Designing a Secure Communication Protocol in IoT Enabled ZigBee Networks using Blockchain System

Submitted in partial fulfillment of the requirements

for the award of the degree of

DOCTOR OF PHILOSOPHY

Submitted by

Bhukya Padma

(Roll No. 719135)

Under the guidance of

Dr. E. Suresh Babu

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL

TELANGANA - 506004, INDIA

August 2023

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL
TELANGANA - 506004, INDIA

THESIS APPROVAL FOR Ph.D.

This is to certify that the thesis entitled, Designing a Secure Communication Protocol in IoT Enabled ZigBee Networks using Blockchain System, submitted by Ms. Bhukya Padma [Roll No. 719135] is approved for the degree of DOCTOR OF PHILOSOPHY at National Institute of Technology Warangal.

Examiner

Research Supervisor
Dr. E. Suresh Babu
Dept. of Computer Science and Engg.
NIT Warangal
India

Chairman
Prof.S.G. Sanjeevi
Dept. of Computer Science and Engg.
NIT Warangal
India

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL
TELANGANA - 506004, INDIA

CERTIFICATE

This is to certify that the thesis entitled, Designing a Secure Communication Protocol in IoT Enabled ZigBee Networks using Blockchain System, submitted in partial fulfillment of requirement for the award of degree of DOCTOR OF PHILOSOPHY to National Institute of Technology Warangal, is a bonafide research work done by Ms. Bhukya Padma(Roll No. 719135) under my supervision. The contents of the thesis have not been submitted elsewhere for the award of any degree.

Research Supervisor
Dr. E. Suresh Babu
Assistant Professor
Dept. of CSE
NIT Warangal
India

Place: NIT Warangal
Date: 02 August, 2023

DECLARATION

This is to certify that the work presented in the thesis entitled "*Designing a Secure Communication Protocol in IoT Enabled ZigBee Networks using Blockchain System*" is a bonafide work done by me under the supervision of Dr. E. Suresh Babu and was not submitted elsewhere for the award of any degree.

I declare that this written submission represents my ideas in my own words and where others ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/date/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Bhukya Padma
(Roll No. 719135)
Date: 02-08-2023

ACKNOWLEDGMENTS

It is with great pleasure that I acknowledge my sincere thanks and deep sense of gratitude to my supervisor Dr. E. Suresh Babu Assistant Professor, Dept. of CSE for his invaluable guidance to complete the work. He always gave me ample time for discussions, reviewing my work and suggesting requisite corrections, which enabled me to attain my objective in time. He has provided me all kinds of inputs directly with his words, indirectly with his values not only to be a good teacher also to be a good human being. His sincerity and commitment to every aspect of the life has influenced me greatly. He always gave me ample time for discussions, reviewing my work and suggesting requisite corrections. I want to inculcate all the great qualities of him for the rest of my life.

I extend my gratitude to all my Doctoral Scrutiny Committee members Prof. S. G. Sanjeevi, Dr. S Ravi Chandra, Dr. P. Venkata Subba Reddy and Dr. Y Sreenivasa rao for their insightful comments and suggestions during oral presentations. I am lucky to attend lectures by Dr. E. Suresh Babu, Dr. M. Sandhya, and Dr. T. Ramakrishnudu during my tenure. I am immensely thankful to Dr. Raju Bhukya, Dr. Ramalingaswamy Cheruku, Prof. P. Radha Krishna and Dr. Padmavathy, Head of Dept. of CSE during my stay in the department, for providing adequate facilities. I wish to express my thanks to faculty members of Computer Science and Engineering department. I also express my thanks to Prof. Bidyadhar Subudhi, Director, NIT Warangal for his official support and encouragement.

My gratitude to Benerji Babu A, Department of Mathematics their support during the difficult situations of my Ph.D journey. I am also thankful to Dr. Sadanadam sir from Kakatiya University for their presence with valuable suggestions during my M.tech.

I wish to express my thanks to Aguru Aswani Devi for their inputs and help during my Ph.D duration. I would also like to thank my seniors Chandra Mohan Dasari, Amilpur Santhosh, Satish Vemireddy, B. Uma Maheswara Sharma and Sanjib Kumar Raul for their valuable suggestions and for extending selfless cooperation. In addition, I want to express my gratefulness to my friend Nishaad Shireen for her continuous encouragement. Special thanks to Aguru Aswani Devi for patiently helping me to present the thesis in the current

form.

I am eternally thankful to the following people who have shaped my career with some key advices.

My parents have made so many sacrifices in their life by having a deep trust in me to see where I am today. Even in the most difficult financial situations at home, they backed me in pursuing higher studies and further in choosing teaching as a profession. My brothers, sisters and who always wish for my best, to make better decisions whenever I am at crossroads of my life. Special heartfelt gratitude to my brother Dr. Raju Bhukya for his support, to whom I am indebted for his encouragement, motivation and support since my childhood. He played a pivotal role in shaping my research journey. The smiles of my nephew Akshay and niece Bhavya have made my days joyful. In addition, I want to express my thanks to my brothers Haridas Bhukya, Ramesh Bhukya and my sister Soujanya for their moral support during my hard times.

Above all I would like to thank my dearest mentor, admirer and husband-to-be, Mr. Prathap Badavath for his continuous support and contribution. Lastly, my deep sense of gratitude to Lord Shiva and Lord Krishna for all the things that come into my life.

Bhukya Padma

Dedicated to

My Family & Teachers

ABSTRACT

The Internet of Things (IoT) is a key technology integrator in Industry 4.0, contributing to the pervasive deployment of low-power IoT networks. These IoT networks gained popularity due to their numerous advantages, which include increased productivity and a higher standard of living. Mobile devices have significantly increased over time, and numerous IoT standards have been developed in response to the constant development of IoT technologies and the growing demand. Few prevalent IoT technologies, such as ZigBee, BLE, and LoRa standards, have a substantial user base due to their lightweight properties, such as low power operation, robustness, and greater scalability. ZigBee is the dominant IoT technology that enables intelligent applications and services. However, this technology creates personal area networks that cannot communicate directly with Internet end users. The IoT-enabled ZigBee devices cannot handle the IPv6 packets, which have a maximum packet size of 1280 bytes, and the transmission of IPv6 packets over ZigBee-based IEEE 802.15.4 networks, which will be performed using a gateway via the ZigBee coordinator. Gateways and the ZigBee coordinator must complete the neighbor discovery procedure, which increases the complexity of the coordinator. ZigBee devices have issues with header size, routing structures, and data forwarding. In addition, the number of malware attacks (Internet of Threats) has increased as the number of smart devices and mobility has increased in an IoT ecosystem. Therefore, security is paramount, and IoT security is always challenging.

In this thesis, we suggested a 6LoWPAN-based, effective end-to-end communication protocol for "IoT-enabled ZigBee devices" and an Internet host. By establishing end-to-end communication between ZigBee devices and IP-based infrastructures, this 6LoWPAN routes IPv6 packets into ZigBee networks that support the Internet of Things. AODV and RPL routing protocols are currently the only two standardized protocols that efficiently use smart devices energy and compute resources to resolve the properties and constraints of ZigBee and IoT networks. We proposed the RPL-AODV routing protocol which combines the advantages of both routing protocols RPL and AODV. The proposed protocol have a ability to forward or route data packets from a ZigBee device to a 6LoWPAN Boarder

Router (6BR) via multiple hops. It incorporates the benefits of RPL and AODV routing protocols in ZigBee devices of IoT networks to establish the path from the source node to the destination node on demand. Furthermore, we evaluated this protocol's efficacy using various metrics and found that its results were superior to those of existing protocols.

In addition, we have modeled collaborative attacks against the RPL-AODV routing protocol that exploit the vulnerability of these routing protocols. The collaborative attacks, such as wormhole and blackhole attacks, will control the AODV protocol's vulnerability, while rank and sinkhole attacks will exploit the RPL protocol's vulnerability. The proposed cooperative IDS effectively monitors and secures IoT-enabled ZigBee networks by combining "specification-based" and "signature-based IDS" to detect cooperative attacks against the RPL-AODV routing protocol.

We provided efficient key management solutions investigating the distribution of security key problems among smart IoT devices using a permissioned blockchain system. This system makes it possible to create end-to-end application keys, join a network securely, distribute keys across the entire network, update network keys, control network access, authenticate routers and end IoT devices, and store key credentials with a reputable security service provider. Finally, we implemented, validated, and demonstrated the efficacy of the proposed methods for securing IoT-enabled ZigBee networks by comparing them to the current state of the art.

Keywords: ZigBee, RPL-AODV protocol, Internet of Things, Security, Attacks, and Blockchain.

Contents

ACKNOWLEDGMENTS i

ABSTRACT iv

List of Figures v

List of Tables vii

List of Symbols viii

1 Introduction 1

1.1 Research Motivation 4

1.2 Limitations and Challenging Issues 5

1.3 Problem Statement 7

1.4 Research Contributions 7

1.4.1 RO-1: To communicate with IoT-enabled ZigBee devices with IPv6 using 6LoWPAN protocol. 7

1.4.2 RO-2: To detect collaborative attacks against the RPL-AODV routing protocol using the cooperative IDS mechanism in IoT-enabled ZigBee Network. 9

1.4.3 RO-3: To design a trust-based Blockchain system to distribute keys among IoT-enabled ZigBee devices. 10

1.5 Technical Background 11

1.5.1 Overview of IoT Networks: 11

1.5.2 Overview of ZigBeeTechnology 19

1.5.2.1 ZigBee Applications: 20
1.5.3 Overview of Blockchain Technology 21
1.5.4 Role of Blockchain in IoT-Enabled ZigBee Networks 23
1.6 Organization of the Thesis 24

2 Related Work **25**
2.1 State-of-the-art work on IoT-enabled ZigBee devices: 25
2.2 State-of-the-Art Work on Routing Protocol in an IoT-enabled ZigBee Network: 29
2.3 State-of-the-art work on IoT-enabled ZigBee Network Security: 32

3 End-To-End Communication Protocol in IoT-enabled ZigBee Network: Investigation and Performance Analysis **38**
3.1 Existing ZigBee Architecture 39
3.1.1 Overview of 802.15.4 standard 39
3.1.1.1 802.15.4 Standard PHY: 40
3.1.1.2 802.15.4 Standard MAC: 41
3.1.2 Mesh Topology in ZigBee Network: 42
3.1.2.1 ZigBee Device Types: 42
3.2 Limitations of ZigBeeNetwork 44
3.3 Proposed Work 45
3.3.1 Protocol Architecture of IoT-enabled ZigBee Networks. . . . 47
3.3.2 Integrating the Network Adaptation Layer in the IoT-enabled ZigBee Environment. 51
3.3.2.1 Header Compression of IoT-enabled ZigBee Packet Header 52
3.3.2.2 Fragmentation and Reassembly in IoT-enabled ZigBee Network 54
3.3.3 Integrating the RPL-AODV Routing Protocol into an IoT-enabled ZigBee Network. 56
3.3.3.1 Overview of RPL-AODV Routing Protocol: 56

3.3.3.2 Modeling of RPL-AODV Routing Protocol for IoT Enabled ZigBee Networks (IEZN): 58
3.3.3.3 Mathematical Formulation 61
3.4 Results and Performance Analysis 63
3.4.1 Hardware setup 63
3.4.2 Performance Analysis 65
3.5 Summary of the Chapter 70

4 Cooperative IDS Mechanism to Detect Collaborative Attacks against RPL-AODV Routing Protocol in the IoT-Enabled ZigBee Networks 72
4.1 Challenging Issues 73
4.2 Modeling of Collaborative Attacks against the RPL-AODV Routing Protocol 74
4.2.1 Wormhole and Blackhole Attacks Against AODV Routing Protocol 75
4.2.2 Rank Attack and Sinkhole Attack Against RPL Routing Protocol 76
4.3 Detection of Collaborative Attacks against RPL-AODV Using Hybrid-Based Intrusion Detection System 77
4.3.1 Hybrid-Based Intrusion Detection System Using Ensemble Machine Learning Approach: 80
4.4 Results and Performance Evaluation 82
4.4.1 Performance Analysis 82
4.5 Summary of the Chapter 90

5 Keys Distribution among End Devices Using Trust-Based Blockchain System for Securing IoT-Enabled ZigBee Networks 91
5.1 Challenging Issues of IoT-Enabled ZigBee Networks 92
5.2 Preliminaries and Basic Building Blocks 93
5.2.1 Review of ZigBee IP Protocol Stack Architecture 93
5.2.2 Cryptographic Primitives Used in Proposed Work 95

5.2.2.1 ECDSA Signature Scheme: 96
5.3 Trust-based Permissioned Blockchain System pBCS to Distribute Keys across IoT-enabled ZigBee Devices 97
5.3.1 ZigBee IP Protocol Stack Security Architecture 100
5.3.2 Registration Phase: IoT-enabled ZigBee devices in pBCS Network 105
5.3.2.1 Joining a Secured Blockchain Network. 106
5.3.3 Authentication and Secure Key Exchange Protocol 108
5.3.4 Keys Updation: 109
5.3.5 Implementation and Performance Analysis 109
5.3.6 Performance Evaluation 116
5.4 Security Analysis 118
5.5 Summary of the Chapter 120

6 Conclusion and Future Scope **121**

Bibliography **123**

List of Publications **134**

List of Figures

1.1 Challenging Issues in the Existing Mode 5
1.2 IoT Architecture 14

3.1 ZigBee Stack Architecture 40
3.2 Frame format of IEEE802.15.4. 41
3.3 ZigBee network: Mesh topology. 43
3.4 ZigBee Network using Traditional Gateway Approach. 44
3.5 6LoWPAN Layer in IoT layered Architecture. 45
3.6 Protocol Architecture of IoT-enabled ZigBee Networks 46
3.7 Interfacing 6LoWPAN in IoT-enabled ZigBee Network. 48
3.8 Adaptation 6LoWPAN layer Functionalities 50
3.9 6LoWPAN Header Compression 52
3.10 6LoWPAN Fragmentation Header 55
3.11 6LoWPAN Mesh Header 56
3.12 RPL-AODV Protocol into Routing Layer on ZigBee 57
3.13 Symmetric and Asymmetric Paired Instances in RPL-AODV Protocol . . . 58
3.14 Packet Format of DIO RREQ Instance option 59
3.15 Format of DIO RREP option 60
3.16 Hardware Setup for Performance Evaluation using Raspberry Pi 66
3.17 Evaluation of proposed framework based on key performance metrics. . . . 68
3.18 Evaluation of Proposed Framework based on Key Performance Metrics . . . 69

4.1 Collaborative attacks against RPL-AODV routing protocol 75
4.2 figure-Based Intrusion Detection System against RPL-AODV Protocol . . . 78
4.3 Ensemble Machine Learning Technique 81

4.4 Visualization of Communication Among devices ZigBeeNetwork 85
4.5 Proportion of Normal and Attack data records for training the proposed framework 88

5.1 ZigBee IP Protocol Stack Architecture 94
5.2 Proposed Architecture of Permissioned Blockchain System pBCS 99
5.3 ZigBee IP Protocol Stack Security Architecture 100
5.4 Proposed ZigBee IP Protocol Stack Security with Attack Landscape 103
5.5 Node Joining Procedure in a Secured Blockchain Network 106
5.6 Using the APUF and Blockchain systems, a secure key exchange protocol . 108
5.7 Registration request and key pair generation 110
5.8 Confirmation messages 111
5.9 Block creation and secure communication 113
5.10 Ipv6 enabled ZigBee Network creation 114
5.11 Visualization of Communication among devices ZigBee Network 115
5.12 Performance analysis of Blockchain based Keys Distribution 117

