AN ADAPTIVE DROPOUT ARTIFICIAL NEURAL NETWORK-BASED APPROACH FOR DETECTING VERSION NUMBER ATTACKS IN RPL-BASED IOT NETWORK

NADIA ADNAN ABDALLAH ALFRIEHAT

UNIVERSITI SAINS MALAYSIA

2025

AN ADAPTIVE DROPOUT ARTIFICIAL NEURAL NETWORK-BASED APPROACH FOR DETECTING VERSION NUMBER ATTACKS IN RPL-BASED IOT NETWORK

by

NADIA ADNAN ABDALLAH ALFRIEHAT

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

July 2025

ACKNOWLEDGEMENT

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

[المجادلة: 11]

First and foremost, all praises are due to Allah, the Almighty, for bestowing upon me the patience, strength, and guidance necessary to complete this thesis successfully. The Prophet Mohammed, "Peace be Upon Him," said, *"Whoever does not thank people has not thanked Allah."* Therefore, I would like to express my deepest appreciation to my main supervisor, Dr Mohammed Anbar, for his invaluable guidance, insightful suggestions, patience, and unwavering support throughout my journey at the Cybersecurity Research Centre. I am equally grateful to my co-supervisor, Dr Shankar Al Karuppayah, for his constructive comments and suggestions, which significantly contributed to the quality of this work. My heartfelt thanks go to my field supervisor, Dr. Basim Alabsi, for his steadfast support and advice, which were instrumental in successfully completing my Ph.D. I am profoundly indebted to my parents, whose prayers and unwavering belief in my potential have been the pillars of strength that enabled me to persevere and achieve this milestone. Their love and support, along with my brothers' and sisters' encouragement and guidance, have been my greatest source of inspiration. I also extend my heartfelt gratitude to my siblings, especially my sister, Dr. Nada Alfriehat, and Mr. Justice Fares Alfriehat, for their constant encouragement, support, and guidance throughout my PhD journey. Their love and belief in me have motivated and comforted me during challenging times.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
ADAN2_VN	Adaptive Dropout Artificial Neural Network for Version Number Attack Detection
ACC	Accuracy
AI	Artificial Intelligence
ANN	Artificial Neural Networks
CAGR	Compound Annual Growth Rate
Chi^2	Chi-Squared
DAG	Directed Acyclic Graph
DAO	Destination Advertisement Object
DDoS	Distributed Denial-of-Service
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DL	Deep Learning
DNN	Deep Neural Network
DNS	Domain Name System
DODAG	Destination-Oriented Directed Acyclic Graph
DR	Decrease Rank
DT	Decision Trees
FNN	Feedforward Neural Networks
FNR	False-Negative Rate
FPR	Low False-Positive Rate
GAN	Generative Adversarial Networks
HF	Hello Flood
ICT	Information Communication Technology

IDC	International Data Corporation
IDS	Intrusion Detection System
IETF	The Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IRAD	IDS for RPL Attacks Dataset
ITU	International Telecommunications Union
LLNs	Low-Power And Lossy Networks
MI	Mutual Information
ML	Machine Learning
MLP	Multi-Layer Perceptron
MP2P	Low Power Wireless Personal Area Networks
MRHOF	Minimum Rank With Hysteresis Objective Function
VNA	Version Number Attack
OF	Objective Function
P2MP	Multipoint-To-Point
P2P	Point-To-Multipoint
PRBA	Point-To-Point
RNN	Recurrent Neural Network
RPL	Routing Protocol For Low-Power And Lossy Networks
SH	Sink Hole
SVM	Support Vector Machine
VN	Version Number
VNA	Virtual Node Attack
NB	Naive Bayes
NN	Neural Networks

LIST OF APPENDICES

PENDEKATAN BERASASKAN RANGKAIAN NURAL TIRUAN ADAPTIF UNTUK MENGESAN SERANGAN NOMBOR VERSI DALAM RANGKAIAN IOT BERASASKAN RPL

ABSTRAK

Ekosistem Internet Benda (IoT) sedang mengalami pertumbuhan pesat luar biasa - mengakibatkan peningkatan data sensitif serta kebimbangan serius terhadap keselamatan, terutamanya pada lapisan rangkaian. Protokol Penghalaan untuk Rangkaian Berkuasa Rendah dan Mudah Terjejas (RPL) masih terdedah kepada pelbagai serangan, dengan serangan Nombor Versi (Version Number - VN) menjadi ancaman kritikal yang memanipulasi tingkah laku penghalaan melalui penyebaran maklumat palsu. Kajian ini memperkenalkan pendekatan berasaskan rangkaian neural tiruan dengan adaptive dropout, iaitu ADAN2_VN, bagi mengesan serangan VN dalam persekitaran IoT berasaskan RPL. Kerangka yang dicadangkan dibahagikan kepada empat fasa: (1) pengekstrakan ciri baharu menggunakan analisis statistik ke atas data trafik IoT; (2) prapemprosesan data yang merangkumi pembersihan, penyeimbangan, dan penormalan; (3) pemilihan ciri secara ansambel untuk mengenal pasti atribut yang paling signifikan; dan (4) pelaksanaan strategi adaptive dropout dalam rangkaian neural tiruan untuk meningkatkan prestasi pengesanan. Pendekatan ini telah diuji ke atas tiga set data: set data asal, set data yang dipertingkat dengan ciri tambahan, dan set data yang dipilih menggunakan kaedah ansambel. Dua senario eksperimen dijalankan dengan membandingkan strategi adaptive dropout dengan strategi dropout tetap yang dioptimumkan. Hasil kajian menunjukkan bahawa strategi dropout tetap memberikan prestasi yang lebih baik, dengan ketepatan pengesanan sebanyak 99.57%, skor F1 sebanyak 99.55%, ketepatan (precision) 99.12%,

kebolehkesanan (recall) 100%, AUC-ROC sebanyak 99.97%, dan Ralat Min Kuasa Dua (MSE) sebanyak 0.38%. Keputusan ini membuktikan bahawa gabungan pemilihan ciri ansambel dengan mekanisme dropout yang dioptimumkan dapat meningkatkan keupayaan pengesanan terhadap serangan VN secara signifikan.

