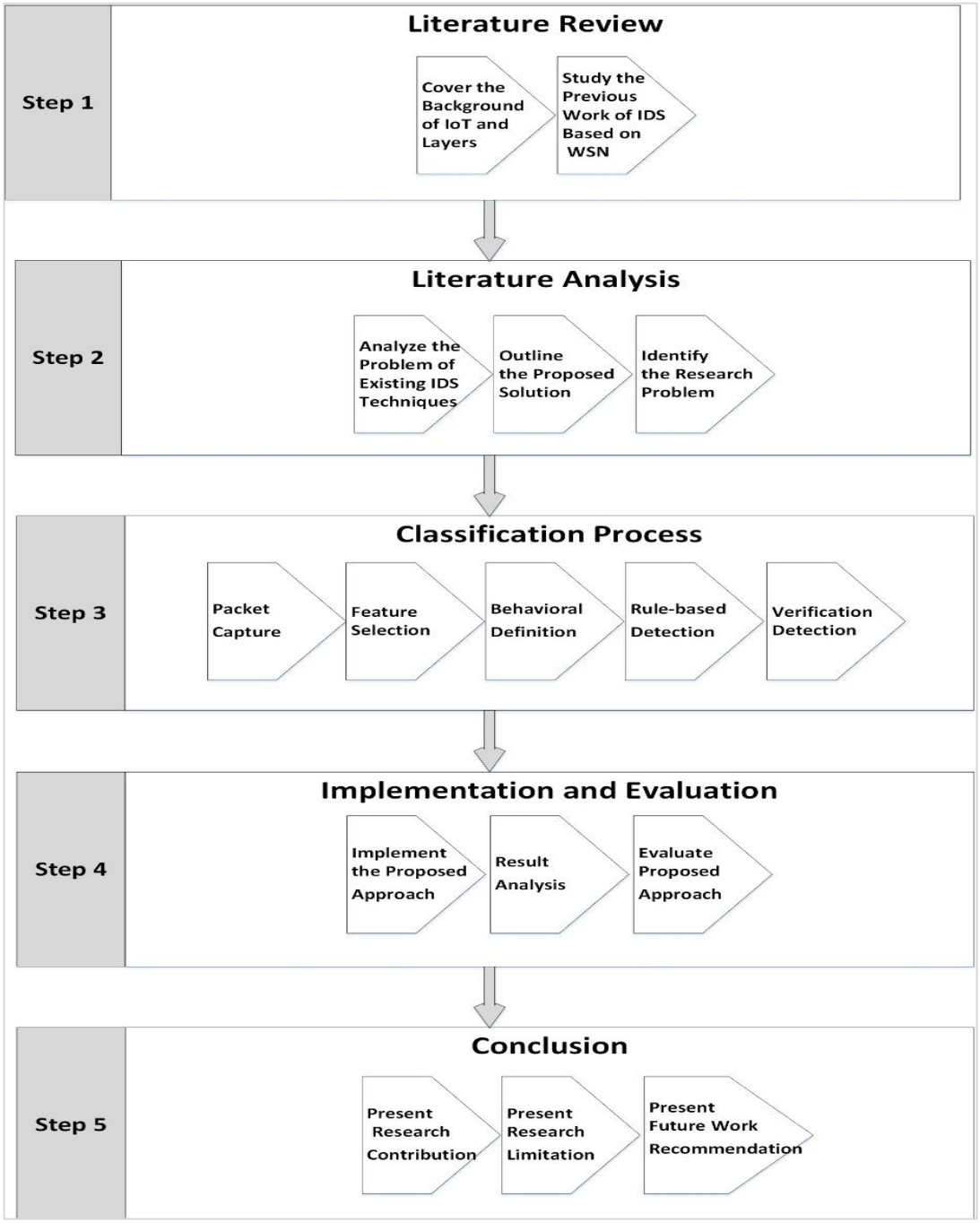

Figure 1.5 Research Steps

1.9 Thesis Organization

This thesis comprises six chapters, as follows:

Chapter 2 provides background information for understanding the work, including an overview of IPv6, 6LoWPAN, RPL networks, limiting factors, IoT attacks, and literature survey of the related work in the research domain, and a look at the proposed detection model to be used.

Chapter 3 presents the proposed approach's methodology by explaining its design and describing its integrated phases to detect sinkhole attacks in RPL-based networks.

Chapter 4 explains the tools and programming languages used for implementation. Also described are the proposed approach's design and implementation scenarios

Chapter 5 describes the threshold values and PRBA topology. Besides, ground truth test scenarios and evaluation methods of PRBA and detection accuracy. Finally, existing approaches compare with PRBA results.