List of Tables

2.1 Comparative Analysis of State-of-the-art work on IoT enabled ZigBee Networks . . . 28

2.2 Summary of the routing protocol and security issues on IoT-enabled ZigBee networks. . . . 33

2.3 Comparative Analysis of existing solutions . . . 36

2.4 Summary of the routing protocol and security issues on IoT-enabled ZigBee networks. . . . 37

3.1 NS-3 Simulation Parameters . . . 64

4.1 NS-3 Simulation Parameters . . . 83

4.2 Proportion of Normal and Attack data records for training the proposed framework . . . 86

4.3 Comparison of Performance Metrics using Snort IDS . . . 87

5.1 NS-3 Simulation Parameters . . . 111

Abbreviations

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
ADCP	Authenticated Devices Configuration Protocol
AODV	Adhoc On-Demand Distance Vector
APDU	Application Protocol Data Units
CBKE	Certificate Based Key Exchange
CRWP	Cyclical Random Waypoint
CSMA-CA	Carrier Sense Multiple Access/Collision Avoidance
DAD	Duplicate address detection
DApps	Decentralized applications
DIO	DODAG Information Object
DODAG	Destination-Oriented Directed Acyclic Graph
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
ECC	Elliptic curve cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FCF	Frame Control Field
FCS	Frame Check Sequence
FPR	False Positive Rate
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Mess

IDS	Intrusion Detection System
IoET	Internet of Everything
IoT	Internet of Things
IPHC	IP header compression
IPHC	IP header compression
LLNs	Low power and Lossy Networks
MAC	Medium Access Control
MLE	Mesh Link Establishment
MoP	Mode of operation
MP2P	Multi-point-to-point
MPDUs	MAC Protocol Data Units
MTU	Maximum Transmission Unit
ND	Neighbor discovery
NS3	Network Simulator-3
P2MP	Point-to- multi-point
PHY	Physical Address Layer
PKC	PublicKey Cryptography
PSDU	Physical Service Data Unit
PUF	Physically Unclonable Function
QoS	Quality of Service
RPL	Routing Protocol for Low Power and Lossy Networks
RREQ	Route Request
SAA	Stateless Address Auto-configuration
SAA	stateless address auto configuration
SAKES	Secure Authentication and Key Establishment Scheme
SE-TRD	Smart Energy Profile 2.0 Technical Requirements Document
SKKE	Symmetric-Key Key Exchange

SN	Sequence Number
SPAM	Secure Password Authentication Mechanism
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WPAN	Wireless Personal Networks
WSNs	Wireless Sensor Networks
ZED	ZigBee end devices

Chapter 1

Introduction

The Internet of Things (IoT) is a key technology integrator in Industry 4.0, contributing to the widespread deployment of low-power IoT networks. These IoT networks have gained popularity due to their numerous advantages, which include increased productivity and a higher standard of living. On the other hand, conventional computers and communication technologies can only be employed at a limited level because IoT devices have severely limited resource capacities. Furthermore, these devices have limited resources, low power consumption, low energy requirements, limited onboard memory, and limited data processing capability. However, various IoT standards [3] have been produced in response to increased market demand and the continued development of this technology. This technology connects embedded computing devices to the internet to transmit and receive data by enabling networked connections among people, processes, data, and things, which is necessary to create intelligent applications and services. In particular, gadgets and physical goods are linked to the internet to make intelligent decisions; insight is available in real-time. People are involved in more relevant and valuable ways due to data utilization, which generally transforms data into more useful information for decision-making. In contrast, the process sends the information required to the right person (or computer) at the right moment.

In a large-scale application of the IoT, several intelligent sensors are interconnected in the IoT ecosystem. According to Safe At-Last data, there has been an exponential increase in internet-connected devices everywhere around us. Gartner, a global technology consult-

ing firm, forecasts that there will be more than 50 billion connected devices by 2025, which is nearly three times the current human population. In addition, Gartner predicts that 70 billion gadgets will be connected in the next five years. According to IDC, 41.6 billion connected Internet of Things devices will generate 79.4 zettabytes (ZB) of data by 2025.

The ZigBee standard is one of the earliest and most commonly used standards. Because of its lightweight features, low power operation, resilience, security, and improved scalability, the ZigBee Standard is a popular IoT communication protocol with a large user base [2],[3]. However, the ZigBee was designed for personal area networks and did not directly communicate with internet end users. For instance, an additional mechanism is required if the end-user wants to control ZigBee devices remotely or collect data from the ZigBee devices. Additionally, the ZigBee devices can't handle the IPv6 packets. The transmission of IPv6 packets over ZigBee-based IEEE 802.15.4 networks using a gateway via the ZigBee coordinator that connects a ZigBee network to the internet. First, the gateway translates the ZigBee frames and routes them to the end consumers across the internet. The gateways and the ZigBee coordinator must undertake the neighbor discovery procedure, which incurs the coordinator's complexity. ZigBee devices have a limited payload and larger header sizes. ZigBee standard possesses several challenging issues for interfacing in IoT networks.

1. The physical layer's maximum packet size is 127 bytes, and the data link layer's maximum frame size is 102 bytes as a result [8] and [9]. The security overhead that comes with using a security parameter is still reduced to 81 bytes on the link layer.

2. Data rates of 20 kbps, 40 kbps, and 250 kbps for each physical layer, defined at 868 MHz, 915 MHz, and 2.4 GHz, respectively, are considered low bandwidth for such a constrained network.

3. The location of the device is not predefined. Occasionally, devices relocate to a new location.

4. Devices may enter sleep mode to conserve energy. When these devices are in sleep mode, they are unable to communicate.

5. It consists of many restricted devices with low power and processing, limited memory, and energy when the devices are battery-operated.

6. All the nodes are connected through lossy links, which are generally unstable and support low data rates.

The interconnection of IoT-enabled ZigBee devices and the internet creates smart applications and services, but ZigBee was designed for personal area networks and did not directly communicate with internet end users. Hence, the ZigBee IP protocol will become more crucial with the continuous growth of dense networks of smart ZigBee IP devices. The IoT Enabled ZigBee network uses the 6LoWPAN protocol to communicate efficiently between ZigBee devices and the Internet Host. This 6LoWPAN links a number of ZigBee sensor devices with IP-based infrastructures, providing end-to-end communication for directing IPv6 packets into regional IoT-enabled ZigBee networks. The IoT Enabled ZigBee network was intended to be integrated into IEEE 802.15.4 low-range devices in various smart appliances such as smart lights, door locks, cameras, sensors, and detectors that help build home automation and industrial controls. However, all the nodes in IoT-enabled ZigBee networks are connected through lossy links, which are generally unstable and support low data rates. Many of these restricted devices have low power and processing limited memory and energy when battery-operated. Moreover, security concerns arise with ZigBee standards, which are more prone to several attacks and infiltration hazards because of their limited memory complexity and processing speed. Specifically, the ZigBee protocol has many flaws relating to

1. The distribution of keys, as they are insecurely installed on devices or transferred over the air.

2. All nodes share the same" master key" or" network key." Suppose this key is compromised on one node, jeopardizing the entire network.

3. Key secrecy and key distributions are vulnerable to attacks. (Active and passive attacks).

4. Existing protocols are based on a faulty adversary model in which all benign devices share (hardcoded symmetric keys in end devices) some secret master key that leads to worm attacks in Phillip Hue lights. The use of asymmetric cryptography is energy-hungry. There is a chance of security, and there is a chance of security attacks such as denial of service (DoS), man in the middle, false data injection, etc.

1.1 Research Motivation

As enormous devices are connected to the internet, the ZigBee IP protocol will play an increasingly significant role. Smart applications and services can be developed due to the interconnection between IoT-enabled ZigBee devices and the internet[81]. On the other hand, ZigBee was designed for local area networks and did not directly communicate with users at the receiving end of internet connections. The sending of IPv6 packets over IEEE 802.15.4 networks using a gateway that the ZigBee coordinator coordinates[108]. Further, a routing method is needed to communicate over larger distances with IoT-enabled ZigBee devices. The RPL routing protocol is one of the special standardised protocols that allows for the effective use of computing and energy resources in smart devices, as well as the development of flexible topologies and data routing to address the characteristics and limitations of IoT networks[109][110]. This protocol is used for IoT-enabled ZigBee devices. However, this protocol itself presents a significant number of potential security holes and avenues open to attack. Most of these efforts have concentrated on developing a defense mechanism to ward off specific assaults on the RPL routing protocol. Intrusion detection cannot handle a high detection rate, early detection of known attacks, the ability to identify innovative, unknown attacks, and a low false-positive rate simultaneously. The limited memory complexity and processing speed of IoT-enabled ZigBee devices also raise issues over their level of security. These devices are more vulnerable to various assaults and infiltration risks than other connected devices. Therefore, high end-to-end security rules are necessary to enable efficient and secure end-to-end communication over IoT-enabled ZigBee networks. This motivates us to provide secure end-to-end communication (ZigBee devices to end users) without relaying devices using the Blockchain system.

1.2 Limitations and Challenging Issues

This section describes the limitations and challenges of IoT-enabled ZigBee networks. The following are numerous issues with IPv6 packet transmission via ZigBee-based IEEE 802.15.4 networks: Generally, communication between the ZigBee node (ZigBee/802.15.4) and any Internet host (802.3) is achieved using a gateway through the ZigBee coordinator, as shown in Figure 1.1

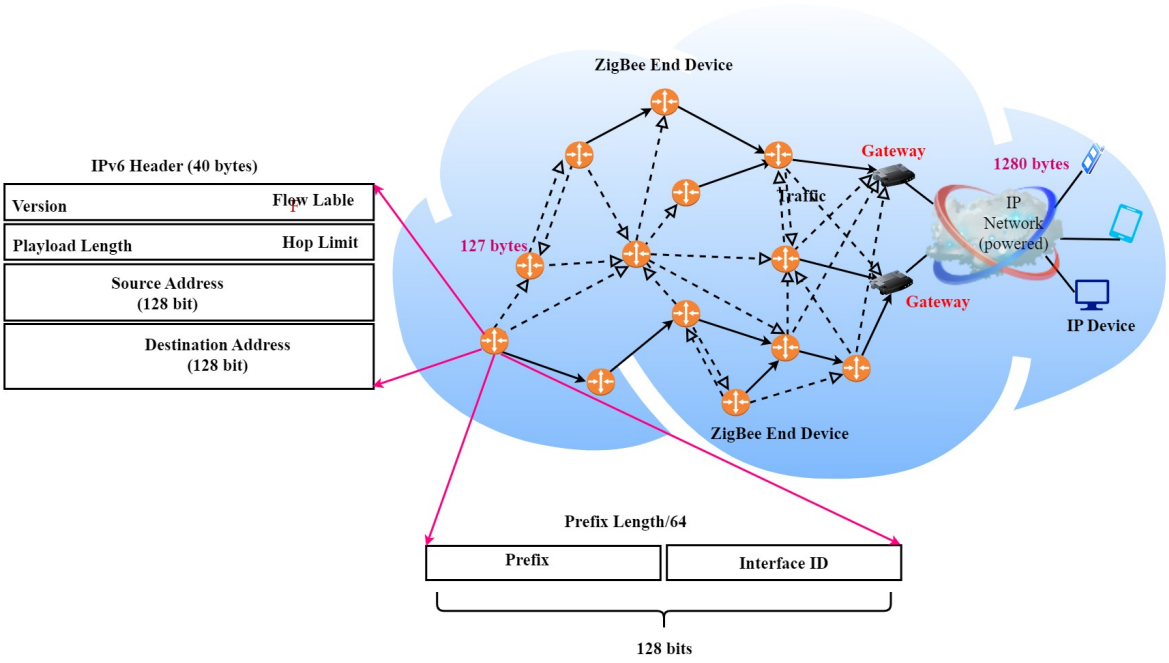


Figure 1.1: Challenging Issues in the Existing Mode

1. When a packet arrives from the internet host, the gateway encapsulates it and forwards it to the ZigBee network. The ZigBee coordinator will decapsulate the received frame and deliver the target ZigBee end device. However, some challenging issues with IoT-enabled ZigBee devices are discussed below.

    - The end-to-end communication between a ZigBee node (802.15.4) and an internet host (ipv6/802.3/802.11) through the gateway has a complex structure that needs to perform application layer protocol translations, neighbor discovery, and routing structures.

- Address assignment and data forwarding incur communication and computation overhead on the coordinator and the gateway.
- A ZigBee coordinator controls a ZigBee network and needs to handle network structures such as star topology, tree topology, and mesh topology.
- New gateways are required with hardware and software.
- The packet size issue is the fundamental issue with IPv6 over ZigBee. ZigBee devices suffer from header size problems. ZigBee devices can't handle IPv6 packets, allowing a maximum packet size of 1280 bytes. It can handle a data unit of 127 bytes only.
- Suppose the coordinator needs to be restarted when it fails. In that case, the coordinator can't rejoin the ZigBee network because all the access and control lies with the coordinator itself, which is not only present in the network, so the whole network will fail, which needs to be a single point of failure.

2. A routing approach is needed to enable communication over greater distances in IoT-enabled ZigBee devices. The existing ZigBee network uses an AODV routing protocol with a flooding mechanism unsuitable for IoT networks. The IoT routing protocol uses the RPL routing protocol, a unique standardized protocol that efficiently uses smart devices' energy and compute resources. It builds flexible topologies and data routing to address the properties mentioned above and the constraints of IoT networks. But this routing protocol is only used on the restricted network. However, the routing protocol has many security risks and possibilities for attacks. Most such efforts have been put into a mechanism to defend against individual attacks against the RPL routing protocol. Intrusion detection fails to handle a high detection rate, early detection of known attacks, a low percentage of false-positives and the capability to detect novel, unidentified threats.

   3.One of the primary reasons why there is still no standardised approach to resolving these issues is the vast number of companies that produce them and the numerous protocols derived from the numerous existing standards. The IoT-enabled ZigBee network uses the 6LoWPAN protocol to communicate efficiently between ZigBee

devices and the internet host[28]. However, security concerns arise with IoT-enabled ZigBee devices, which are more prone to several attacks and infiltration hazards because of their limited memory complexity and processing speed. Hence, enabling efficient IPv6 communication over ZigBee networks requires high end-to-end security rules.

1.3 Problem Statement

To design secure end-to-end communication utilising the Blockchain system in a ZigBee network that is IoT enabled.

1. Research Objective 1 (RO-1): To communicate with IoT-enabled ZigBee devices with IPv6 using 6LoWPAN protocol.

2. Research Objective 2 (RO-2): To detect collaborative attacks against the RPL-AODV routing protocol using the cooperative IDS mechanism in IoT-enabled ZigBee Network.

3. Research Objective 3 (RO-3): To design a trust-based Blockchain system to distribute keys among IoT-enabled ZigBee devices.

1.4 Research Contributions

In this proposed work, we contributed three research objectives to address the above problem statement:

1.4.1 RO-1: To communicate with IoT-enabled ZigBee devices with IPv6 using 6LoWPAN protocol.

This objective provides an efficient end-to-end communication protocol that addresses the above challenge issue 1, discussed in the limitation and section 1.3, by interfacing an adaptive 6LoWPAN communication protocol in an IoT-enabled ZigBee network. In order to

route IPv6 packets into ZigBee networks that support the Internet of Things, this 6LoWPAN protocol links IP-based infrastructures with ZigBee devices that offer end-to-end communication. The adaptation protocol offers services to the network and internet layers by taking data from the end devices. Once the 6LoWPAN protocol receives the query from the internet host or the user, it performs the three primary services.