AN ADAPTIVE DROPOUT ARTIFICIAL NEURAL NETWORK-BASED APPROACH FOR DETECTING VERSION NUMBER ATTACKS IN RPL-BASED IOT NETWORK

ABSTRACT

The Internet of Things (IoT) ecosystem is witnessing unprecedented growth, resulting in the proliferation of sensitive data and raising significant security concerns, particularly at the network layer. The Routing Protocol for Low-Power and Lossy Networks (RPL) remains vulnerable to various attacks, with the Version Number (VN) attack representing a critical threat that manipulates routing behaviour through falsified information dissemination. This study introduces an adaptive dropout artificial neural network-based approach, ADAN2_VN, for the detection of VN attacks in RPL-based IoT environments. The proposed framework is structured into four phases: (1) extraction of novel features using statistical analysis of IoT traffic data; (2) data preprocessing encompassing cleansing, balancing, and normalization; (3) ensemble feature selection to isolate the most significant attributes; and (4) implementation of an adaptive dropout strategy within an artificial neural network to enhance detection performance. The approach was evaluated on three datasets: the original dataset, an enhanced dataset with additional features, and an ensemble feature-selected dataset. Two experimental scenarios were conducted, comparing adaptive dropout with an optimally fixed dropout strategy. The results demonstrate that the fixed dropout approach achieved superior performance, attaining a detection accuracy of 99.57%, an F1 score of 99.55%, a precision of 99.12%, a recall of 100%, an AUC-ROC of 99.97%, and an MSE of 0.38%. These outcomes validate that the integration of ensemble feature selection with optimized dropout mechanisms significantly

enhances the detection capability against VN attacks. The findings affirm the achievement of the research objectives, offering a robust and scalable solution for securing RPL-based IoT networks against sophisticated threats.

.

CHAPTER 1

INTRODUCTION

1.1 Overview

The IoT is a buzzword that has gained popularity in recent years as it can potentially transform various aspects of our lives. IoT refers to the growing network of devices and objects connected to the internet, allowing them to collect and exchange data. This network includes smartphones, wearables, sensors, cameras, and other smart devices. The IoT encounters several constraints, such as limited processing power, low storage capacity, short battery life, and restricted transmission range. Therefore, the successful implementation of IoT heavily depends on leveraging the existing Internet Protocol (IP) infrastructure. This infrastructure optimizes readily available resources and benefits from the extensive address space provided by Internet Protocol Version 6 (IPv6) (Ghaleb et al., 2018).

The International Data Corporation (IDC) projects that by 2025, there will be 55.7 billion connected IoT devices. These devices are expected to generate 73.1 zettabytes of data by 2025, a significant increase from the 18.3 zettabytes generated in 2019 (Gaber et al., 2022). Despite increased IT spending on endpoint security, IDC reports that 70% of breaches originate at these points. Columbus (2020) also predicted that the global security market would grow from $167.1 billion in 2019 to $248.26 billion by 2023, with a Compound Annual Growth Rate (CAGR) of 10.4%.

The COVID-19 pandemic has further heightened security needs, as remote work has become widespread and a top priority for nearly every company. Statista (2021) also forecasted that end-user spending on IoT solutions would continue to rise steadily globally from 2017 to 2025, as illustrated in Figure 1.1. This increasing

investment underscores the growing reliance on IoT technologies and the critical need for robust security measures to protect these expanding networks.

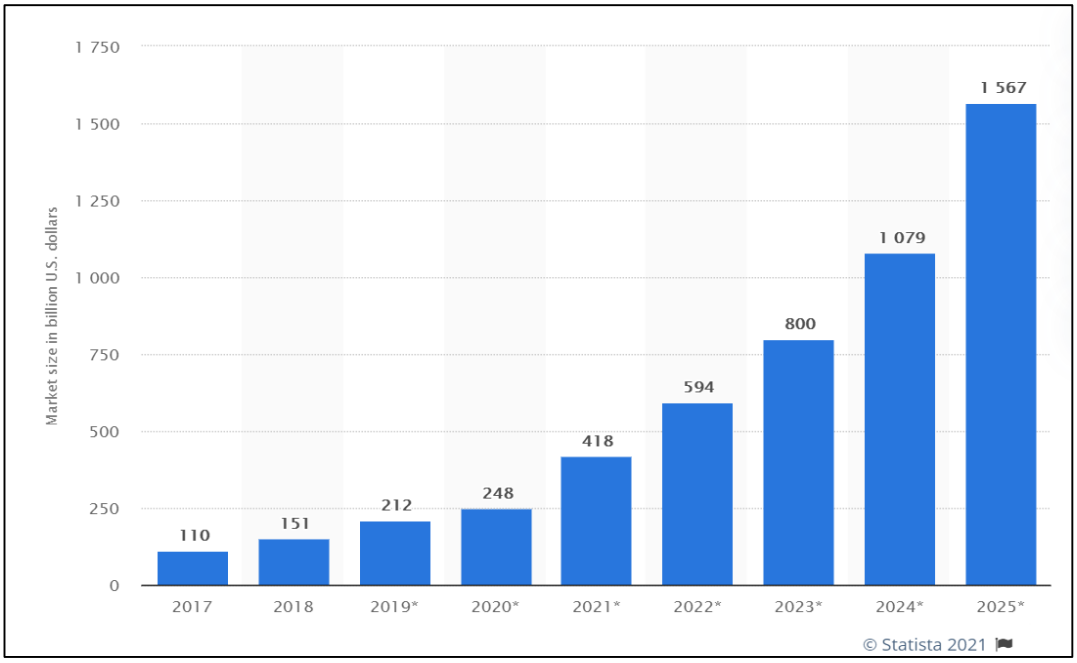

Figure 1.1 Forecast on Global Spending of End-Users on IoT (Statista, 2021)

IoT allows wearable devices, home appliances, and systems to exchange information in order to provide services to end users. Consequently, IoT enables billions of devices to exchange information and connect with services and people. Information security is a critical concern due to the substantial amount of personal and confidential information in shared data, and information security is a crucial concern that must be considered. Additionally, reused passwords easily compromise hardcoded credentials. The primary goal of IoT security is to maintain user confidentiality and privacy by ensuring device, data, and infrastructure security within the IoT ecosystem and guaranteeing service availability (Hassan et al., 2019; Zhang et al., 2014).