Chapter 6 concludes this thesis and provides several future works for this research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents the study of the state-of-the-art IDS approaches developed to detect sinkhole attacks in RPL-based networks for IoT, reviews the literature on the improvements of this protocol, and highlights these studies' limitations that serve as the basis for this work. The reviewed literature includes approaches against phishing sinkhole attacks in the RPL-based network and various detection classifications according to the different approaches.

The chapter's organization is as follows. Section 2.3 provides an overview of IPv6, followed by an overview of 6LoWPAN in Section 2.4. Next, Section 2.5 outlines the background of RPL, RPL security, IoT attacks, and IDS classification for IoT. The adaptive threshold value is covered in Section 2.6. Section 2.7 formulates the feature selection for sinkhole attack detection in RPL-based networks for IoT. Section 2.8 discuss the related works in sinkhole attack detection in RPL networks for IoT. Finally, Section 2.9 summarizes Chapter 2.

Figure 2.1 illustrates the major research background areas, literature review, and relationship between research elements. This chapter presents each level in a section for a clear overview of its content.

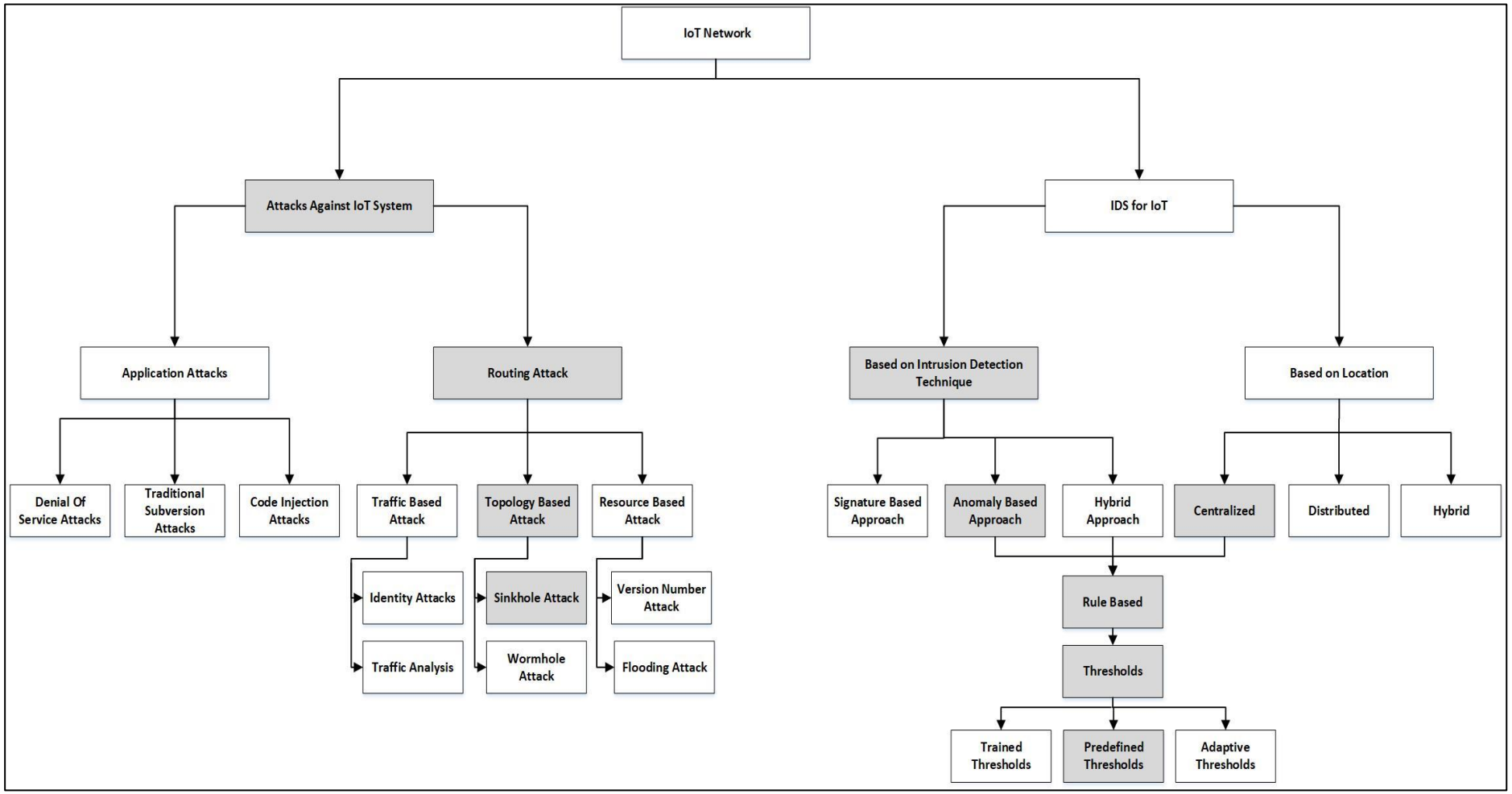

Figure 2.1 Literature Survey and Related Work

2.2 Background

A sinkhole attack is a network layer attack in which an attacker draws a vast amount of traffic and diverts or drops them to deny a base station (root) from getting complete data from nodes. The sinkhole node transmits fabricated routing information to the neighboring nodes, which use it in their routing metrics to select the best route for data transmission, resulting in all their traffic going through the sinkhole node before reaching the destination (Padmanabhan et al., 2022; Kibirige & Sanga, 2015). The sinkhole node decreases the network lifetime since it continuously consumes and drains the node's energy.

The IETF introduced two standard IoT protocols, 6LoWPAN and RPL. Unfortunately, both lack an effective measure to protect against security attacks, and it is challenging to implement secure routing approaches in IoT networks. At the same time, 6LoWPAN has many challenges and limitations in IP connectivity, network topologies, small packet size, security discovery, constrained resources, and management. Therefore, researchers must consider all the challenges and constraints to achieve secure routing in IoT networks (Airehrour, 2017; Bhale et al., 2020).

The subsequent sections present an overview of IPv6, 6LoWPAN, and RPL with their terminologies, control messages, security, IoT attacks, and IoT classifications. Finally, it also discusses various IDS approaches.

2.3 Overview of IPv6