1. Fragmentation and reassembly are performed to meet the IPv6 minimum MTU requirements.

2. Header compression: compressing the header deduced from link-level information is a basic shared context feature.

3. Link-layer forwarding is supported to transport IPv6 data-grams over many hops. In order to enable end-to-end communication and route IPv6 packets into local IoT-enabled ZigBee networks, the 6LoWPAN Broader router (6BR) joins IP-based infrastructures between IoT-enabled ZigBee sensor devices and the internet.

The 6LoWPAN Broder router (6BR) connects IP-based infrastructures between IoT-enabled ZigBee sensor devices and the internet to provide end-to-end communication and route the IPv6 packets into regional IoT-enabled ZigBee networks. However, packets must be transmitted or routed through a series of steps. We suggested using the RPL-AODV routing protocol and the mesh address header to transmit data packets from a single ZigBee device to 6BR over multiple steps. The combination of RPL and AODV allows route discovery for symmetric and asymmetric network flows using a reactive peer-to-peer route discovery protocol called AODV-RPL[30]. This routing protocol permits point-to-multipoint traffic from a 6BR to ZigBee devices and multipoint-to-multipoint traffic from ZigBee devices to a 6BR. The multiple traffic flows are handled using" a root-based DODAG. Further, the AODV-RPL protocol can be employed in source and hop-to-hop routing networks. The RPL-AODV routing protocol supports two routing modes: storage and monitoring. A routing table and a neighbor table are stored on all devices in the IoT-enabled ZigBee networks. The routing table and the neighbor table are used to find devices' routes and keep track of a node's immediate neighbors. The source device sends information to the edge router,

which searches its routing table for the whole path and adds it to the packet's destinations. Finally, to assess and measure the efficiency of the proposed protocol, we evaluated the performance of the proposed 6LoWPAN protocol and RPL-AODV routing protocols with various performance metrics and compared them with existing work[82].

1.4.2 RO-2: To detect collaborative attacks against the RPL-AODV routing protocol using the cooperative IDS mechanism in IoT-enabled ZigBee Network.

This objective provides solutions for the above-mentioned challenging issue 2, discussed in limitation and challenge section 1.3. First, we modeled the collaborative attacks, such as "wormhole" and "black-hole attacks", which exploit the vulnerability of the AODV protocol, and rank attacks and sinkhole attacks, which exploit the RPL protocol's vulnerability. This collaborative attack may have a more devastating impact on IoT networks than an uncoordinated attack[31]. The collaborative model was developed to investigate the weaknesses of AODV and RPL protocols in IoT-enabled ZigBee networks that exploit the IoT environment's vulnerabilities. From a security perspective, these collaborative attacks use the combined efforts of more than one attacker against the target victim. To achieve this objective, we proposed a hybrid IDS that combines signature and specification-based techniques to overcome the limitations of signature and anomaly-based approaches. This combination enables the hybrid IDS to detect signature or specification attacks, consuming less energy. The proposed cooperative IDS is a hybrid-based intrusion detection system[105] that uses an ensemble machine learning approach to combine specification-based and signature-based IDS as a cooperative IDS to detect "collaborative attacks" against the "RPL-AODV" routing protocol and effectively monitor IoT-enabled ZigBee networks.

1.4.3 RO-3: To design a trust-based Blockchain system to distribute keys among IoT-enabled ZigBee devices.

This objective provides solutions for the above-mentioned challenging issue 3, discussed in limitation and challenge section 1.3.

1. We designed efficient end-to-end security among IoT-enabled ZigBee devices by reusing the same cryptographic credentials among the ZigBee IP protocol stack using a trusted-based BCS.

2. To identify and authenticate IoT-enabled ZigBee devices using a trusted-based BCS.

3. To securely distribute the key pairs and secure communication among the ZigBee nodes with trusted storage using a physically unclonable function (PUF)

4. To provide router and end ZigBee device authentication, secure network joining, network-wide key distribution, network key update, end-to-end application key establishment, key credential storage utilising the Trust Security Service Provider, and network access control.

5. Secure IoT-enabled ZigBee against ZigBee chain worms (duplicate symmetric keys) using a proposed BCS.

This objective provides efficient solutions that use the trust-based Blockchain system pBCS to distribute keys across IoT-enabled ZigBee devices. The proposed BCS, called Blockchain: The" Trust Security Service Provider (B-TSSP)," provides the open trust model that allows end-to-end security among IoT-enabled ZigBee devices by reusing the same cryptographic credentials among the ZigBee IP protocol stack on the ZigBee edge device with trusted storage using a Physically Unclonable Function (PUF) mechanism. The trusted Blockchain will create the signed certificates using a private validator key commonly used as a root of trust. All the ZigBee coordinators, routers, and end devices must be enrolled with a BCS before their operations are performed. The ZigBee IP Coordinator is the full-function device that can initiate a new ZigBee network and maintain the Blockchain system. As per the ZigBee Alliance Specifications, each ZigBee network must have a single coordinator.

The end user will communicate with any ZED only through the ZigBee IP Coordinator when an existing ZigBee network needs to accommodate adding a new end device. Then the user must change the network's status through Blockchain DApps from closed to open state and send the exact request (open state) command to the coordinator. Then the smart contract of the Blockchain system will verify the state and change the system's state. When the ZigBee network switches to an open state, the coordinator authorizes the broadcast of a join response message, telling all ZD that the network is now accepting new joining requests and is in an open state. On the other hand, the ZigBee network cannot accept any new devices once it has reached its closed state. Only the trusted, permissioned Blockchain technology can create authentically signed certificates.

Any router or edge device that holds the validator's public key can validate the signed certificate and guarantee the public key's integrity. Finally, the secure communication protocol is designed to transfer the data between the ZED and the coordinator via a registered ZR. This secure communication protocol derives the shared secret key between the coordinator and edge devices in the untrusted field through authenticated and encrypted communication. We performed mutual authentication with less non-volatile memory (ROM) in this secure communication protocol. The Blockchain validator and ZED must be enrolled in the BCS before performing the mutual authentication. This proposed BCS solves the problem of less non-volatile memory usage and improves key management. The Blockchain validator will access the shared ledger that stores the digital key credentials of all the enrolled ZED and ZigBee Routers (ZR), including the ZigBee Coordinators.

1.5 Technical Background

This section presents the technical background used in our proposed work.

1.5.1 Overview of IoT Networks:

Internet of Things (IoT) networks [7] enable networked connections among people, processes, data, and things. However, resource constraints for IoT devices include low power, low processing, and low storage; communication technologies are susceptible to highly

asymmetric link characteristics, high data loss, low data rates, variable data loss on lossy links, and short-range communication. The nodes in the Internet of Things typically share similar characteristics, although there may be variances in their storage and processing capacities. In this matter, IETF has defined sensor nodes depending upon the capabilities of nodes into several classes, i.e., class 0, class 1, and class 2. Devices in class 0 are highly constrained in processing and memory and cannot communicate without a gateway node. Devices in class 1 are less restrictive than class 0 devices and can communicate without a gateway node. Devices in class 2 are the least restrictive and can support a protocol stack similar to that used in traditional computers.

IoT Characteristics:

1. The maximum packet size at the physical layer is 127 bytes, resulting in a maximum frame size of 102 bytes at the data link layer. Other than this, there may be security overhead on the link layer; therefore, the maximum size for data packets is 81 bytes.

2. Low bandwidth for such a constrained network includes data rates of 20 kbps, 40 kbps, and 250 kbps for each physical layer, respectively defined at 868 MHz, 915 MHz, and 2.4 GHz.

3. Device locations are not always fixed; they can occasionally change.

4. IoT devices may enter sleep mode for energy conservation, and devices in sleep mode cannot communicate.

5. It is comprised of numerous battery-operated devices with limited processing power, memory, and energy consumption.

6. All IoT nodes are connected via lossy links, which are typically unstable and support low data transfer rates.

7. It supports various traffic patterns, including point-to-point (P2P), point-to-multipoint (P2MP), and in many cases multi-point-to-point (MP2P).

Some of the key components of the IoT:

- Things/Devices: The "things" in the Internet of Things can be any physical object, ranging from simple household items such as smart thermostats, refrigerators, and light bulbs to more complex industrial machinery, wearable devices, and vehicles. These devices have sensors and actuators to collect data and take action.

- Data processing: IoT devices can process data locally on the device or send it to the cloud for further analysis and storage. Edge computing is another strategy involving data processing closer to the source, reducing latency and bandwidth demands.

- Cloud Computing: The IoT ecosystem relies heavily on cloud-based platforms. They provide scalable storage, computing power, and data analytics, allowing for real-time data processing, long-term data storage, and managing many connected devices.

- Data Analytics and Artificial Intelligence: The massive amount of data generated by Internet of Things (IoT) devices presents a tremendous opportunity for valuable insights. Patterns, trends, and actionable information are extracted from the data using advanced analytics and AI algorithms, enabling data-driven decision-making and automation.

Advantages of IoT:

1. Improved Efficiency: The Internet of Things optimizes processes, reducing the need for human intervention and streamlining operations. This efficiency can result in cost savings and increased output.

2. Enhanced Convenience: Smart home devices, wearables, and other IoT applications offer enhanced convenience by automating tasks and customizing user experiences.

3. Real-time Monitoring and Control: The Internet of Things enables real-time monitoring of various systems, allowing for prompt responses to changes and potential problems.

4. Insights Driven by Data: The data collected by IoT devices can be used to inform business strategies, predictive maintenance, and customer experiences.

5. Impact on the Environment: IoT solutions can aid in reducing energy consumption and waste, thereby contributing to more sustainable practices.

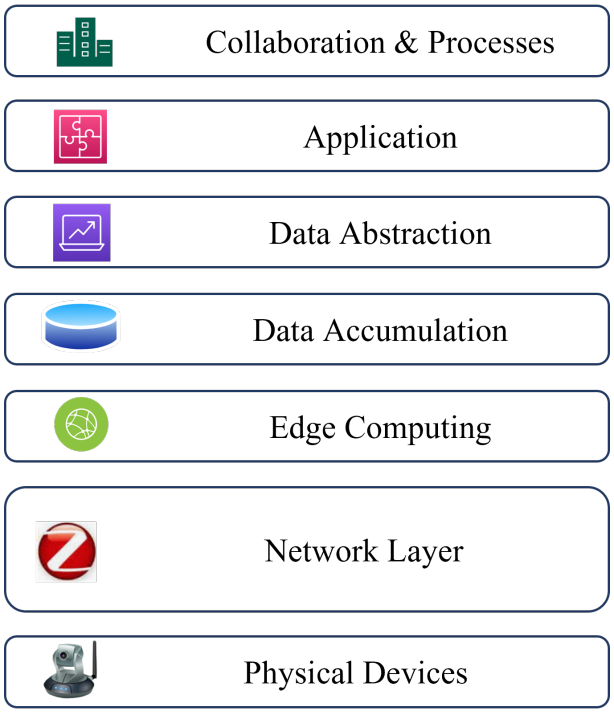


Figure 1.2: IoT Architecture

IoT Architecture: The Internet of Things (IoT) architecture comprises various layers and components that enable seamless communication, data exchange, and intelligent decision-making. The architecture of IoT can differ depending on the specific use case and application requirements. Some Internet of Things solutions may have a more decentralized architecture with edge computing capabilities, whereas others may rely heavily on cloud-based services. To enable the successful implementation of IoT solutions in various domains such as smart cities, healthcare, industrial automation, Smart agriculture,and more, the architecture must address challenges such as scalability, interoperability, reliability, and security[2][79]. The following layers are common in IoT architecture, as shown in Figure 1.2:

1. *Physical Layer:* In the Internet of Things (IoT), physical devices are very important because they are the base of the network of connected things. IoT is a system of

connected physical objects, or "things," that can collect and share data over the internet because they have sensors, software, and other technologies built into them. These physical devices, often called IoT devices or smart devices, interact with their surroundings, collect data, and talk to each other and central systems to give useful insights and automate tasks. Smart sensors, actuators, smart home devices, wearable devices, connected vehicles, industrial IoT (IIoT) devices, smart grid devices, healthcare devices, environmental monitoring devices, retail and inventory management devices, agricultural IoT devices, and smart city infrastructure are all examples of common physical devices used in IoT[6].

2. *Network Layer:* The network layer connects Internet of Things devices to the Internet. Wi-Fi, Bluetooth, Zigbee, LoRaWAN, cellular networks, and other communication protocols are included. Gateways are important in this layer because they act as intermediaries between IoT devices and the Internet. In particular,

3. *Edge Computing:*IoT uses edge computing. It processes data at the network's edge rather than sending it to the cloud. Edge computing reduces latency, bandwidth, real-time data processing, and IoT system efficiency and responsiveness. Edge computing is growing in IoT for several reasons: Low latency, bandwidth optimization, offline operation, scalability, redundancy, and resilience. IoT edge computing uses network-edge gateways or devices. Edge devices process, store, and network. Filter, aggregate, pre-process, and run lightweight analytics and machine learning models. After edge processing, relevant data can be sent to the cloud or a centralized data center for further analysis, long-term storage, and more comprehensive decision-making. Edge computing complements cloud computing in IoT ecosystems. It offers a distributed and hybrid data management and processing approach, allowing IoT applications to optimize performance and efficiency using local and cloud resources.

4. *Data Accumulation:* Data accumulation in the IoT refers to collecting and storing data generated by various Internet of Things (IoT) devices over time. IoT devices are equipped with sensors and other technologies that continuously collect data from the surrounding environment or specific processes. This data can be diverse, includ-

ing environmental conditions, device status, user interactions, machine performance, etc. Data accumulation in IoT typically involves the following: Data Collection, Data Processing at the Edge, Data Transmission, Data Storage, Data Retention, Data Security, and Privacy Data Analysis and Insights and Data Cleanup Maintenance.

5. *Data Abstraction:* Data abstraction in IoT refers to simplifying and representing complex raw data collected from various Internet of Things (IoT) devices in a more structured and manageable format. It involves creating higher-level views of the data to hide unnecessary details and expose only relevant information to the applications or systems that consume it. Data abstraction is essential for enabling efficient data processing, analysis, and decision-making in IoT applications. The key aspects of data abstraction in IoT include Data Representation, Data Aggregation, Contextual Information, Standardisation, Data Filtering, semantic representation, and Representation modeling.

6. *Applications:* The Internet of Things (IoT) has numerous applications in various industries and markets. It involves connecting commonplace objects, devices, and systems to the internet to collect and exchange data, resulting in improved automation, efficiency, and insights. Here are several prominent IoT applications: Industrial IoT (IIoT), Agriculture, Smart Cities, Transportation and Logistics, Environmental Monitoring, Retail and Customer Experience, Energy Management, Wearable Devices, Smart Grids, Security and Surveillance, Education, Sports, and Fitness.

7. *Collaboration and processes:* Collaboration and processes are critical to successful Internet of Things (IoT) implementations. The complexity of IoT solutions often involves multiple stakeholders, devices, and systems working together to achieve a common goal. Effective collaboration and well-defined processes are essential for ensuring IoT projects' smooth development, deployment, and operation. Here are some key aspects of collaboration and processes in IoT: Interdisciplinary Collaboration, IoT Ecosystem Partnerships, Data Sharing and Integration, Standards and Interoperability, Agile Development, Security and Privacy Collaboration, Testing and Validation Processes, Data Governance and Compliance, Deployment and Mainte-

nance Processes, Continuous Improvement, and Change Management

IoT Challenges: Some of the challenges of IoT networks are discussed below.