Among routing attacks, VN attacks are particularly insidious in IoT environments. These attacks can become even more destructive when combined with others, potentially causing significant harm. If a VN attack goes undetected, it may

lead to information loss and the failure of packets to be delivered to the base station, effectively disconnecting nodes from the internet. Furthermore, a VN attack increases network overhead and reduces the network's lifespan due to elevated energy consumption, ultimately leading to network destruction (An & Cho, 2022; Rehman et al., 2019; Rouissat et al., 2023). According to (Alsukayti & Singh, 2022), VN attacks are a common threat in IoT networks, where attackers manipulate the VN of the routing protocol, deceiving nodes into frequently updating their routes. This leads to increased network traffic and energy consumption, degrading the overall performance and security of the network.

1.1.1 Introduction

This section presents an introduction to the IoT, IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN), Low-power and lossy networks (LLNs), RPL, security issues, and different types of attacks that threaten IoT networks as shown in Sections 1.1.2, 1.1.3, 1.1.4,1.1.5, and 1.1.6, respectively.

1.1.2 IoT

IoT architecture comprises various internet-connected sensors and end devices, including smart cars, appliances, and homes. These devices are strategically placed and configured to communicate with users over the Internet through gateway nodes that receive and transmit data, as illustrated in Figure 1.2 (Pundir et al., 2020). The potentially unlimited address space of IPv6 enables billions or even trillions of these devices to be connected to the internet. The Internet Engineering Task Force (IETF) has introduced 6LoWPAN, extending the connectivity of intelligent devices and integrating IPv6 into Wireless Sensor Networks (WSN). 6LoWPAN utilizes the RPL

protocol to route data. However, RPL is vulnerable to various routing attacks, which can cause significant network damage (MelancyMascarenhas & PV Jain, 2018).

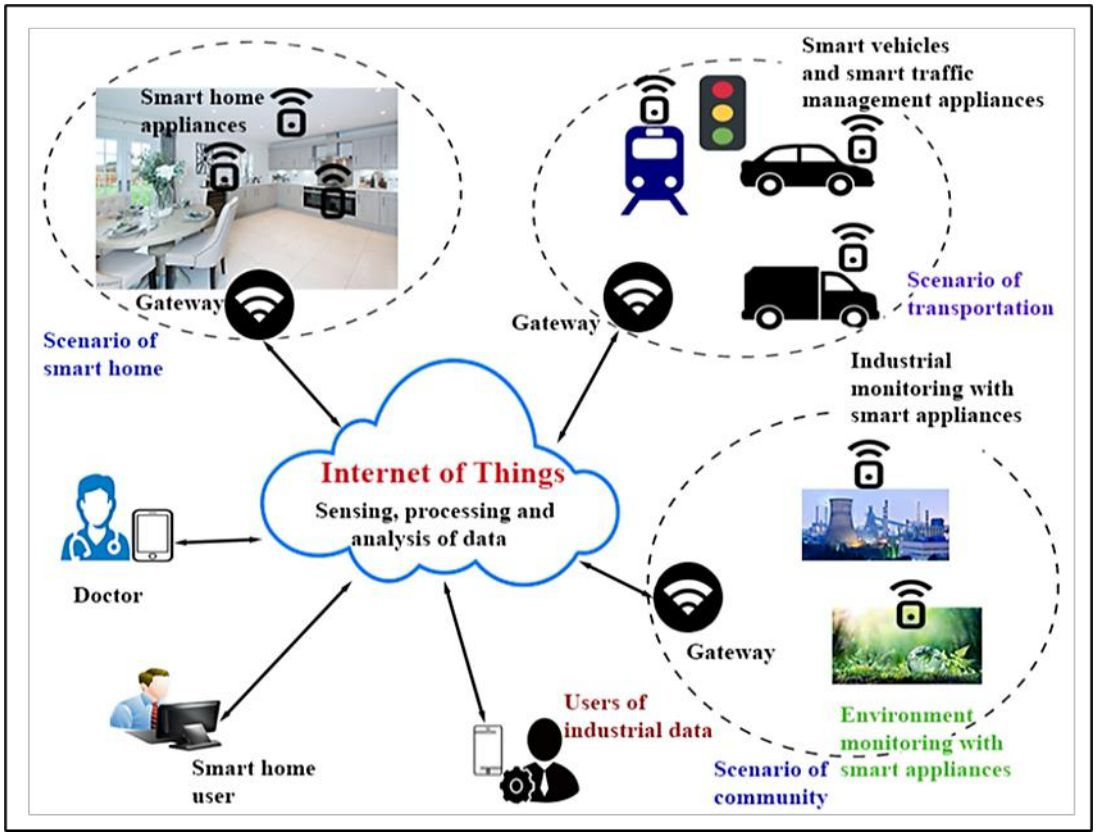

Figure 1.2 Generic IoT Architecture (Pundir et al., 2020)

1.1.3 6LoWPAN

The WSN is the heart of IoT technology because it allows various sensor applications to be integrated into intelligent ecosystems. The most challenging aspects of this system are power consumption, 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;

MelancyMascarenhas & PV 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).