The IoT implementation usually leverages the current IP architecture and infrastructure to maximize the utilization of existing resources and benefit from the vast IPv6 address space. Additionally, 6LoWPAN is a promising solution that enables wireless communication for constrained devices via low-power networks by adding an

adaptation layer in the network protocol stack, as shown in Table 2.1 (Yang and Li, 2010; Xiong et al., 2011; Kfoury et al., 2019).

Table 2.1 6LoWPAN Protocol Stack (Kfoury et al., 2019)

Application Layer	COAP
Transport Layer	UDP
Network Layer	IPv6 | ICMP | RPL
Adaptation Layer	6LoWPAN Adaption
MAC Layer	IEEE 802.15.4
PHY Layer	IEEE 802.15.4

IPv6, developed in 1995, is the next generation of IP to replace Internet Protocol Version 4 (IPv4), designed as an upgrade to IPv4 to enable global connectivity of internet-enabled devices. IPv4 was introduced in 1981, and the number of interconnected computers has grown dramatically, leading to the exhaustion of publicly available IPv4 addresses. The address space of IPv4 is 32-bit (4 bytes), constituting a maximum of 2^{32} or roughly 4.3 billion unique IP addresses for use within the Internet, whereas IPv6 address space size is 128-bit (16 bytes), constituting a maximum of 2^{128} IP addresses. The ample IPv6 address space can resolve the IP address exhaustion issue in IPv4. Table 2.2 summarizes the 12 main differences between the two IP versions (Shiranzaei & Khan, 2015).

Table 2.2 Differences between IPv4 and IPv6 (Shiranzaei & Khan , 2015)

Features	IPv4	IPv6
Developed	1981	1999
Address Space	32 bits (4 bytes)	128 bits (16 bytes)
Total number of unique addresses	4,294,967,296	340,282,366,920,938,463, 463,374,607,431,768,211, 456
IP Address format	Represented in four sets of decimal digits separated by dots (“.”). For instance, 10.30.203.30, and the limit for each set is from “0” to “255”. If a set is zero, use a single zero. For example, 10.30.0.0	Represented in eight hexadecimal digit sets separated by colons (“:”). For instance, FE80:0000:0000:0000:03 01:A5B3:D123:3134, If all digits in each set are zero, then use a double colon. For example, FE80::0301:A5B3:D123:3 134
Fragmentation	It is fragmented when a packet is too big for the next link. In IPv4, the sender and forwarding routers are responsible for the fragmentation.	Only the sender does fragmentation.
Mobility	Not supported. If a mobile node changes its location, its address must be re-established	Supported with MIPv6

2.4 Overview of 6LoWPAN

6LoWPAN is a promising solution that integrates IPv6 into low-power networks by adding an adaptation layer in the network protocol stack, such as IEEE 802.15.4, as shown in Figure 2.2. This solution allows using the current IP architecture and infrastructure to maximize the utilization of existing resources and benefit the vast IPv6 address space (Xiong et al., 2011; Devasena, 2016).