1. *Security and Privacy:* IoT devices are often vulnerable to cybersecurity threats due to their large-scale deployment and diverse communication protocols. Many devices lack built-in security measures, making them susceptible to hacking and unauthorized access. Data privacy is a major concern as IoT devices collect and transmit sensitive information. Ensuring data encryption, access control, and secure authentication mechanisms are essential to protecting user data and privacy.

2. *Interoperability:* The IoT ecosystem consists of various devices from different manufacturers, each with its communication protocols and standards. Ensuring seamless interoperability between devices is a significant challenge. The lack of standardization hampers the integration and scalability of IoT solutions, making it challenging for different devices to communicate and work together effectively.

3. *Data Overload and Management:* The IoT generates massive volumes of data from numerous connected devices. This data overload poses challenges regarding data storage, processing, and analysis. Efficient data management strategies, including data filtering, aggregation, and analytics, are crucial to derive meaningful insights and prevent system overload.

4. *Power Consumption and Battery Life:* Many IoT devices operate on batteries, and optimizing power consumption is essential for their long-term viability and usability. Low-power design techniques, energy harvesting solutions, and advancements in battery technology are needed to improve the battery life of IoT devices.

5. *Scalability:* As the number of connected devices increases, IoT solutions must be scalable to handle the growing demands of data processing, communication, and management. Scalability challenges can arise in IoT systems' hardware (devices and networks) and software (cloud platforms and applications) components.

6. *Reliability and Stability:* IoT applications often involve critical tasks such as healthcare monitoring, industrial automation, and autonomous vehicles. Ensuring the reliability and stability of these systems is essential to preventing failures and potential dangers. Network outages, device malfunctions, and communication issues can disrupt the functioning of IoT solutions, making reliability a critical concern.

Specific Challenging Issues in IoT-enabled ZigBee Networks:

1. *Duty cycle and Power:* Battery-operated wireless devices must keep the percentage of time active low. In IP, the assumption is device is always connected.

2. *Multicast:* IEEE 802.15.4, which is embedded wireless radio technology, does not support multicasting, and in such a constrained network, flooding is a waste of bandwidth and power.

3. *Frame size and Bandwidth:* Generally, embedded wireless radio technologies have a limited bandwidth range of 20-250 kbps, while the frame size is 40-200 Bytes. In the case of IEEE 802.15.4 frame size is 127 bytes. In standard IPv6, the minimum size of the frame is 1280 bytes and therefore requires fragmentation.

4. *Reliability:* In a wireless embedded network, unreliability problem occurs due to low energy or energy exhaustion, node failure, and sleep duty cycle.

5. *Limited Management and Configuration:* IOT devices have limited capabilities for input, and it is hard to reach the location of such devices. Therefore, the protocols used in IOT must have minimized configuration and be easy for bootstrapping.

6. *Fragmentation and Reassembly:* In IEEE 802.15.4, the maximum frame length is 127 bytes at the data link layer, which does not match the maximum transfer unit of 1280 bytes in IPv6. So to transmit IPv6 frames over the wireless radio links in IEEE 802.15.4, the frames are required to divide into different small segments. For this work, the extra overhead is generated in the header to reassemble the data packets at the end in the correct sequence. When the data packets are reassembled, the extra overhead is removed, added earlier, and the data packet is restored to its original IPv6

format. Based on the routing used, there can be different fragmentation sequences. When it meshes under routing, then at the final destination, only other fragments are reassembled, while when it is a route over the network, packets are reassembled at every hop. Therefore, every node needs sufficient storage to route over the network for the fragments. More traffic is generated since all the fragments pass instantly in the mesh under the system. In mesh under the system, if a single fragment is missing when reassembling, there is a need to retransmit the whole packet. Since when the devices are battery-operated, fragmentation needs to be avoided. Memory need is a major factor since all fragments are reassembled at the final destination. Therefore, header compression and keeping the payload low are of utmost importance.

7. *Header Compression:* In the most pessimistic scenario, the greatest size accessible for transmitting IP parcels over an IEEE 802.15.4 wireless frame is 81 B, and without optional headers, the header in IPv6 is 40 bytes. After this, only 41 bytes are left for the upper layer protocols like TCP and UDP. 8 bytes are used in the UDP header, while 20 are for the TCP header. This leaves data over UDP of 33 bytes and 21 bytes over TCP. Fragmentation and reassembly are also required, consuming more bytes and leaving only a few data bytes. Hence, if one somehow manages to utilize the protocols as may be, it leads to more fragmentation and reassembly; this happens even when the packet size is just 10s of bytes. This point requires header compression.

1.5.2 Overview of ZigBeeTechnology

ZigBeeis a wireless communication protocol for low-power, low-data-rate, and short-range wireless device-to-device communication. It is among the most prominent wireless sensor networks and Internet of Things (IoT) standards[32]. ZigBeeis designed to be highly efficient, making it suitable for battery-powered devices that require extended operation. Some of the key features and characteristics of ZigBee technology.

1. *Low Power:* ZigBeeis optimized for low power consumption, making it ideal for battery-powered sensors, smart home devices, and industrial applications. The protocol enables devices to enter sleep mode when not transmitting or receiving data,

significantly extending their battery life.

2. *Low Data Rate:* ZigBeeoperates at low data rates, typically between 20 and 250 kbps. This is ideal for applications that require the random transmission of small amounts of data.

3. *Mesh Network Topology:* ZigBeeutilizes a mesh network topology in which each device acts as a router and forwards data to other devices on the network. This increases network coverage, redundancy, and dependability, as multiple routes can relay messages.

4. *Self-Healing and Self-Organising:* ZigBeenetworks are self-healing, which means that if a device or router fails, the network will find alternative data routes. In addition, the network can self-organize, allowing new devices to join without manual configuration.

5. *Low Latency:* ZigBeeprovides communication with low latency, which is advantageous for real-time control and automation applications.

6. *Security:* ZigBeeincorporates security measures to safeguard data transmitted over the network. It employs encryption and authentication mechanisms to prevent unauthorized access and preserve the integrity of the data.

7. *Frequency Bands:* Depending on the region, ZigBeeoperates within the 2.4 GHz, 900 MHz, and 868 MHz frequency bands. The 2.4 GHz band is the most popular, but other bands offer superior range and penetration through walls and obstructions.

1.5.2.1 ZigBee Applications:

ZigBee is widely used in various applications, including:

1. *Smart Home Automation:* ZigBeeis a common choice for smart home devices such as smart light bulbs, door locks, thermostats, and motion sensors. It is suited for these applications due to its low power consumption and mesh networking capabilities.

2. *Industrial Automation:* ZigBeeis used in industrial settings to monitor and control equipment, collect sensor data, and enable wireless communication in harsh environments.

3. *Healthcare:* ZigBeeis utilized in healthcare applications, including patient monitoring systems, remote health monitoring, and medical equipment tracking.

4. *Smart Lighting:* Smart Lighting: Zigbee's mesh network enables efficient and flexible control of smart lighting systems, allowing for simple integration of a variety of lighting fixtures.

5. *Environmental Monitoring:* Zigbee-based sensor networks are used for environmental monitoring, including monitoring of air quality, temperature, and humidity.

ZigBeeis supported by the ZigBeeAlliance, a global organization that develops and promotes the ZigBeestandard. As the Internet of Things (IoT) and wireless communication technologies continue to develop, new enhancements and updates are introduced to the standard.

1.5.3 Overview of Blockchain Technology

Since introducing cryptocurrencies, most notably Bitcoin, in 2009, blockchain technology has garnered considerable attention as a revolutionary concept. A blockchain is essentially a distributed, decentralized ledger that records transactions in a secure, immutable, and transparent manner. The technology can disrupt multiple industries and revolutionize data storage, sharing, and verification. A summary of blockchain technology follows.

1. *Decentralization:* Unlike traditional centralized systems, where a single entity (such as a bank or government) controls the data, a Blockchain operates on a decentralized network of computers (nodes). Each network node stores a copy of the entire Blockchain, ensuring no single point of failure and bolstering the system's resilience.

2. *Distributed Ledger:* A blockchain is a chain of blocks, with each block containing a group of transactions. These transactions are encrypted to the previous block, forming a chain. This structure guarantees that the data are sequentially organized and tamper-proof.

3. *Consensus Mechanisms:* Blockchains utilize various consensus mechanisms to achieve consensus on the ledger's state and validate transactions. Proof of Work (PoW) is the most well-known algorithm utilized by Bitcoin, in which participants (miners) compete to solve complex mathematical puzzles to add a new block to the chain. Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT), among others are additional consensus mechanisms.

4. *Security:* The security of Blockchain is ensured by cryptographic techniques. Each transaction is digitally signed, and the data in blocks cannot be modified retroactively without altering subsequent blocks. The network's distributed nature also makes it highly resistant to attacks.

5. *Immutability:* Once data is recorded in a block and added to the Blockchain, it is exceedingly difficult to modify or delete it. This immutability feature ensures data integrity and fosters participant confidence.

6. *Transparency:* All network participants have access to the complete transaction history. While the users' identities may remain anonymous, the transactions are visible to all, which promotes transparency and accountability.

7. *Smart Contracts:* Smart contracts are contracts that automatically execute, with the terms of the agreement written directly in code. They execute automatically when certain conditions are met. Ethereum, a blockchain-based platform, popularised smart contracts, enabling decentralized applications (DApps) with diverse use cases outside of cryptocurrencies.

8. *Use Cases:* Blockchain technology is not limited to cryptocurrency transactions. It has numerous applications, including supply chain management, voting systems,

identity verification, real estate, healthcare, and finance. Diverse industries are attracted to it because it can increase transparency, security, and efficiency.

9. *Scalability and Energy Efficiency:* Blockchain technology faces scalability and energy consumption issues, particularly in PoW-based networks. Several initiatives are underway to address these issues and create more energy-efficient consensus mechanisms.

Blockchain technology constantly evolves, and its effects on various industries are still being investigated. While it presents many opportunities, it also faces obstacles that necessitate additional research and development to realize its full potential.

1.5.4 Role of Blockchain in IoT-Enabled ZigBee Networks

Blockchain plays a crucial role in the IoT-enabled ZigBee networks by addressing diverse challenges and improving IoT ecosystems' security, privacy, and efficiency. Here are some of the key functions of Blockchain in IoT:

1. *Decentralization and Trust:* Typically, IoT devices rely on centralized servers or cloud platforms to manage data, resulting in single points of failure and potential security vulnerabilities. Blockchain enables decentralization by distributing data across multiple nodes in a network. This decentralization fosters trust because data cannot be easily tampered with, ensuring the network's integrity.

2. *Data Integrity and Immutability:* The underlying technology of Blockchain is based on cryptographic hashing and consensus algorithms, making it nearly impossible to alter previously recorded data. This immutability ensures that the data collected from IoT devices remains secure and trustworthy, preventing unauthorized modifications and preserving a reliable historical record of events.

3. *Security and Authentication:* Blockchain improves IoT device security by enabling authentication and authorization mechanisms. Each device's identity can be recorded on the Blockchain, and network access can be regulated using cryptographic keys, thereby reducing the risk of unauthorized access and device spoofing[83].

4. *Data Sharing and Monetization:* The IoT generates vast quantities of data to which multiple parties may require access. Blockchain enables secure and transparent data sharing between authorized parties while allowing data owners to retain control over their data. This can also facilitate the development of new data monetization models that reward IoT device owners for sharing data with others.

5. *Smart Contracts and Automation:* Smart contracts are contracts with predefined, blockchain-encoded rules that execute themselves. They allow for the automated and untrusted execution of actions when certain conditions are met. Smart contracts can automate IoT-related processes without intermediaries, such as triggering actions based on IoT device data.

Despite its potential benefits, integrating Blockchain with IoT systems is still a complex task, and carefully considering the specific use case, scalability, and privacy requirements is necessary to fully realize its potential in IoT applications[10][9][64].

1.6 Organization of the Thesis

The remainder of this thesis is organized as follows. In **Chapter 2**, we discussed the literature review related to every chapter of this thesis. In **Chapter 3**, we proposed a framework for efficient communication between ZigBee-enabled IoT devices and Internet Hosts using the 6LoWPAN protocol. The proposed protocol routes IPv6 packets into regional IoT-capable ZigBee networks by integrating IP-based infrastructures with end-to-end ZigBee sensor devices. In **Chapter 4**, we proposed a cooperative IDS mechanism that detects collaborative attacks against RPL-AODV routing protocol in IoT Enabled ZigBee Networks (IEZN). In **Chapter 5**, we proposed the key management mechanism for distributing keys among IoT-Enabled ZigBee Networks utilizing a trust-based blockchain system. Finally, we summarize our contributions as presented in this thesis and discuss directions for future work in **Chapter 6**.

Chapter 2

Related Work

This chapter presents the state-of-the-art work on IoT-enabled ZigBee networks, the routing protocol on IoT-enabled ZigBee networks, and IoT security that provides the basis for the proposed work.

2.1 State-of-the-art work on IoT-enabled ZigBee devices:

In this study, we reviewed the earlier researcher's proposal to improve ZigBee node (802.15.4) connection with any Internet host using gateway through the ZigBee coordinator for security is given. The packet size issue is the fundamental issue with IPv6 over ZigBee. The ZigBee devices can't handle the IPv6 packets, allowing a maximum packet size of 1280 bytes. ZigBee devices can operate on a data unit of 127 bytes only. ZigBee technology was designed for personal area networks and did not directly communicate with internet users. IPv6 packets are sent through IEEE 802.15.4 networks built on ZigBee using a gateway and the ZigBee coordinator. However, the ZigBee devices can't handle the IPv6 packets. The gateways and the ZigBee coordinator need to perform the neighbor discovery process. Moreover, ZigBee networks use state-of-the-art routing protocols such as "Adhoc On-Demand Distance Vector" (AODV), limiting resources, causing significant packet loss, and resulting in low network speed. The route discovery process still possesses significant network overhead. However, many ZigBee devices lack such an interface due to their limitations.

Don Sturek et al. [2] proposed The ZigBee IP specification's goal is to define a standard, inter-operable protocol stack for use in IEEE 802.15.4-based wireless mesh networks using IETF-defined networking protocols. They operate in Smart Energy Profile 2.0 applications and other ZigBee applications that might transition to a ZigBee IP stack. Sometimes MLE messages are sent and received before a node joins the network and configures secure links with its neighboring nodes. The MLE protocol defines its mechanism to secure its payload because MLE messages cannot always rely on MAC security.

Amit Kumar Sikder et al. [4] proposed an overview of the SLS. They looked at various "IoT-enabled communication protocols" that may be used to implement the SLS in the context of smart cities. Moreover, the author analyzed different usage scenarios for IoT-enabled indoor and outside SLS and analyzed the power consumption. The authors have developed "IoT-enabled smart lighting systems" to reduce power consumption by 33.33 indoors and outdoors.

Reen-Cheng Wang et al. [5]proposed an internetworking mechanism for effortless communication of IP-based networks and ZigBee networks based on IEEE 802.15.4. However, the proposed mechanism suffers from an "address-in-address problem," in which the MTU problem occurs in Ipv4/ ipv6 NAT-PT design.