1.1.4 LLN

Routers and devices in the LLN network operate under restrictions on their energy consumption, memory, and storage capacities. These networks are unstable, have insufficient data, and have high loss rates. Since most WSN devices are battery-powered, power consumption is a significant concern. LLNs have devised customized protocols for efficient traffic flow to circumvent these limits. WSNs commonly use 6LoWPAN as one of these protocols (Melancy Mascarenhas & PV Jain, 2018). Table 1.1 summarizes the general characteristics of IoT, LLN, 6LoWPAN, and WSN networks.

1.1.5 RPL

For LLNs, RPL is an IPv6 distance vector routing protocol. RPL is commonly chosen as it provides several benefits, such as moderate control overhead, IPv6 support, and efficient low-power operation (Baranyai, 2024; Violettas et al., 2021). The RPL protocol ensures no cycles are present in the network by building a Destination Oriented Directed Acyclic Graph (DODAG) routed at a single destination (Figure 1.3). An objective function (OF) constructs this graph. During network topology construction, the OF controls how routing functions and constraints are considered. RPL avoids routing loops by computing a specific node's position relative to other nodes, taking into account the DODAG root. The specific node's position is called its "rank," which increases with the node's position from the root and vice versa. As shown in Figure 1.3 (Liscio, 2016).

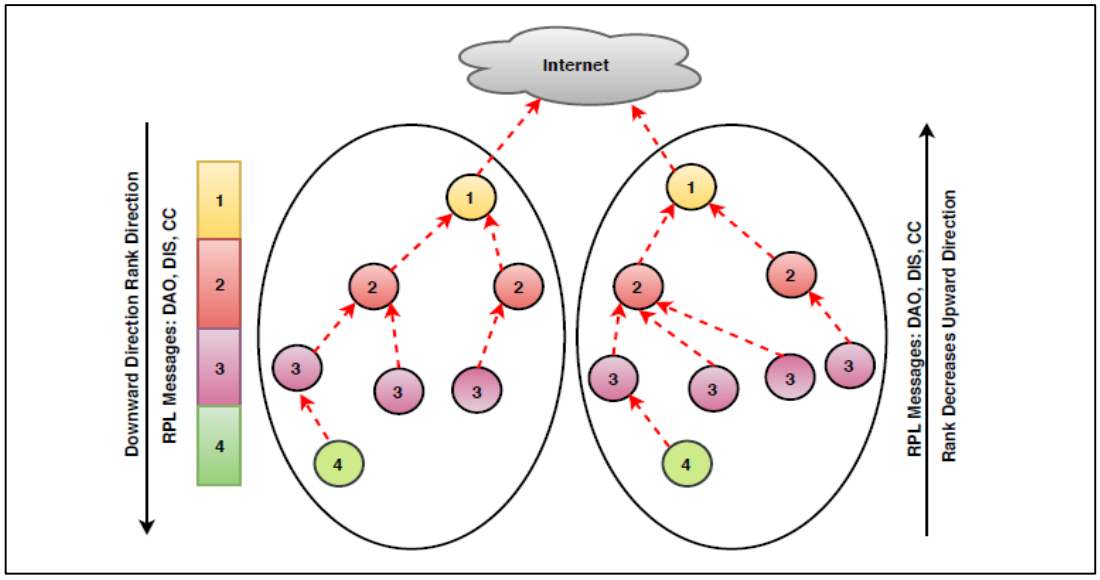

Figure 1.3 RPL Topology (Bhale et al., 2020)

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

Table 1.1 provides a general overview of the core network types and protocols that form the foundation for IoT environments where RPL is deployed. Understanding these network characteristics is crucial, as they influence the behavior and vulnerability of IoT systems, particularly in the context of security threats such as the VN attack addressed in this research.

Table 1.1 General Characteristics of IoT, WSN, LLN, and 6LoWPAN Networks

Feature	IoT	WSN	LLNs	6LoWPAN
Definition	Network of physical devices connected to the internet, enabling communication and data exchange	Networks of spatially distributed sensors to monitor and record environmental conditions.	Networks designed for devices with constraints on power, processing, and memory, operating in high packet loss environments	A communication protocol that enables IPv6 packets to be transmitted over IEEE 802.15.4-based networks.
Scope	Broad includes applications like smart homes, healthcare, industry, and more.	Mainly focused on environmental monitoring, military applications, and industrial sensing.	Broad concept encompassing any low-power and lossy network.	Specific protocol for transmitting IPv6 over low-power wireless networks.
Power Constraints	It generally depends on the application and device type.	Typically, it is very low to support long-term deployment of battery-operated sensors.	Devices are typically battery-operated, needing to conserve energy.	Supports low-power operation by integrating IPv6 with low-power wireless networks.
Scalability	It is highly scalable and can support a massive number of devices.	Limited scalability, primarily designed for localized sensor deployments.	It can support many devices over a wide area.	Ensures compatibility with existing IPv6 infrastructure, facilitating large-scale IoT deployment.
Functionality	Diverse functionality, including sensing, actuating, and data processing across various domains.	Focused on data collection, environmental monitoring, and reporting.	Focuses on the network characteristics and requirements, such as power efficiency and robustness to packet loss.	Provides a technical solution for fitting IPv6 packets into the frame size of IEEE 802.15.4.
Common Security Attacks	DoS attacks, data breaches, malware injection	Node capture, Sybil attack, sinkhole attack	Wormhole attack, selective forwarding	Replay attack, VN attack, sinkhole attack

1.1.6 RPL Security

The RPL protocol is susceptible to numerous vulnerabilities due to the characteristics of LoWPANs, such as low power consumption and the limited capabilities of the connected devices. In specific environments, 6LoWPAN-connected devices may sleep for extended periods to conserve energy, making them unable to communicate during these intervals. Furthermore, the expected deployment of many devices necessitates an extensive address space, which IPv6 efficiently manages. The RPL protocol has many features to ensure that data is safe, like local and global repair steps and ways to find and avoid routing loops (Arshad et al., 2020; Ech-Chaitami et al., 2011).