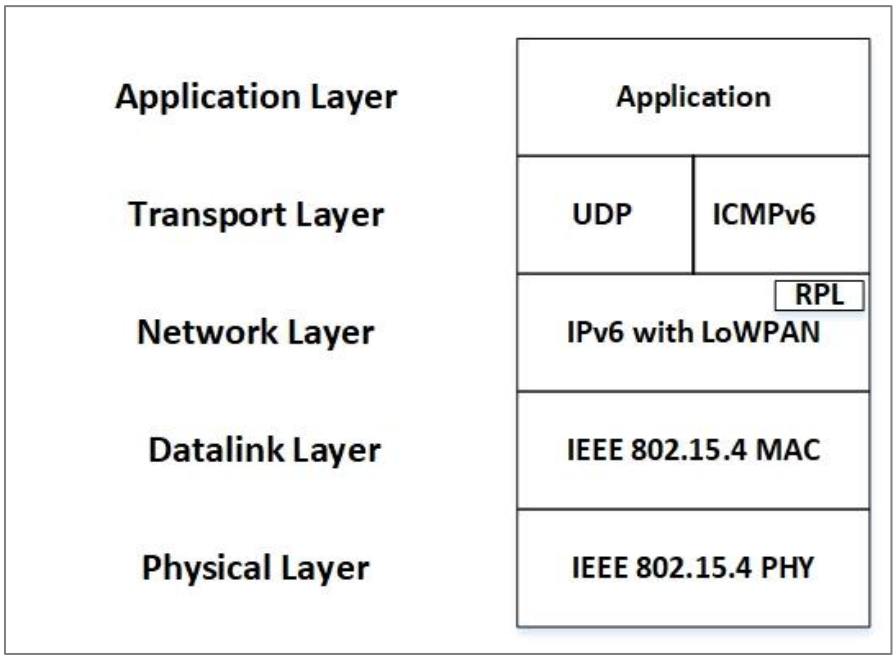

Figure 2.2 6LoWPAN Protocol Stack (Devasena, 2016)

A mote is a sensor node in a sensor network that can process, gather sensory data, and communicate with other nodes. Figure 2.3 visualizes the standard connectivity of a 6LoWPAN network, comprising motes, to the Internet via an edge router. Since ingress and egress traffic passes through the edge router, there is a possibility of a threat to the 6LoWPAN network from the Internet and vice versa. The nodes send control information to an Internet-connected device and might pose a threat. Security breaches may compromise data and motes within the networks, which indirectly threatens the CIA (Confidentiality, Integrity, and Availability) of data and resources (RENUKA, 2016).