Chia-Wen Lu et al. [6] have proposed a SIP-based protocol for effective communication in smart grids. Thus, the status of the WSN may be monitored by reusing several current IP-based services. The author contrasts the benefits and drawbacks of IP and ZigBee from the standpoint of network management service. ZigBee is only suitable for small-scale networks and suffers from a sensor network's scope growth. Yan Li et al. [7] have introduced Passive-ZigBee, which demonstrates and transforms an existing productive Wi-Fi signal into a ZigBee packet for a CoTS low-power consumption receiver while consuming 1,440 times lower power than traditional ZigBee.

Alaoui Ismaili et al. [11] proposed a comparative study of ZigBee and 6LoWPAN protocols. To conduct a comparative analysis of ZigBee's strengths and shortcomings based on energy consumption, mesh architectural scope, and dependability to arrive at a more suitable standard for industrial demands. They gave two ZigBee versions for comparison. According to Alaoui, the most appropriate protocol is applicable for WSN, analyzing and

comparing ZigBee, ZigBee IP, and 6lowpan protocols based on the network topology, Max Outdoor Range, Security, and Max Nodes.

Emanuele Toscano et al. [19] proposed addressing Using experimental measurements made on a genuine testbed, the low-power techniques offered by the IEEE 802.15.4/ZigBee and 6LoWPAN protocols are compared. After discussing this tuning step, the chapter compares the protocol's performance gained on the same network, with the same workload, and while operating at the same duty cycle. The comparison focuses on how low-power techniques affect the functionality of networks. The experimental evaluations highlight the advantages and disadvantages of the two methods when operating in low-power mode.

Yu-Kai Huang et al. [15]proposed that ensure low power consumption for ZigBee devices, the IEEE 802.15.4 MAC layer implements duty-cycle operations by setting two system parameters, mac "BeaconOrder" (BO) and mac "SuperFrameOrder" (SO). The duty-cycle functioning of IEEE 802.15.4 is thoroughly examined in this chapter. In particular, a fresh analytical model that considers typical traffic patterns is created. An NS-2-based simulation model is also suggested and verified as a developed analytical model.

Chen et al. [16] presented Some significant performance-evaluation insights gathered from the trials run by the analytical and simulation models. These insights can be utilized as recommendations for deploying future low-power ZigBee networks. Connectivity, compatibility, and coverage can be improved in WSNs by employing the 6LoWPAN protocol. Recent works in which the simulation of energy efficiency-based smart IoT applications.

Zheng Huang et al. [17] have presented a 6LoWPAN-based neighborhood area network for a smart grid communication infrastructure is proposed. A NAN is essential to a smart grid communication network architecture that permits communication between end devices and multiple controllers. Infrastructure-based access networks, such as WiMAX or LTE-based systems, may be developed to cover a large geographic region. The author developed a 6LoWPAN-based NAN architecture that can handle all smart meters in a NAN coverage area while meeting the QoS requirements of various applications inside NANs. The author created a thorough OPNET-based simulation model that analyses the performance of a 6 LoW PAN-based NAN. The simulation scenario comprises a few smart meters divided into two groups. Each cluster serves 12 smart meters linked to a router mounted on a power

S.No	Title	ZigBee	6LoWPAN	IPv6	RPL	AODV	RPL-AODV
1	Rahman et al. [74]	✓	✗	✗	✗	✗	✗
2	Mahajan et al. [49]	✓	✗	✗	✓	✗	✗
3	P. Aithal et al. [81]	✓	✗	✓	✗	✗	✗
4	A.K. Sangaiah et al. [5]	✓	✓	✓	✗	✗	✗
5	A. Haka et al. [1]	✓	✓	✗	✗	✗	✗
6	Wang et al. [114]	✓	✓	✓	✗	✗	✗
7	Venna et al. [28]	✗	✓	✓	✗	✓	✗
8	Samuel et al. [28]	✗	✓	✓	✓	✓	✓
9	Sobral et al. [64]	✗	✓	✓	✓	✓	✓
10	Santos et al. [21]	✗	✓	✓	✗	✓	✓
11	Kassab et al. [111]	✓	✓	✓	✗	✓	✓

Table 2.1: Comparative Analysis of State-of-the-art work on IoT enabled ZigBee Networks

pole.

Dharmini Shreenivas et al. Proposed identified intrusions to disrupt the RPL. In [18], the intrusion detection module that employs the "Expected Transmissions" (ETX) metric to SVELTE, an Internet of Things intrusion detection system, increases security inside 6LoWPAN networks. Monitoring the ETX value can stop an attacker from aggressively engaging 6LoWPAN nodes in harmful operations. ETX is a link reliability statistic in RPL. They suggest using geographic cues to spot rogue nodes that attack ETX-based networks.

B. Priyeash et al. [19]. A "wireless sensor network" is called a "Low-power and Lossy Network" (LLN) (WSN). These networks have limitations regarding memory, power, size, etc. Devices placed in these networks must be tuned to consume the least resources possible for an extended period carefully. Sometimes these networks are set up in locations where it is impossible to have regular human interaction. It is crucial to choose the right routing protocols for these low-power devices. Two significant protocols are "ad-hoc on-demand distance vectors" (AODV) and low-power and lossy networks (RPL) routing protocols[27] [28]. The Tetcos NetSim network simulator thoroughly examines the benefits and drawbacks of these two protocols. According to the findings, RPL uses more energy but has higher throughput. Transmitting control packets often causes the data packets to travel farther than AODV. The comparative analysis of exiting work is shown in Table 2.1.

2.2 State-of-the-Art Work on Routing Protocol in an IoT-enabled ZigBee Network:

In this section, we presented the literature review on routing protocol in an IoT-enabled ZigBee network that provides the basis for chapter-4. IoT routing attacks have to be detected, prevented, and mitigated by reviewing existing techniques [26]. Routing attacks are mostly caused by a lack of standards inside the domain. It is crucial to realise that the majority of IoT users are non-technical individuals who use the technology in smart homes, smart watches, CCTV cameras, and other devices. It is not advised for such individuals to analyse the internal workings of the system, such as networking. Therefore, it would make sense for the companies that manufacture electronic devices to implement safeguards like shutting ports that end users wouldn't use and setting up complex authentication procedures. We also studied the prevention mechanism in which unused ports are closed and default login credentials are changed to thwart brute-force DoS attacks [3],[25] which are currently the most happening. These attacks can also be stopped if standards are maintained across devices and companies manufacturing them. Some chapters have described different security attacks [10] against the RPL protocol. The attacks include attacks on topology, attacks against resources, and attacks on traffic. The significant consequences of these attacks are denial of service, network congestion, and network instability, leading to performance degradation. Some protocols were mentioned to detect the attacks or general solutions, like heartbeat protocol, rank authentication, IDS system-based building global view of the network, etc. We investigated various attacks and mechanisms to ensure secure routing against security attacks in RPL protocol.

The goal of this analysis of existing methods is to identify, stop, and lessen Internet of Things routing assaults. The absence of domain-wide standards is the main cause of routing assaults[49]. It is essential to recognise that the majority of IoT users are non-technical individuals utilising CCTV cameras, smartwatches, smart homes, etc. Analysis of the system's inner workings, such as networking, is not recommended for these individuals. Therefore, it would make sense for device manufacturers to implement measures such as closing ports that end-users would not utilise and establishing complex credentials. We

also studied a prevention mechanism in which unused ports are closed, and default login credentials are changed to thwart brute-force DoS attacks [3], which are currently the most common[25]. These attacks can also be stopped if standards are maintained across devices and companies manufacturing them. Some referred papers have described different security attacks [10] against the RPL protocol. The different attacks include attacks on topology, attacks against resources, and attacks on traffic. The major consequences of these attacks are denial of service, network congestion, and network instability, leading to performance degradation [21]. Some protocols were mentioned to detect the attacks or general solutions like heartbeat protocol, rank authentication, IDS system-based building global view of the network, etc. The interconnection of IoT devices with the IPv6 or 6LoWPAN protocol is beneficial for enabling low-powered IoT devices to achieve scalability.

Ghada Glissa et al. [3] The proposed solution was developed and tested using the Contiki operating system. Compared to lighter PSec and other upper-layer security solutions, it has demonstrated efficacy. As a result, we can attest that 6LowPSec performs admirably in terms of latency and memory footprint. While assuming favorable conditions like mesh-under routing (LOADng) and existing security features of the MAC IEEE 802.15.4 layer, the security solution's impact on the overall system is tolerable. We presented the "6Low-IP-Sec" security protocol, which offers an excellent end-to-end security solution but operates at the adaptation layer. The MAC security sub-layer specifies the hardware security features used by 6Low-PSec. A thorough campaign comparing the capabilities of 6Low-PSec and the lightweight IP-Sec is presented. Results demonstrate the viability of a low-overhead, end-to-end hardware security solution for the Internet of Things that operates at the adaptation layer. This new mechanism necessitates mesh-under routing turned on in the adaptation layer, which offers low-level end-to-end communication between terminals to facilitate the integration of embedded link layer security features.

Amit Kumar Sikder et al. [38] proposed an overview of the SLS. They looked at various IoT-enabled communication protocols that could be applied to implement the SLS in the context of smart cities. Additionally, the author examined several IoT-enabled indoor and outdoor SLS usage situations as well as power consumption. The authors have created IoT-enabled smart lighting solutions that can save electricity usage in both indoor and outdoor

environments by up to 33.33%.

Chia-Wen Lu et al. [13] have proposed a SIP-based protocol for effective communication in smart grids. Many existing IP-based services can thus be reused to monitor WSN's real-time status. From a perspective on network management services, the author compares the advantages and disadvantages of ZigBee and IP protocols. Since ZigBee is only appropriate for small-scale networks and suffers from the scope expansion of a sensor network. In [7], BLSTM-RNN detection is performed at the packet level, focusing on text recognition within features, otherwise usually discarded by flow-based techniques. The BLSTM introduced has two independent layers to accumulate contextual information from the past and the future. The authors choose four attack vectors used by Mirai-User Datagram Protocol (UDP) flood, Acknowledgement (ACK) flood, Domain Name System (DNS) flood, and Synchronize (SYN) flood. Messages between the C&C server and the infected device were captured along with the normal data generated by the device. After converting them into the CSV format, all the analysis was done using the .pcap files.

In [25] discussed, the traditional attack detection systems cannot be located in IoT environments because of the diverse architecture of the underlying network methodologies and the different natures of such devices. Additionally, new attacks can be distinct from those already on traditional network devices. Heavy encryption methods cannot be deployed on these resource-hungry devices. Rule-based detection systems are comparatively easier to circumvent, and machine learning-based systems can somewhat detect the variances of many attacks. Furthermore, the ML classifier training process is tough to implement on these low-resource devices. Authors' Model - The authors' model uses ANN, J48 Algorithm (called C4.5 and is a descendant of ID3), Naive Bayes, and Correlation-Based Feature Selection. Using multiple Machine Learning algorithms selects, the best matching one according to the detection accuracy obtained for each sub-engines. In this way, the authors successfully create a hybrid detection architecture.

In [29], the authors have proposed the Merkle tree-based wormhole attack avoidance mechanism against the DAG-based structure of the RPL protocol that generates the hash for the information and is stored in the tree. The author has proposed an authentication mechanism for avoiding the promotion of routes but increases the cost of communication with

the root. If an entry is not discovered, the authentication element is authenticated with the hashed security element at the root and the public key of the new node. [22] discussed the TRAIL - Trust Anchor Generic topological inconsistency detection and prevention method called the Interconnection Loop. Each node has the ability to verify the path leading up to the root and to recognise rank faking.

The 6LoWPAN protocol provides connectivity, compatibility, and coverage using IoT devices. A 6LoWPAN-based neighborhood area network for a smart grid communication infrastructure is proposed in [13], [1], and [28]. A NAN is a key component of a smart grid communication network infrastructure that enables communication between end devices and various controllers within a smart grid. It can cover a vast geographic area using infrastructure-based access networks such as WiMAX or LTE-based systems. The author developed a 6LoWPAN-based NAN architecture that can handle all smart meters in a NAN coverage area while meeting the QoS requirements of various applications inside NANs. A protocol for 6LoWPAN and its application in smart lighting and healthcare are proposed in [45], [26]. These smart lights based on Power Line Communication (PLC) are short on data rates and use inappropriate communication protocols. They have updated the smart lighting system from PLC to 6LoWPAN. 6LoWPAN nodes replace the PLC nodes, and 6LoWPAN routers replace the controllers. From these implementations, they have gained more advantages in transmission rate, signal range, and compatibility compared to PLCs. 6LoWPAN with IP-standard interconnection makes integrating various types of sensors for monitoring easier. The Table 2.2 shows the comparative summary of routing protocol in IEZN.

2.3 State-of-the-art work on IoT-enabled ZigBee Network Security:

In this section, we investigated the literature survey on consortium Blockchain systems to secure the IoT-enabled ZigBee network due to the numerous security issues with sending IPv6 packets across IEEE 802.15.4 ZigBee networks. It's challenging to authenticate and

Table 2.2: Summary of the routing protocol and security issues on IoT-enabled ZigBee networks.

Ref.	A	B	C	D	E	F	G	H
Ambili et al. [15]	×	✓	×	✓	×	✓	×	×
Anhtuan et al. [71]	×	✓	×	✓	×	✓	×	×
Semih Cakir et al. [30]	×	✓	×	✓	✓	×	×	✓
Chin-Yang et al. [37]	✓	×	×	✓	×	✓	×	×
John Foley et al. [43]	×	✓	×	✓	×	✓	×	×
Jian-Ming et al. [31]	✓	×	×	✓	×	✓	✓	✓
M. Zhang et al. [17]	×	×	✓	×	×	×	×	×
M. Napiah et al. [80]	×	✓	×	×	×	✓	×	×
Ioulianou et al. [62]	×	✓	×	✓	×	✓	×	×
Mina Zaminkar et al. [119]	×	✓	×	✓	×	✓	×	×
Junqi Duan et al. [37]	✓	×	×	✓	×	×	×	×
Van Kerkhoven et al. [63]	×	✓	×	×	×	×	×	×

A = AODV Routing Protocol, B = RPL Routing Protocol C = RPL-AODV Routing Protocol, D = Routing Attacks, E= Collaborative Attacks, F = Specification-Based IDS, G = Signature-Based IDS, H = Hybrid IDS

check a new device when it tries to join a network and deliver the network key securely from the coordinators to the new device [3][1]. Following are some of the most pertinent answers offered in earlier literature.

Mostafa Yavari et al. [4] proposed the IBCbAP, a better Blockchain-based authentication protocol with anonymity and secure access management. Implemented by using the local Ethereum Blockchain and JavaScript programming language. Blockchain, essentially an anti-hacking, distributed, and event-logging mechanism, seems very helpful for resolving important issues related to networks where connected devices automatically interact with each other or IoT. IoT security is crucial, so numerous plans have been put forth in this area. The author also suggested a better protocol called IBCbAP and demonstrated its security informally and formally using the Scyther tool to address the security flaws in Cha et al. In the end, the author used the local Ethereum Blockchain network and the JavaScript programming language to implement IBCbAP, measured some processes' timing, and looked into the viability of implementing IBCbAP. The IBCbAP-developed protocol is completely secure and costs a reasonable amount of time and money compared to its predecessor. The transfer of ownership is one of the most crucial issues in the IoT

network.