One of the critical vulnerabilities in RPL-based networks is the VN attack, which can severely disrupt the network topology (Nandhini et al., 2023). During a VN attack, a malicious node manipulates the VN in the RPL control messages, causing legitimate nodes to reset their routing tables and trigger unnecessary global repair processes. This increases overhead, network instability, and significant energy consumption as nodes repeatedly re-establish routes (Le et al., 2016; Hkiri et al., 2022). For instance, a VN attack can create routing loops or lead legitimate nodes to choose suboptimal paths, increasing latency and packet loss. The frequent reconfiguration of the network due to false VN increments also depletes the energy resources of nodes, particularly in energy-constrained environments, ultimately reducing the network's lifespan (Jamalipour et al., 2021).

The VN attack is therefore considered a serious weakness in RPL-based IoT networks, with problems such as network instability, energy depletion, and performance degradation being caused. Although several security measures have been

incorporated into RPL, major threats continue to be posed by VN attacks. Consequently, this research aims to develop a DL-based detection model utilizing adaptive dropout techniques to effectively detect and mitigate VN attacks, thereby improving the safety and resilience of IoT systems operating over RPL. To better understand the security threats facing RPL-based IoT networks, Table 1.2 summarizes the most common attack types, their impacts. It highlights the specific attack, VN Attack, that this research aims to detect and mitigate.

Table 1.2 Common Security Attacks in RPL-Based IoT Networks

Attack Type	Description	Impact	Focus of This Research
VN Attack	A malicious node manipulates the VN in control messages, forcing unnecessary network repairs.	Network instability, energy depletion, and packet loss	✓
Sinkhole (SH) Attack	A malicious node advertises a high-quality route to attract network traffic for interception or drop.	Data interception, routing disruption	✗
Wormhole (WH) Attack	Two malicious nodes create a low-latency link to disrupt normal routing paths.	Topology distortion, packet misrouting	✗
Selective Forwarding (SF)	A malicious node selectively drops packets instead of forwarding them.	Data loss, unreliable communication	✗
Hello Flood (HF) Attack	An attacker sends numerous hello messages to exhaust the resources of neighboring nodes.	Energy exhaustion, denial of service	✗

While the VN attack is briefly introduced in this chapter to highlight its importance, a more detailed and technical discussion of its mechanisms, impacts, and detection challenges is presented in Chapter 2, Section 2.4.4.

Various methods have been utilized for detecting VN attacks, ranging from rule-based and statistical approaches to ML and DL techniques. In particular, DL models have been increasingly adopted due to their ability to automatically learn complex attack patterns and anomalies within large-scale network traffic data without the need for extensive manual feature engineering. Recent advances in DL-based detection models have significantly enhanced the detection of VN attacks by providing a robust solution against malicious behaviors. A key innovation in these models is the application of dropout, a regularization technique by which a fraction of neurons is adaptively disabled during training to prevent overfitting and to enable better generalization to unseen data. In this research, an adaptive dropout-based DL detection model has been proposed to further address the challenges of overfitting and to improve the accuracy of VN attack detection in RPL-based IoT networks.

In the context of RPL-based networks, dropout has been shown to be particularly valuable, as it allows detection models to maintain high accuracy in distinguishing normal behavior from VN attack patterns across various deployment scenarios. Moreover, its adaptive application improves model robustness by adaptively adjusting the dropout rate based on data complexity. This enables the model to manage varying traffic conditions and energy constraints more effectively, making the detection process more reliable in constrained environments. As a result, IoT networks with limited power resources can be sustained longer without compromising security.

The practical importance of securing RPL-based IoT networks has also been demonstrated through real-world statistics and experimental testbeds. According to Unit 42 (Palo Alto Networks, 2020), approximately 98% of IoT device traffic remains unencrypted, leaving such networks highly vulnerable to routing-based attacks,

including the VN attack. Empirical results from real-world environments such as FIT IoT-LAB and RIOT OS have confirmed that minimal manipulation of VNs can cause substantial routing failures, increased latency, and rapid energy depletion. Studies such as those by Albishari et al. (2023) and Osman et al. (2021) have reported routing failure rates exceeding 50% in affected RPL scenarios.

To effectively mitigate such threats, the use of DL models with appropriate feature selection mechanisms has become essential. Feature selection has been shown to significantly enhance detection accuracy and reduce computational complexity. Retaining only statistically and structurally relevant features ensures the model remains efficient and accurate, particularly in resource-constrained IoT environments. As such, the proposed approach in this research integrates adaptive dropout regularization with a multi-phase feature engineering pipeline to maximize the system's reliability in detecting VN attacks.

1.2 Research Motivation

Technology has become an essential component of human existence, and one of the most groundbreaking technologies is the IoT. Given the interconnected nature of many things, the possibility of security breaches exists. Deploying billions of IoT devices will give rise to significant challenges in administration, scalability, reliability, availability, and security (Mayzaud et al., 2016). Therefore, researchers need to prioritise protecting networks and systems from weaknesses and bugs. This is especially important for protecting against the biggest threats to IoT that aim to slow down networks, drain device batteries, fill up storage space, and cause packet loss and delay (Ganchev et al., 2018).

The RPL protocol, commonly employed in 6LoWPAN for facilitating IoT networks, is prone to several vulnerabilities, with VN attacks being of particular concern. VN attacks take advantage of the lack of methods to guarantee the accuracy of the stated VN in RPL control messages. This vulnerability can potentially cause forced network rebuilds, higher overhead, exhaustion of energy reserves, and routing topology loops, significantly impairing the network's overall performance. Significant deficiencies and gaps remain unaddressed despite previous studies examining RPL network security. Further research is needed to develop effective strategies for safeguarding RPL networks against VN attacks and enhancing their security.