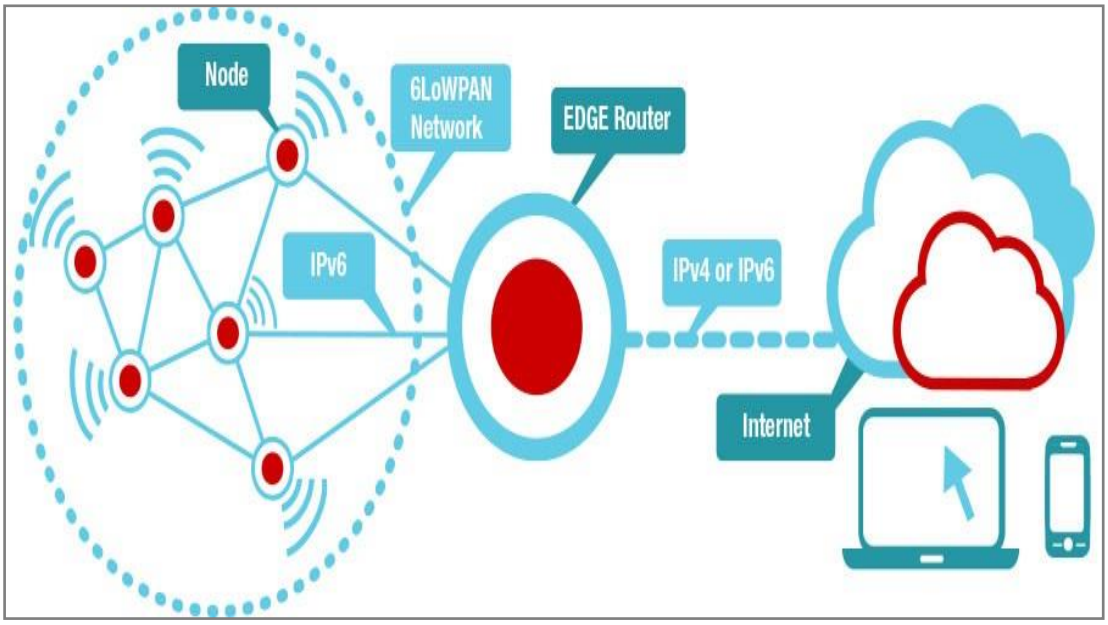

Figure 2.3 6LoWPAN Network (RENUKA, 2016)

2.5 Overview of RPL

RPL is a standard routing protocol used in WSNs and used in various settings like smart grids, industrial, and home networks. RPL Messages start from a root node or sink node; RPL builds with the Root's DIO messages. DODAG tree contains only one Root. Nodes receiving the DIO message select the parent to sender, with a rank value calculated for the parent's rank value and other parameters. The rank value may depend on the distance from the root node energy of the link. The network owner can decide the rank value calculation parameters. The nodes continue to broadcast the DIO message from the Routing Tree (Patel, 2016), as shown in Figure 2.4.

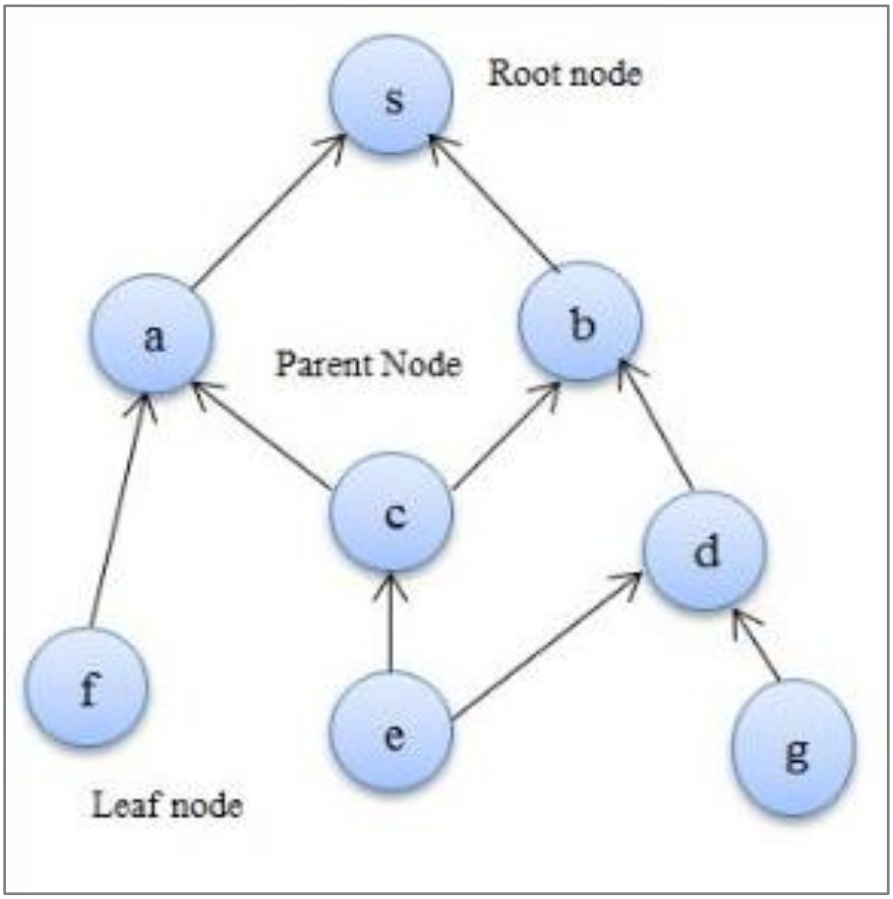

Figure 2.4 RPL Routing Tree (Patel, 2016)

Table 2.3 lists the main features of RPL according to Zhao et al. (2017).

Table 2.3 Features of RPL

Features	Description
Loop avoidance and detection	RPL has global and local recovery mechanisms for loop detection and topology recovery if the topology changed. In RPL, node's rank must be higher than its parent.
Self-configuration	Network paths are discovered dynamically using IPv6 neighbor discovery mechanisms. The dynamic discovery of destinations and new routes improves performance of the network via self-configuration.
Target networks	6LoWPAN networks, Low-Power and Lossy Networks (LLNs), and other IPv6 networks.