Weicheng Wang et al. [5] presented a new ZigBee joining protocol built on cheap public-key primitives without certificates. The second method uses public key encryption; a new joining method was added to ZigBee 3.0 to improve the installation code's security. They are using the formal verification techniques offered by ProVerif. The author proposes two cryptographic improvements to the ZigBee security protocols and then implements and tests the suggested protocols. The author's evaluations also offer compelling evidence that these improvements are doable and successful in fending off passive and active attackers.

Ender Yuksel et al. [1] proposed the fundamental security provisions of the most current ZigBee specification, ZigBee-2007. They delved further into the calculations behind authentication and key establishment methods like SKKE, CBKE, and MEA, as well as the critical protocol narrations like "Authentication," "NK Update," etc. Their author defines the key ideas, computations, and protocols and creates them using standard protocol narratives. These mainly focus on authentication characteristics and conclude that pre-deployed key mechanisms, "symmetric key" agreements, and ECC-based algorithms are now the trend for performing authentication in WSNs. The author anticipates that the wide range of applications for ZigBee will require a lot more work in ZigBee security and intends to examine and confirm the security protocols for ZigBee.

Ghada Glissa et al. [3] The proposed solution was developed and tested using the Contiki operating system. Compared to lighter PSec and other upper-layer security solutions, it has demonstrated efficacy. As a result, we can attest that 6LowPSec performs admirably in terms of latency and memory footprint. The MAC security sublayer specifies the hardware security features used by 6Low- PSec. A thorough campaign comparing the capabilities of 6LowPSec and the lightweight IPSec is presented. The outcomes show the potential of an adaption layer-based, low-overhead hardware security solution for the Internet of Things. Mesh-under routing with the adaption layer activated is required for this new technique because it provides a low-level end-to-end terminal connection that makes it easier to include integrated link layer security measures.

Bernardo David et al. [6] proposed a Blockchain-based incentive system for Tor's partially decentralized anonymous routing network nodes. Most of them are reputation-based

approaches, effectively providing nodes with a mechanism to evaluate the contribution of their peers to routing and retaining local records of each other's reliability. Based on these results, nodes can decide which peers to work with. However, because each node keeps track of its reputation records locally, existing reputation-based methods enable dishonest nodes to accuse their peers of wrongdoing. These problems affect the accuracy and effectiveness of the existing reputation systems, which employ complex heuristics to lessen unfounded misconduct charges and produce a uniform reputation impression among honest nodes. The solutions also included financial incentives, urging the creation of a "central bank" entity that compensates nodes for participating in routing.

Chi Ho Lau et al. [13] The proposed solution can be implemented in the existing network without requiring significant changes to the communication standards. Blockchain technology identifies IoT devices before they connect to a network. IoT devices can be authenticated and created with digital identification based on the properties of Blockchain. This authentication procedure is proposed using the Authenticated Devices Configuration Protocol (ADCP). A detailed discussion of the system's design and mechanism has taken place to demonstrate the solution's viability. A fully functional implementation supports The solution's conclusions rather than just theoretical arguments or computer simulations.

Muhammad Tanveer et al. [16] proposed a method that, independent of the IPSec protocol, performs header or origin verification of the message. To support a secure handover procedure in proxy mobile IPv6 networks, the authors suggest a "Secure Password Authentication Mechanism (SPAM)." The primary flaw in the SPAM mechanism is the longer transmission delay associated with the re-authentication process. The "Secure Authentication and Key Establishment Scheme (SAKES)," based on public-key cryptography, is recommended by the authors for devices with limited resources. According to the BAN logic analysis, S6AE is logically conclusive. According to AVISPA's security verification, the suggested scheme is safe from malicious attacks. The performance evaluation shows that S6AE has lower overheads than leading schemes in communication, computational handover, energy, and storage. S6AE can be extended to different security levels using safe cryptographic algorithms. The comparative analysis of exiting solutions is shown in Table 2.3 and Summary of the routing protocol and security issues on IEZN show in Table 2.4

Table 2.3: Comparative Analysis of existing solutions

Ref.	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Ender Yuksel, Nielson [41]	×	×	×	×	×	×	✓	✓	✓	✓	×	✓	×	×
Sturek, Don et al. [97]	×	✓	×	×	×	✓	✓	✓	×	×	×	✓	×	×
Glissa, Ghada and Rachedi et al. [46]	×	✓	×	×	×	✓	✓	✓	×	×	×	×	×	×
Yavari, Mostafa and Safkhani.et.al [117]	×	×	×	×	✓	×	✓	✓	✓	×	✓	✓	×	×
Wang, Weicheng, and Cicala et al. [113]	×	×	×	×	×	×	✓	✓	✓	✓	✓	✓	×	×
Kiayias, Aggelos.et.al [68]	✓	×	×	×	✓	×	✓	✓	✓	×	×	✓	×	×
Lau, Chi Ho and Alan et al. [70]	×	×	×	×	✓	×	✓	✓	×	✓	×	✓	×	×
Ghada Glissa.et.al [44]	×	×	×	×	×	✓	×	✓	✓	×	✓	×	×	×
B. Priyeash, J. Thyagarajan.et.al [19]	✓	✓	×	×	×	✓	×	×	×	×	×	×	×	×
Tanveer, Muhammad.et.al [102]	✓	×	×	×	×	×	✓	✓	×	✓	×	✓	×	×
Zucheng Huang, Feng Yuan.et.al [121]	✓	×	×	×	×	×	✓	✓	×	✓	×	✓	×	×
Dharmini Shreenivas, Shahid Raza.et.al [34]	✓	×	×	×	✓	✓	×	✓	×	✓	×	×	✓	×
Emanuele Toscano, Lucia Lo Bello et al. [40]	×	×	×	✓	×	×	✓	✓	×	×	✓	✓	×	×
Jamal Zbitou. et al.[65]	×	×	×	×	×	✓	×	✓	×	×	×	×	×	✓
Don Sturek, Joseph Reddy et al. [36]	×	×	✓	×	✓	×	×	✓	×	✓	×	×	×	×
Rajesh K et al. [87]	×	×	×	✓	×	×	×	✓	×	×	×	✓	×	×
Hasan, Shah Muhammad Jannatul et al. [52]	✓	×	×	×	×	✓	✓	×	×	×	✓	×	✓	✓
Gupta, Tania, and Bhatia et al. [48]	×	×	×	✓	×	×	×	✓	×	×	×	×	×	✓
Proposed Mechanism	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

A = AODV Routing Protocol, B = RPL Routing Protocol C = RPL-AODV Routing Protocol, D = Routing Attacks, E=Blockchain, F = 6LoWPAN, G = Security, H= Authentication, I = Key Agreement, J = Trust Centre, K = Lightweight Property, L = Access Control, M = Routing Optimization, N= ZigBee Network Key Sniffing Attacks

Table 2.4: Summary of the routing protocol and security issues on IoT-enabled ZigBee networks.

Ref.	A	B	C	D	E	F	G	H	I	J	K	L	M
Ambili K N.et.al [15]	×	✓	×	✓	×	×	×	×	×	×	×	×	×
Anhtuan et al. [7]	×	✓	×	✓	×	×	×	×	×	×	×	×	×
Semih Cakir. et al. [30]	×	✓	×	×	×	✓	×	×	×	×	×	×	×
Chin-Yang.et.al [37]	✓	×	×	✓	×	×	×	×	×	×	×	×	×
John Foley. et al.[43]	×	✓	×	✓	×	×	×	✓	×	×	✓	×	×
S.M.J. Hasan.et.al [91]	✓	×	×	✓	✓	✓	×	×	✓	×	×	✓	×
M. Zhang et al.[16]	×	×	✓	×	×	×	×	×	×	×	×	×	×
M. Napiah.et.al [80]	×	✓	×	✓	×	×	×	✓	×	×	×	×	×
Feng Yuan.et.al [121]	×	✓	×	✓	×	×	×	✓	×	×	×	✓	×
Mina Zaminkar.et.al [119]	×	✓	×	✓	×	×	×	×	×	×	×	×	×
Junqi Duan.et.al [37]	✓	×	×	×	×	×	×	×	×	×	×	×	×
Pavan Pongle.et.al [84]	×	✓	×	×	×	×	×	×	×	×	×	×	×
Rahman et al. [50]	×	×	×	×	×	×	✓	×	×	×	×	×	×
S.A. Abdulzahra et al.[90]	×	×	×	×	×	×	✓	✓	✓	×	×	×	×
Xueyine, Wang et al. [55]	✓	✓	✓	✓	✓	✓	×	✓	✓	×	✓	✓	✓
Ender Yuksel et al.[41]	×	×	×	×	✓	×	✓	×	×	×	✓	✓	✓
Yavari et al.[117]	×	×	×	×	✓	×	✓	×	×	✓	✓	✓	✓
Kiayias et al.[68]	✓	×	×	×	×	×	×	✓	✓	✓	×	✓	✓
Lau, Chi Ho et al.[70]	×	×	×	×	×	×	×	×	×	✓	✓	✓	×
Reen-Cheng Wang et al. [88]	×	×	×	×	×	×	×	×	×	×	✓	✓	✓
Proposed Mechanism	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

A = AODV Routing Protocol, B = RPL Routing Protocol C = RPL-AODV Routing Protocol, D = Specification-Based IDS, E=Signature Based IDS, F = Hybrid IDS, G = ZigBee, H= 6LoWPAN, I = Ipv6, J = Blockchain, K = Security, L = Authentication, M = Key Agreement

Chapter 3

End-To-End Communication Protocol in IoT-enabled ZigBee Network: Investigation and Performance Analysis

The interconnection of IoT-enabled ZigBee devices and the Internet creates smart applications and services, but ZigBee was designed for personal area networks and did not directly communicate with internet end users. The transmission of IPv6 packets over ZigBee-based IEEE 802.15.4 networks using a gateway via the ZigBee coordinator. However, the ZigBee devices cannot handle the IPv6 packets very efficiently [1]. The end-to-end communication between the ZigBee node (802.15.4) and the internet host (IPv6/802.3/802.11) occurs through a gateway, which works as a protocol translator and has a complex structure that incurs communication and computation overhead. This gateway converts the IPv4 packets to IPv6 packets, and the IPv6 packets to ZigBee frames, requiring new specialized hardware and software to handle challenges such as (1) The packet size problem. (2) Increases the complexity of the ZigBee coordinator; (3) Single point of failure: if the coordinator needs to be restarted when it fails, the coordinator can't rejoin the ZigBee network, then the whole network will fail. This motivates us to provide end-to-end communication (ZigBee devices to end users) without relaying devices[59].

This chapter presents the proposed framework for efficient communication between "IoT-enabled ZigBee devices" and Internet Hosts using the "6LoWPAN protocol"[74]. The

proposed protocol integrates IP-based infrastructures with end-to-end ZigBee sensor devices to route IPv6 packets into local IoT-capable ZigBee networks. Specifically, this communication protocol solves challenging state-of-the-art issues such as (1) The packet size problem (2) Reducing the complexity of the coordinator (3) Header size problems in ZigBee devices. However, packets must be routed or forwarded over multiple steps. Additionally, we augmented the proposed work with the RPL-AODV routing protocol, which alludes to the ability to deliver data packets from a ZigBee device to 6BR via multiple hops. We investigated "RPL-AODV routing protocol" and combines the advantages of RPL and AODV routing protocols in ZigBee devices on IoT networks[21][101]. This routing protocol of the IoT network establishes the path from the origin node to the target node on-demand basis using the 6LoWPAN protocol[90]. Additionally, it offers improved routing structures, which provide successful address assignment and data forwarding mechanisms. Finally, the proposed framework ends with performance evaluation with and without integrating the 6LoWPAN Protocol and RPL-AODV routing protocols[5].

3.1 Existing ZigBee Architecture

The ZigBee Alliance supports the independent producers of interoperable 802.15.4 compatible wireless sensors and radios as shown this Figure 3.1. The physical and MAC layers are specified in IEEE 802.15.4. Unlike ZigBee, which specifies the network and application levels[111], regardless of the manufacturer, all ZigBee devices are compatible[23][24].

The ZigBee/802.15.4 wireless network is suitable for various applications, such as Industrial Automation, Energy Automation, Access Control, Heart Rate Monitoring, Home Security, Environmental Management, Lighting Control, Meter Reading, HVAC/Heating control, etc. A combined interface device in the Home Automation profile is an intriguing example of an existing gateway[73].

3.1.1 Overview of 802.15.4 standard

The section describes the overview of the 802.15.4 standard used in ZigBee networks. As shown in Figure 3.2, in the NWK layer, the IPv6 stack is constructed on top of ZigBee, and

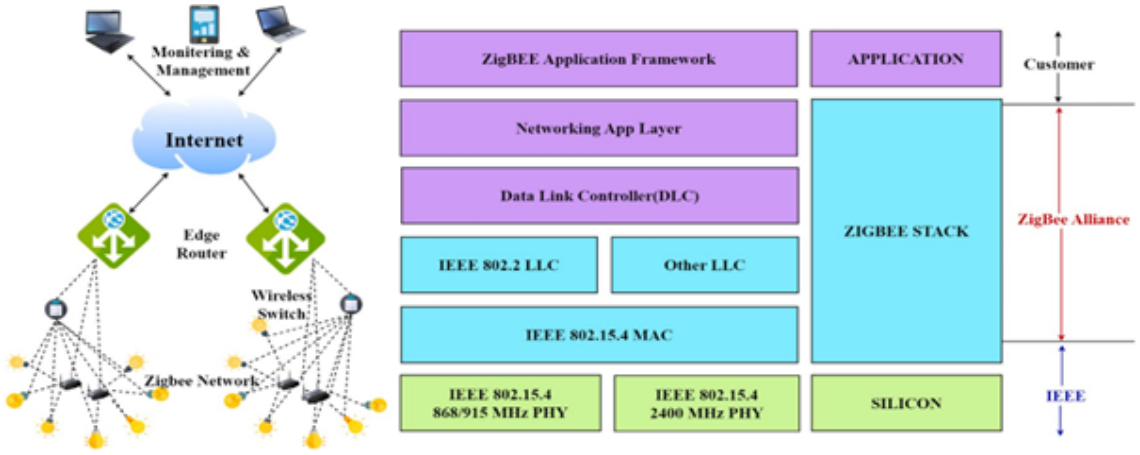


Figure 3.1: ZigBee Stack Architecture

IPv6 addresses are assigned to all ZigBee devices. A ZigBee node (ZigBee/802.15.4) uses a coordinator to communicate through a gateway with an internet end device (IPv6/802.3). When a packet is received from an internet end device, the coordinator will wrap it in a ZigBee NWK and send the ZigBee frame to the 802.15.4 device [85]. A ZigBee gateway provides an easy way to send data between devices on one network and those on another. Gateway has a complex structure, and it will work as a protocol translator. It converts the IPv4 packets to IPv6 packets. It again converts the IPv6 packets to ZigBee networks. IPv6 is transmitted via the IEEE 802.15.4 standard, as seen in figure-3.2. In the NWK layer, the IPv6 stack is constructed on top of ZigBee, and IPv6 addresses are assigned to all ZigBee devices. A ZigBee node (ZigBee/802.15.4) uses a coordinator to communicate through a gateway with an internet end device (IPv6/802.3). When a packet is received from an internet end device, the coordinator will wrap it in a ZigBee NWK and send the ZigBee frame to the 802.15.4 device[114].