Intrinsic weaknesses in routing protocols expose IoT networks to several risks, including Sybil, SH, blackhole (BH), and HF attacks. Combining these threats intensifies their gravity, making VN attacks a crucial area of concern. For example, an SH attack can deplete the energy of nearby nodes, and when combined with VN attacks, the resultant network instability might have disastrous consequences. Statista (2020) reports that routing protocol and attacks account for 20% of worldwide risks, which is projected to increase to 23% by 2021. Compromised IoT devices comprise 13% of global threats, with a projected increase to 21% by 2021.

Statista (2021) projects that worldwide spending on IoT security will reach $36.6 billion by 2025. This increase is mainly due to the rise in ransomware attacks, concerns about the security of vital infrastructure, data-related risks in IoT networks, and the implementation of stricter IoT security rules. In the first half of 2018, Kaspersky Lab documented more than 120,000 instances of malicious software assaults on IoT devices, which is three times the number recorded in 2017. According to IBM, there was a fourfold rise in the number of combined assaults on IoT devices

between October 2019 and June 2020 compared to the preceding two years (IBM, 2021).

With the growing number of IoT devices and the increased security risks, it is critical to understand and address VN attacks to maintain the reliability and efficiency of RPL-based networks. To overcome these issues, it is necessary to conduct new research and implement robust security measures to protect IoT infrastructures from ever-changing cyber threats. The IoT Attack Volume between 2018 and 2020, as illustrated in Figure 1.4 (IBM, 2021), highlights the significant rise in cyberattacks targeting IoT devices over this period. This trend underscores the growing vulnerability of IoT networks and the increasing sophistication of attack methods, emphasizing the urgent need for robust security solutions in these environments.

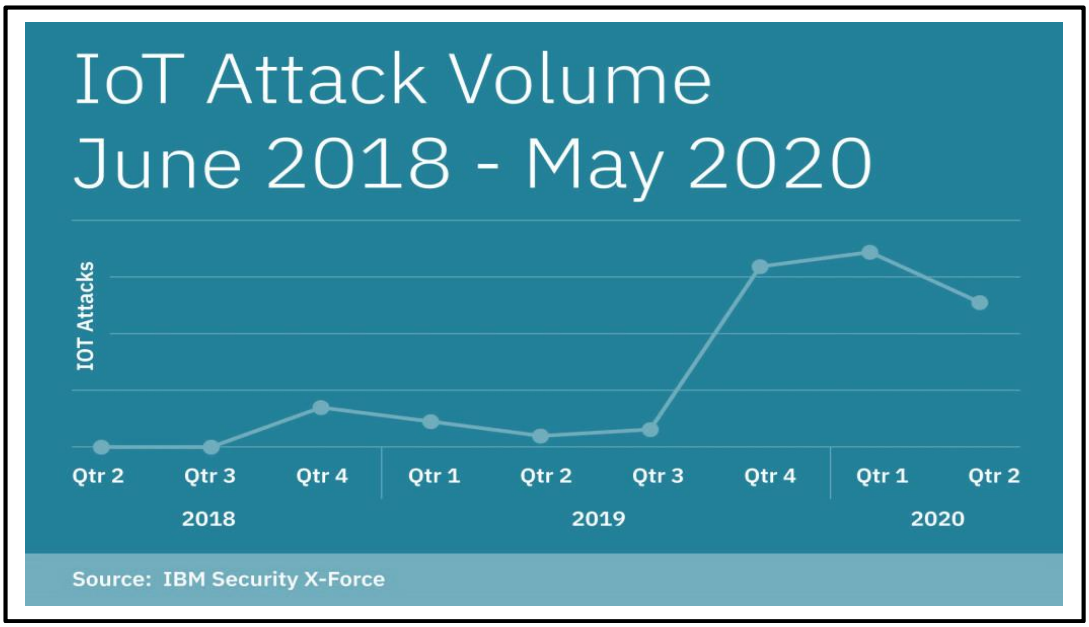

Figure 1.4 IoT Attack Volume between 2018 and 2020 (IBM, 2021)

Undetected attacks can have severe repercussions, potentially affecting millions of internet-connected devices and numerous applications and services that rely on RPL protocol sensors. Such attacks can lead to information loss and endanger

human lives in the worst-case scenario. For instance, if an intelligent medical device monitoring a patient's heart rate is disconnected from the internet due to an attack on the RPL protocol, the heart monitor's data cannot reach the hospital's monitoring system.

This disconnect prevents the patient from receiving timely medical attention in an emergency. Additionally, attacks on hospitals can result in fatalities due to service disruptions. For example, in September 2020, a hospital in Germany experienced a DoS attack, leading to the death of a patient after health services were halted due to the attack (Jalali et al., 2021).

1.3 Problem Statement

The IoT connects heterogeneous devices, enabling data transfer over a network without requiring human-to-human or human-to-computer interaction. These devices are often deployed in open environments but face significant constraints due to their limited power, storage, and energy capacities. As a result of these limitations, IoT devices are vulnerable to various routing attacks. Existing security solutions have not been adequate, leaving nodes exposed to compromise. Attackers can capture sensor nodes and gain access to critical information, data, and code stored on these previously legitimate network members (Stephen & Arockiam, 2021).

Given the constrained nature of RPL, the IoT network is susceptible to several types of attacks, with one of the most critical being the VN attack. In a VN attack, a malicious node manipulates the VN field in RPL control messages, causing legitimate nodes to reset their routing tables and initiate unnecessary global repairs. This disruption results in misleading routing information, increased control message overhead, energy depletion, and routing loops, ultimately leading to continuous

reconfiguration of the network. This can create energy gaps, significantly reducing the overall efficiency and lifespan of the IoT network (Gill et al., 2024; Ghadi et al., 2024; Rehman et al., 2019). Consequently, researchers have proposed several approaches to detect and mitigate VN attacks in RPL networks.