3.1.1.1 802.15.4 Standard PHY:

The "Physical Address Layer" (PHY) data service allows data packets known as headers with a preamble (4 octets) and the start of the packet (octet), PHY headers with frame length (octet), and PSDU. As illustrated in figure-3.2 of the IEEE 802.15.4 header format, SHR: The synchronization header includes the preamble and "start of packet delimiter," or SFD. The preamble sequence defines it as 4 bytes, whereas SFD defines it as only one byte. A

synchronization header is used to communicate in all modes that authorize synchronizing and locking into the bit stream [64]. "Physical Header" (PHY): The frame length field in the header indicates how many bytes make up the PPDU [18]. The actual length field is excluded from the frame length. Included in it are concepts of minimum physical distance. The maximum frame length is 127 bits, And the frame length is 7 bits. It is engaged and set to zero, the most important part of the frame length. "Physical Service Data Unit" (PSDU): The media access control frames of the MPDU are acquired by the physical as a PSDU, which is now the biological payload[58].

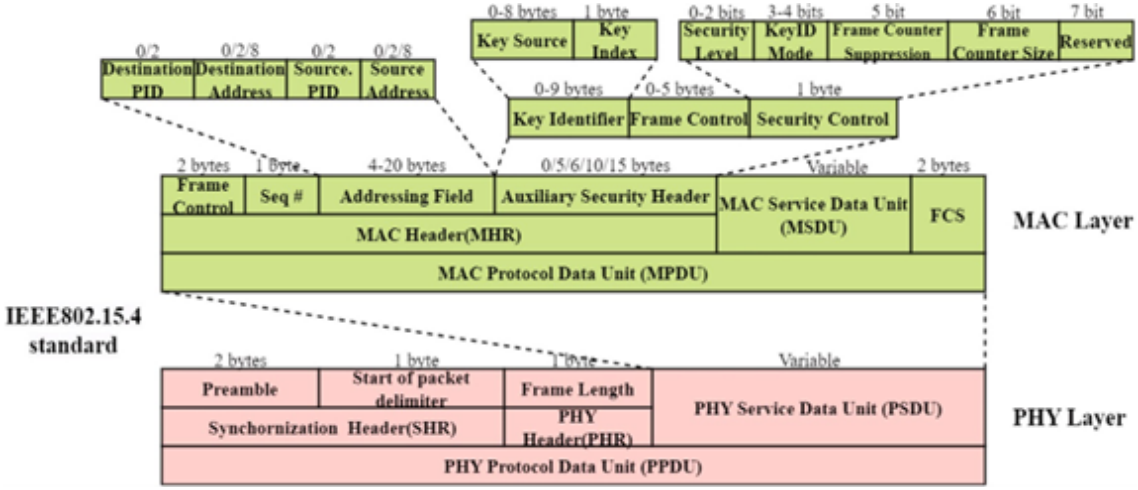


Figure 3.2: Frame format of IEEE802.15.4.

3.1.1.2 802.15.4 Standard MAC:

The "Medium Access Control" (MAC) layer interfaces between the physical and adaptation layers. The sub-layer performs two functions. The MAC data service and the MAC management service interface with the "MAC sublayer management entity" (MLME). The MAC data service facilitates the transmission and receipt of MPDU over the PHY data service. The MAC is responsible for developing beacons and syncing the device with them (in a beacon-enabled network). It defines how different types of 802.15.4 radios operate in identical areas. The two functions of these layers are data handling and data management. "Data Request" and "Data Confirm" are examples of data handling functions. The MAC layer adds a destination address and sends alternatives for departing data frames. The data

is formatted into the relevant MAC header. The physical header's frame length is added when the ZigBee network layer invokes the "data request" function. The data frame is now ready to be sent. The "data confirm" function's objective is to communicate the status of the data that has been transferred. When the transmission frames are exceeded, or there is no response to the received information, it sends a fail group[17]. Beacon management and generation Carrier Sense Multiple with Obstacle Detection is now available. Time slot allocation and control are guaranteed. The data frame and acknowledgment frame formats As shown in figure-3.2. MAC Frame Format: There are four alternative Mac frame formats for medium access control (e.g., data, beacon, acknowledge, and command frames). There are three types of "MAC Protocol Data Units" (MPDUs): MHR (header), MSDU (service data unit), and MAC footer (MFR). "MAC Header (MHR): MAC header contains "Frame Control Field" (FCF), Sequence Number (SN), and "Frame Check Sequence" (FCS), along with Addressing fields and an Auxiliary Security Header." Frame Control Field (FCF) is defined with two octets, Sequence Number (SN) defines only one byte, Frame Check Sequence (FCS) defines two octets, and Addressing Fields and Security Header define more than one byte[100].

3.1.2 Mesh Topology in ZigBee Network:

Unlike traditional wireless networks, which mainly use point-to-multipoint or point-to-point topologies such as star, ring, bus, distributed, or tree structures, the ZigBee Network uses a mesh network topology that is wirelessly connected in a multi-hop fashion with the coordinator[1]. The mesh network topology will find routes to ensure the packets reach their destination.

3.1.2.1 ZigBee Device Types:

ZigBee defines three devices: coordinator, router, and end device, as shown in Figure 3.3.

1. **Coordinator:** A single coordinator device is always present in ZigBee networks. This device begins the network by picking a channel and PAN ID. Assigns addresses to routers and end devices, allowing them to join the network. Assists with data rout-

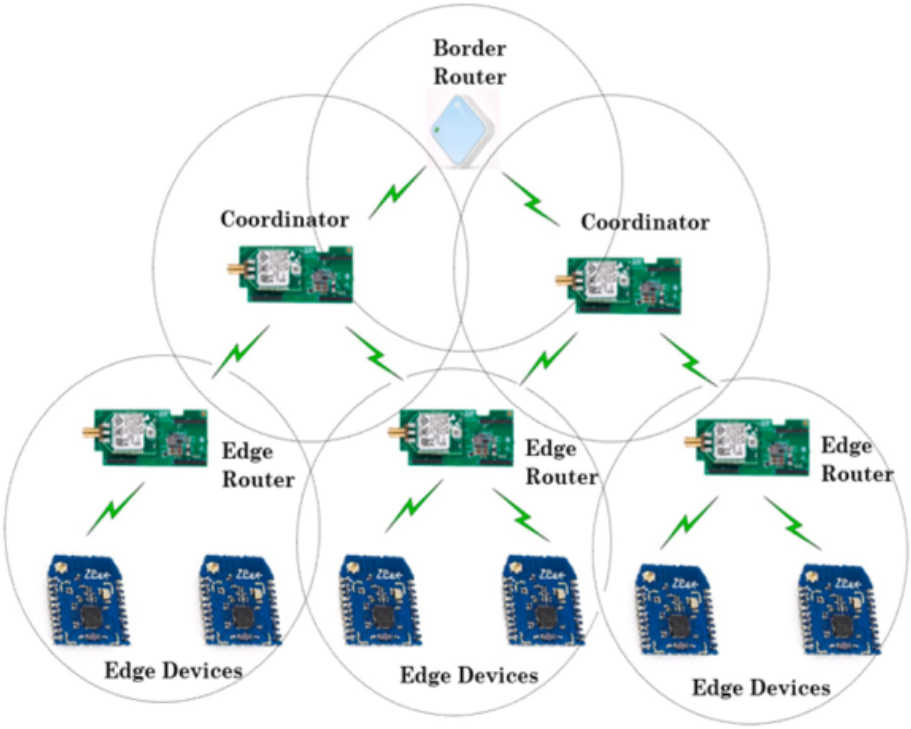


Figure 3.3: ZigBee network: Mesh topology.

ing. Wireless data packets are buffered for children sleeping with their end devices. Oversees the various functions that define, safeguard, and maintain the network's health. This gadget cannot sleep and must be turned on at all times[78].

2. **Router:** A router is a ZigBee node with all of the features. It can connect to existing networks and send, receive, and route data. Routing entails serving as a relay for communications between devices too far away to communicate independently. Wireless data packets can be buffered for sleeping, end-device children. Other routers and end devices may be able to join the network. It is unable to sleep and must be kept awake at all times. A network can contain numerous router devices[91].

3. **End device:** An end device is a router that has been scaled down. This device can connect to existing networks and send and receive data but cannot communicate with other devices. Other devices are unable to join the network. It requires a router or the coordinator to be its parent device. It uses less costly hardware and can power itself down occasionally to save energy by momentarily entering a non-responsive sleep state. When end devices are sleeping, the parent assists them in connecting to

the network and saves messages for them. End devices on ZigBee networks can be any number. A grid can consist of just one coordinator, a few end devices, and no routers[18].

3.2 Limitations of ZigBeeNetwork

This section presents the limitations of the ZigBee Network. Generally, the communication between the ZigBee node (ZigBee/802.15.4) and any Internet host (802.3) is achieved using a gateway through the ZigBee coordinator, as shown in Figure 3.4. When a packet arrives from the Internet host, the gateway encapsulates it and forwards it to the ZigBee network. The ZigBee coordinator will decapsulate the received frame and deliver the target ZigBee end device. However, some challenging issues of IoT-enabled ZigBee devices are discussed below:

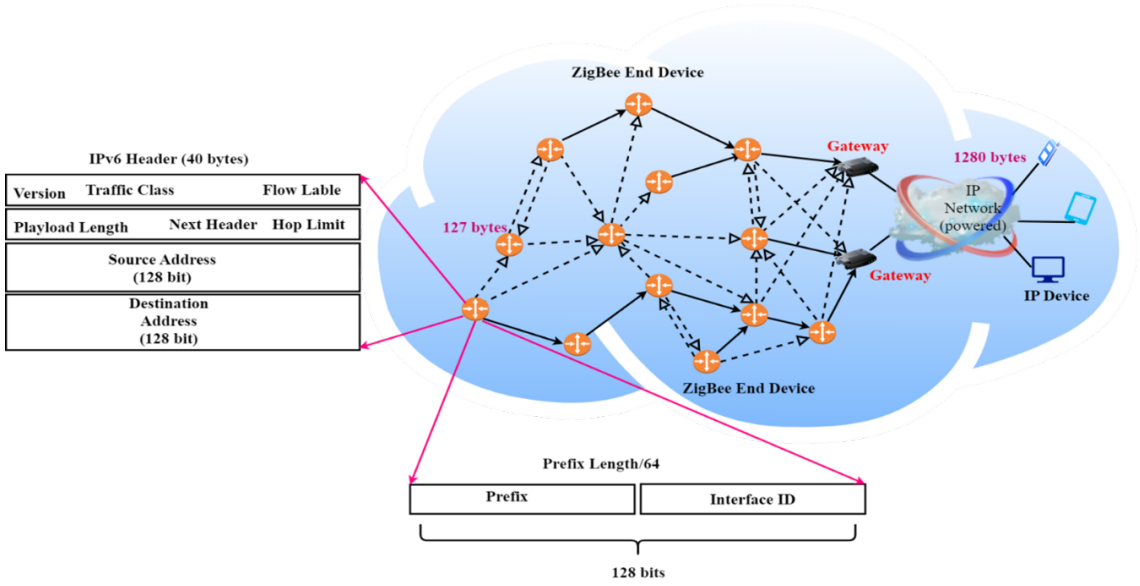


Figure 3.4: ZigBee Network using Traditional Gateway Approach.

1. The end-to-end communication between ZigBee nodes (802.15.4) and internet hosts (IPv6/802.3/802.11) occurs through a gateway that has a complex structure and needs to perform application layer protocol translations, neighbor discovery, routing structures, address assignment, and data forwarding, which incurs communication and computation overhead on the coordinator and the gateway[31].

2. A coordinator controls a ZigBee network and needs to handle network structures such as star topology, tree topology, and mesh topology.

3. New gateways are required with hardware and software

4. The packet size issue is the fundamental issue with IPv6 over ZigBee. ZigBee devices suffer from a header size problem. ZigBee devices cannot handle IPv6 packets, allowing for a maximum packet size of 1280 bytes; they can only handle data units of 127 bytes.

5. If the coordinator needs to be restarted when it fails, it is not possible to the coordinator to rejoin the ZigBee network because all the access/controls lie with the coordinator itself, and that is not only present in the network, so the whole network will fail, which needs to Single Point of failure[29].

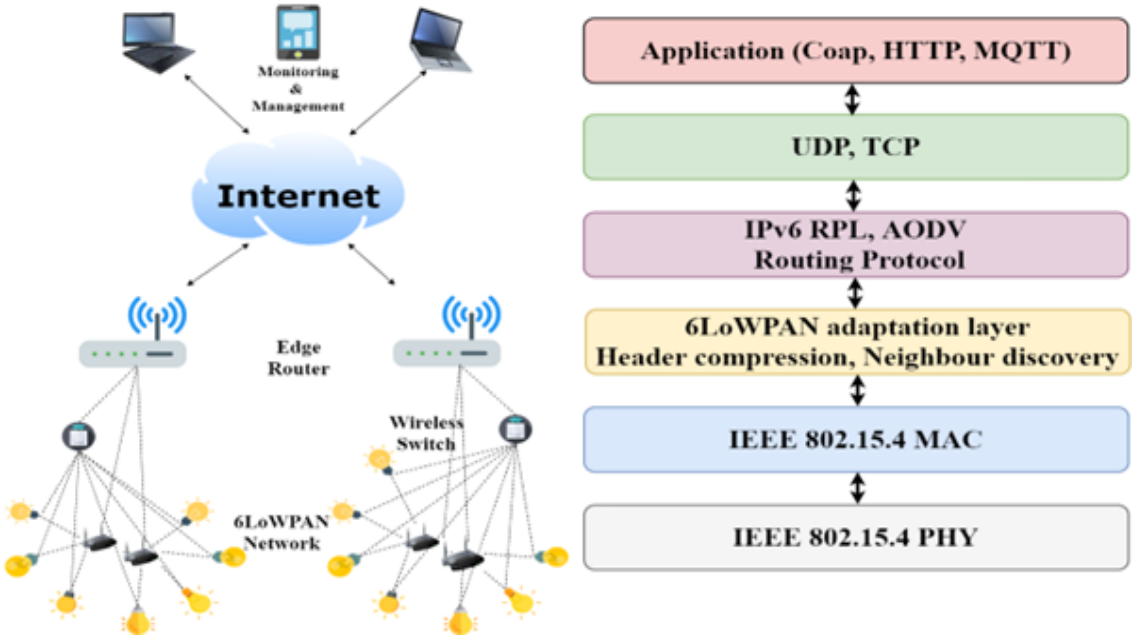


Figure 3.5: 6LoWPAN Layer in IoT layered Architecture.