However, previous studies addressing VN attacks in RPL-based IoT networks, such as (Nayak et al., 2021; Albishari et al., 2023), have exposed significant security issues and limitations. These approaches often fail to detect VN attacks accurately due to inadequate representation of key network behaviors and limitations in the features selected for detection. These shortcomings result in poor detection accuracy, higher false alarm rates, and unreliable generalization across different network environments.

DL-based approaches have been widely regarded as among the most efficient for detecting VN attacks. Nevertheless, DL models face significant challenges, including overfitting and data loss during the training process, which hampers their robustness in online detection of VN attacks. These challenges often arise from the use of default hyperparameters, particularly the Dropout parameter, which is typically not optimized for specific use cases. Furthermore, traditional feature selection mechanisms such as Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE) fail to identify the most critical features for characterizing VN attacks.

Additionally, existing research works such as (Nayak et al., 2021; Albishari et al., 2023) rely on default feature sets that represent the dataset used for evaluation. These features, typically based on simple heuristics like packet size, hop count, or message frequency, do not fully capture the complex behaviors associated with VN attacks. The use of inappropriate features leads to inefficiencies in the detection

process, making it difficult to differentiate between normal network activity and malicious behavior.

These weaknesses highlight the need for further research to develop more effective mechanisms for detecting VN attacks, improving network security (Almusaylim et al., 2020), and addressing the existing limitations. To this end, it is essential to propose a robust intrusion detection system (IDS) that enhances detection accuracy, reduces the false alarm rate, and increases key performance metrics such as the F1 measure for VN attack detection.

The statement of the problem is summarized as follows:

i) Existing DL based approaches for detecting VN attacks lack comprehensive features that reflect the characteristics of VN attacks.

ii) Existing feature selection mechanisms fail to prioritize the most relevant features, reducing the overall detection efficiency.

iii) The existing DL-based approaches still suffer from significant challenges, including data loss and overfitting, which negatively impact their performance

1.4 Research Objectives

The main goal of this research is to propose an adaptive dropout artificial neural network-based approach for detecting VN attacks in RPL-based IoT networks with enhanced accuracy. The following objectives are set to achieve the primary goal of this research:

1.4.1 Objectives 1

To design and evaluate a new set of statistical and behavioral features that contribute to the accurate detection of VN attacks in RPL-based IoT environments.

1.4.2 Objectives 2

To implement an ensemble-based conditional intersection feature selection mechanism that effectively identifies and reduces features, while retaining only the most relevant characteristics associated with VN attack behavior.

1.4.3 Objectives 3

To develop and validate a neural network model with adaptive dropout in order to enhance generalization and robustness in detecting VN attacks under varying network conditions.

1.4.4 Alignment Between Problem Statements and Objectives

To ensure clarity and alignment, each research objective was explicitly formulated to address a specific issue outlined in the problem statements. The connections between these elements were carefully established and are presented in Table 1.3. This alignment was intended to ensure that all research activities remain focused on solving the core challenges identified at the outset of the study.

Table 1.3 Mapping of Problem Statements to Research Objectives

Objective	Problem Statement
Objective 1: A new set of statistical and behavioral features was designed and evaluated to improve VN attack detection.	1. DL-based approaches lack comprehensive features to reflect VN attack characteristics.
Objective 2: An ensemble-based conditional intersection feature selection approach was implemented to retain key features.	2. Feature selection methods fail to prioritize relevant features, lowering detection efficiency.
Objective 3: An adaptive dropout neural network model was developed and validated to improve performance and generalization.	3. DL models suffer from overfitting and data loss, reducing model robustness and generalization.

1.5 Research Scope

This thesis proposes an approach to detect VN attacks in RPL-based IoT networks using an adaptive artificial neural network with enhanced detection accuracy. The proposed approach involves training ANNs to analyze network behaviour and identify anomalies associated with VN discrepancies in RPL control messages. This research leverages the capabilities of ANNs, known for their ability to handle complex patterns and large datasets effectively (Kumar et al., 2024; Mallaradhya & Babu, 2024). Table 1.4 illustrates the scope of this thesis, highlighting the utilized concepts and their relationships in detecting VN attacks in RPL networks.

Table 1.4 Research Scope

Items	Scope of Research
Environment	IoT
Attack Type	VN attack
Target Layer	Network layer
Performance metrics	Accuracy, Training Accuracy, Validation Accuracy, F1 Score, Mean Squared Error, Area Under Curve, precision, recall, Mean absolute error, prediction time, Loss
Detection Approach	Anomaly-based Approach
Routing Protocol	RPL
Dataset	IRAD dataset

1.6 Research Contribution

The main contribution of this research is a high-level approach for detecting VN attacks in RPL-based IoT networks with high accuracy and efficiency, utilizing adaptive dropout in ANNs. The ANN-based model is optimized to analyze network behaviour and identify anomalies associated with VN discrepancies in RPL control messages without significantly impacting the power resources of other nodes in the network. Additionally, the proposed approach includes mechanisms to ensure reliable network operation even when jamming attacks target IoT node communication channels. This research makes the following key contributions:

i) New Feature Set for VN Attack Detection: This research proposed and validated a new set of features specifically designed to capture the unique characteristics of VN attacks in RPL networks. This feature set is critical in improving detection accuracy by better identifying attack patterns and behaviours.

ii) An ensemble feature selection mechanism enables identifying and prioritising the most relevant features for detecting VN attacks. This

reduces the dataset's dimensionality and improves the detection model's effectiveness by focusing on the features that contribute the most to accurate attack detection.

iii) A new dropout adaptive mechanism for the ANN detection model of VN attacks. This mechanism adaptively adjusts the dropout rates in the neural network, improving detection accuracy and identifying the optimal dropout value at which the model performs best. This optimal dropout value enhances the model's ability to effectively detect VN attacks while preventing overfitting in the DL model used for VN attack detection. Furthermore, the dropout mechanism ensures the model generalizes better across various attack scenarios, achieving a higher detection accuracy and robustness.

In conclusion, this research significantly contributes to IoT security by proposing a novel and efficient solution for VN attack detection. Adding a new feature set, advanced feature selection techniques, and adaptive dropout makes this method a perfect and expandable way to protect RPL-based IoT networks.

1.7 Research Steps

The following steps are followed while conducting this research:

First Step - Literature Review. This step presents the background of IoT, 6LoWPAN, LLNs and RPL. It also studies the accuracy of the existing related work to detect VN 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 to adaptive artificial neural network algorithms for VN attack detection based on dropout adaptive selection (ADAN2_VN) 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 behavioural 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.

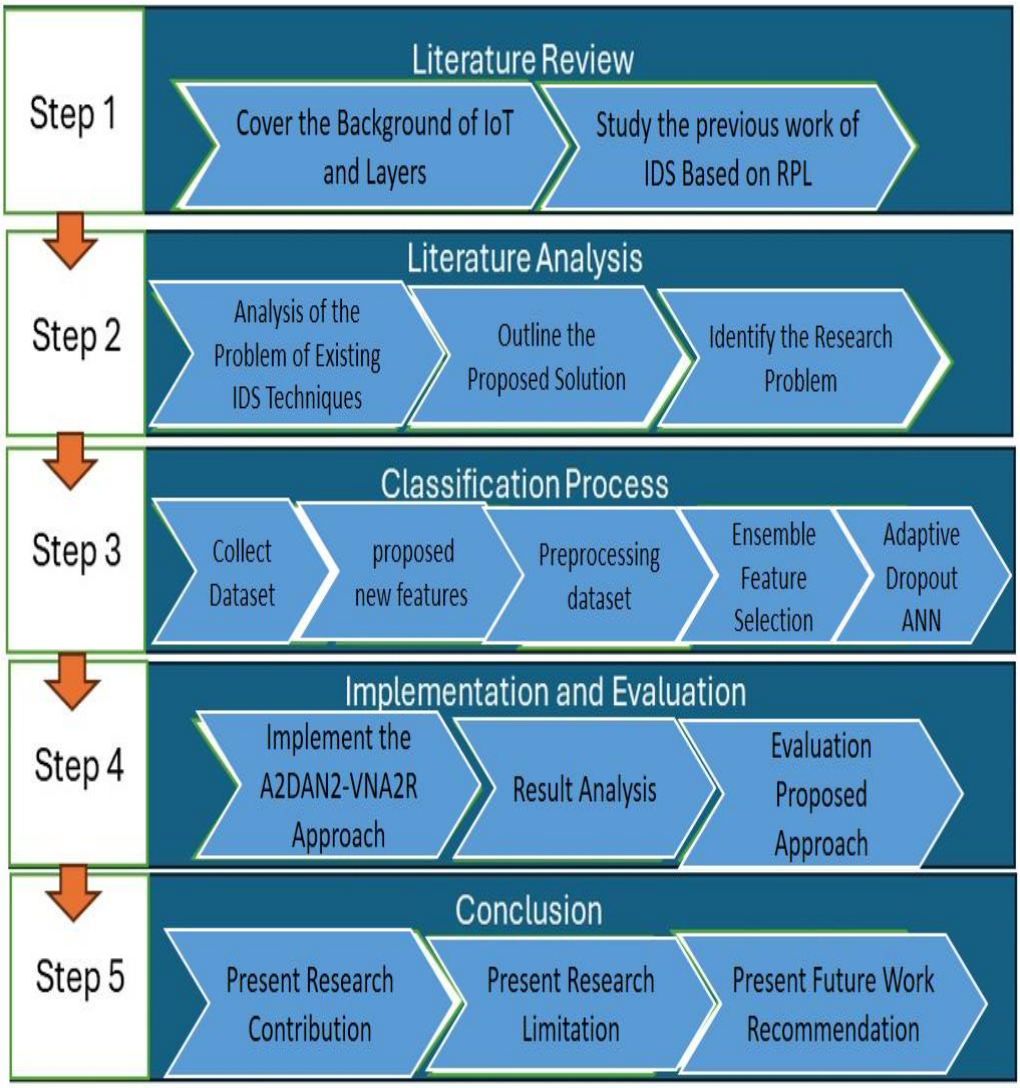

Figure 1.5 Research Steps

1.8 Thesis Organization

This thesis comprises six chapters, as follows:

Chapter 2 provides background information for understanding the work, including an overview of IPv6, 6LoWPAN, LLN, RPL networks, limiting factors, IoT attacks, a 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 VN attacks in RPL-based networks.

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

Chapter 5 describes the threshold values and the topology of the proposed ANN-based approach for detecting VN attacks in RPL-based IoT networks. Additionally, it details the ground truth test scenarios and evaluation methods used to assess the proposed approach's detection accuracy and F1 score accuracy. Finally, it compares the results of the ANN-based approach with those of existing detection methods to highlight its effectiveness, accuracy, and power efficiency improvements.

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 VN 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 VN attacks in the RPL-based network and various detection classifications according to the different approaches.

The organization of this chapter is structured as follows: Section 2.2 presents an overview of IPv6 and LLN. Sections 2.3 and 2.4 provide a comprehensive background on RPL, including its security challenges and the classification of IDS for RPL. The feature selection techniques are explored in Section 2.5. Sections 2.6 and 2.7 examine related works in VN attack detection within RPL networks, specifically for IoT environments, and follow a critical review of the problem of existing approaches. Finally, Section 2.8 concludes the chapter with a summary of the key points.

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.