3.3 Proposed Work

This section presents the protocol architecture of IoT-enabled ZigBee networks. The ZigBee Network supports low-cost, low-power protocols that allow communication between

the edges and application profiles. Figure 3.5 shows the protocol architecture of IoT-enabled ZigBee networks, consisting of the IEEE 802.15.4 standard with PHY, MAC protocols, adaptation protocols (6LoWPAN), and network protocols IPv6 and RPL. AODV

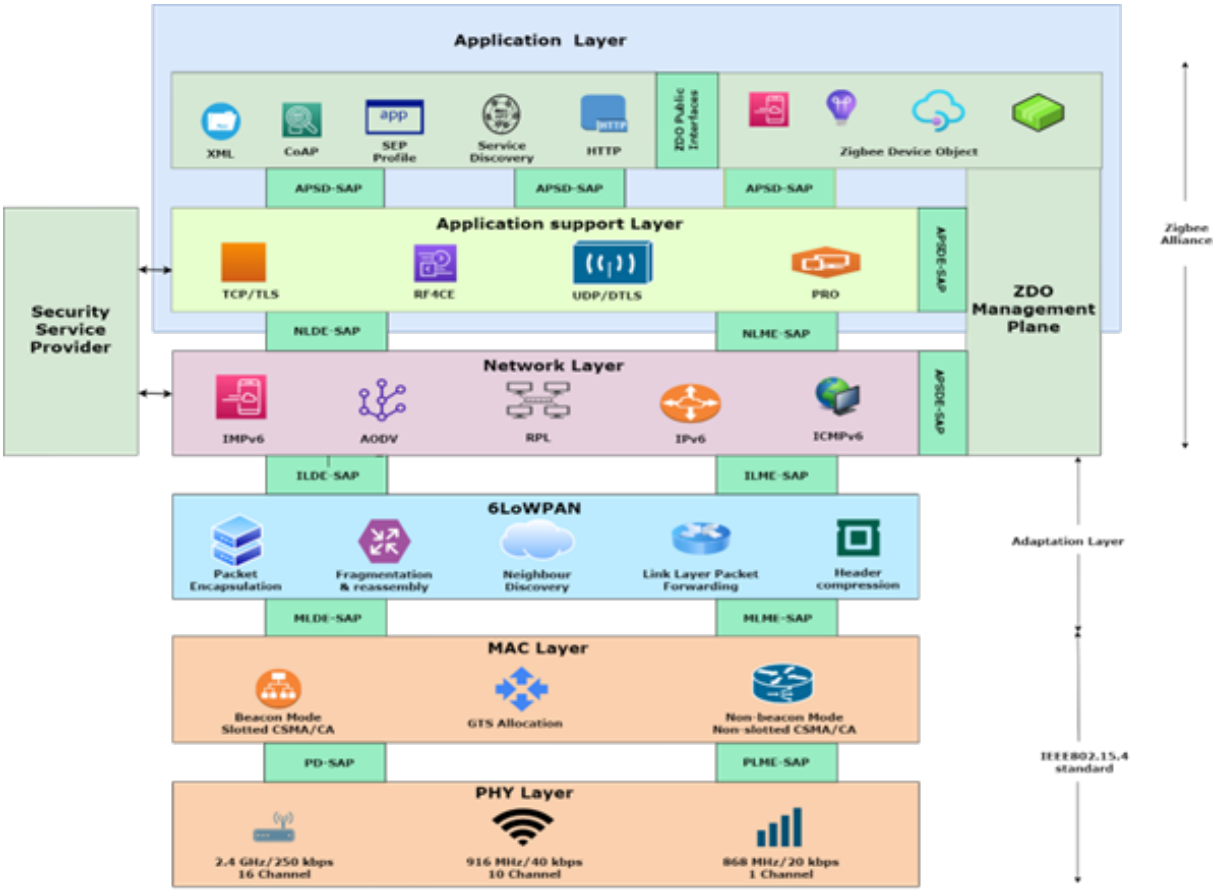


Figure 3.6: Protocol Architecture of IoT-enabled ZigBee Networks

routing protocols, security protocols, and application protocols—starting from the bottom of Figure 3.5 ZigBee adheres to the WPAN IEEE 802.15.4 standard that supports smart energy, home automation, telecom applications, plant monitoring, smart commercial buildings, health care, etc. The IEEE 802.15.4 standard uses PHY and MAC layers. The PHY is responsible for sending and receiving packets through physical media. This layer also provides services such as radio transceiver activation and deactivation, energy detection, connection quality indication, channel selection, and clear channel evaluation to the upper layer. The PHY layer works in two frequency bands, 2.4 GHz and 868–916 MHz, based on Direct Sequence Spread Spectrum. For 2.4 GHz, 40 kbps is for 916 MHz, and 20 kbps

is for 868 MHz. These bands offer data speeds of 250 kbps, 40 kbps, and 20 kbps, respectively. There are 27 channels accessible over three unlicensed bands: 16 channels in the 2.4 GHz band, one in the 868.3 MHz band, and ten channels in the 902–928 MHz range. Low data rates at low frequencies result in lesser propagation losses and a more excellent range of operation.

On the other hand, a greater rate results in faster throughput, shorter latency, and a lower duty cycle. The IEEE 802.15.4 standard is also used in the MAC layer to define the CSMA-CA or slotted CSMA-CA communication links. The MAC layer provides three possible channel access mechanisms: (i) beacon mode, (ii) non-beacon mode, and (iii) allocation of GST. To achieve reliable transmission, devices rely on the acknowledgment in a beacon-less way to RPL-AODV routing protocol supports two routing modes: storage and monitoring. A routing table and a neighbor table are stored on all devices in the IoT-enabled ZigBee networks. The routing table and the neighbor table are used to find devices' routes and keep track of a node's immediate neighbors. The source device sends information to the edge router, which searches its routing table for the whole path and adds it to the packet's destinations.

3.3.1 Protocol Architecture of IoT-enabled ZigBee Networks.

In this section, we presented the protocol architecture of IoT-enabled ZigBee networks. The ZigBee Network supports low-cost, low-power protocols that allow communication between the edges and application profiles. Figure 3.6 shows the protocol architecture of IoT-enabled ZigBee networks, consisting of the IEEE 802.15.4 standard with PHY, MAC protocols, adaptation protocols (6LoWPAN), and network protocols IPv6 and RPL. AODV routing protocols, security protocols, and application protocols—starting from the bottom of Figure 3.7. ZigBee adheres to the WPAN IEEE 802.15.4 standard that supports smart energy, home automation, telecom applications, plant monitoring, smart commercial buildings, health care, etc. The IEEE 802.15.4 standard uses PHY and MAC layers. The PHY is responsible for sending and receiving packets through physical media. This layer also provides services such as radio transceiver activation and deactivation, energy detection,

connection quality indication, channel selection, and clear channel evaluation to the upper layer. The PHY layer works in two frequency bands, 2.4 GHz and 868–916 MHz, based on Direct Sequence Spread Spectrum. For 2.4 GHz, 40 kbps is for 916 MHz, and 20 kbps is for 868 MHz. These bands offer data speeds of 250 kbps, 40 kbps, and 20 kbps, respectively. There are 27 channels accessible over three unlicensed bands: 16 channels in the 2.4 GHz band, one in the 868.3 MHz band, and ten channels in the 902–928 MHz range. Low data rates at low frequencies result in lesser propagation losses and a greater range of operation. On the other hand, a greater rate results in faster throughput, shorter latency, and a lower duty cycle.

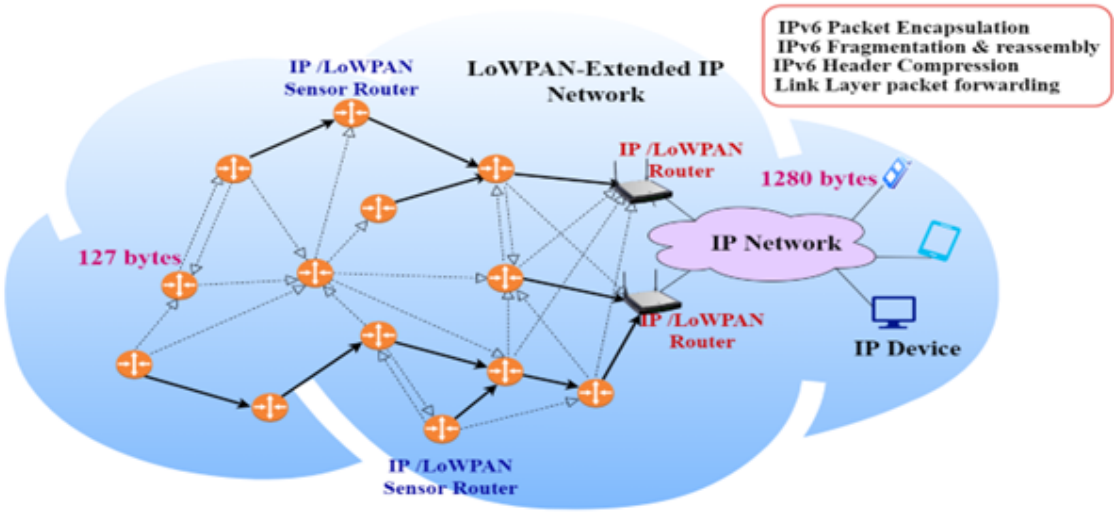


Figure 3.7: Interfacing 6LoWPAN in IoT-enabled ZigBee Network.

The IEEE 802.15.4 standard is also used in the MAC layer to define the CSMA-CA or slotted CSMA-CA communication links. The MAC layer provides three possible channel access mechanisms: (i) beacon mode, (ii) non-beacon mode, and (iii) allocation of GST. To achieve reliable transmission, devices rely on the acknowledgment in a beacon-less way to attain power-saving solutions. ZigBee networks employ beacon-enabled channel access to improve latency and provide longer sleep durations. ZigBee routers periodically emit beacons in beacon-enabled networks to announce their existence. The coordinator's transmitted beacon frames act as a clock. It is compatible with the slotted transmission technique. The beacon interval can range from 15 ms to 252 s. Between beacon intervals,

the nodes can slumber, reducing their duty cycles. It not only lowers latency but also increases battery life. ZigBee end devices synchronize their duty cycles to only wake up when a beacon activates. The primary MAC frame structure is discussed in the background chapter. This frame structure ensures that data is transmitted reliably in conjunction with message acknowledgment. To improve latency in a large WMN, nodes rely on the beacon architectures specified. As shown in Figure 3.8, a ZigBee MAC frame comprises five fields. one of which is the payload. The first field is a frame control with a length of 2 bytes that specifies the kind of MAC frame broadcast. The frame sequence number is displayed in the subsequent 1-byte field.

The address field is in the third field. It defines the address field format and manages acknowledgment. The address field's size ranges from 0 to 20 bytes. The payload size is limited to 127 bytes. A 2-byte CRC frame check sequence makes up the last field. Long and short addressing is specified by the IEEE 802.15.4 using 64-bit and 8-bit addresses, respectively. Short addressing is a quick addressing system mainly used to assign ad hoc network IDs within a network with 255 nodes and for personal area networking. At the same time, the extended addressing used for network size might be as large as 264, which is generally more than adequate for constructing a smart environment. The following protocol stack layer is the 6LoWPAN protocol, an adaptation layer that provides services to the internet layers. This protocol transfers the data from the end devices via the MAC and PHY layers to the upper layer. The IEEE 802.15.4 standard, primarily intended for long-lived application domains requiring many low-cost nodes, is reflected in IPv6 as an advancement in Internet connectivity technology. Because of these limitations, the maximum throughput for WPAN connections and the microcontrollers they connect to is 250 kbps. When bit-error rates are non-negligible, the frame length is limited to 128 bytes to ensure low packet error rates and match microcontrollers' limited buffering capabilities.

Some of the services provided by the 6LoWPAN protocol are header compression, fragmentation and reassembly, stateless auto-configuration, and neighbor discovery in the upper layer. The header compression uses standard fields to reduce the 8-byte UDP and 40-byte IPv6 headers. They are omitted when header fields can be extracted from the link layer. A detailed description is discussed in the chapter. While IEEE 802.15.4 can only

accept a maximum frame length of 127 bytes, the fragment and reassembly are mainly employed to have a greater payload because the data connection does not match the MTU of IPv6, which is 1280 bytes. The IPv6 neighbor discovery (ND) to find neighbors, retain reach-ability information, create default routes, and transmit configuration parameters. The RS message comprises the network's IPv6 prefix, among other things. These messages are sent out regularly by all routers in the network. The link-local unicast address must be created for an end device before it can join a 6LoWPAN network. This address is sent to other subnet members in an NS message to see if it is already used. Suppose it does not get a NA message within a specific time. The Internet layer uses the predominant IPv6 protocol,

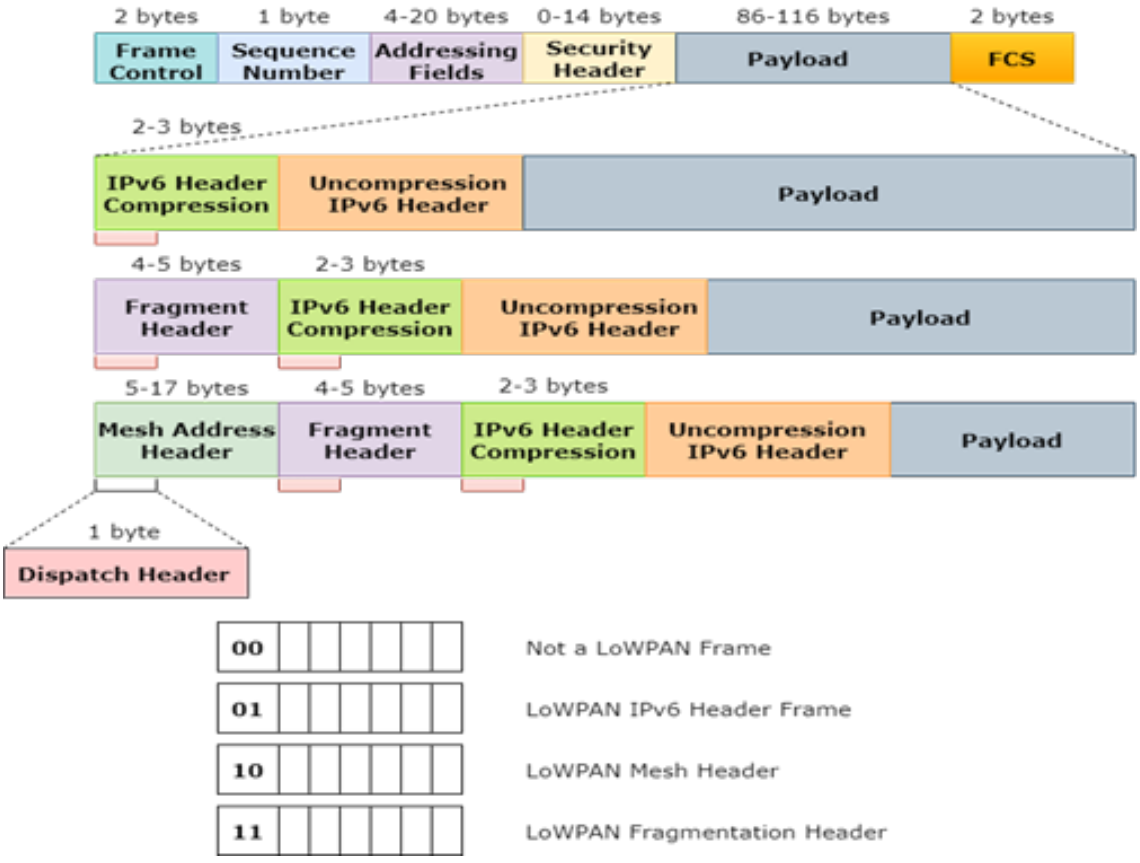


Figure 3.8: Adaptation 6LoWPAN layer Functionalities

the IPv4 successor, tolerating for decades the growth of the Internet. IPv6 increases the IP address space from 32 to 128 bits to compensate for limited unallocated address space and assumes that networked appliances and instruments will considerably outnumber traditional end devices. The IPv6 protocol boosts the minimum MTU requirement from 576 to

1280 bytes in response to increased network capacity. IPv6 uses fragmentation at endpoints rather than intermediary routers to make routers simpler and faster. IPv6 contains scoped multicast as a key component of its architecture to boost protocol efficiency and reduce the requirement for ad hoc link-level services to bootstrap a subnet. Link-local scoped multicast is used by Neighbor Discovery (ND) and other essential IPv6 components for address resolution, duplicate address detection (DAD), and router discovery. By enabling nodes to assign valid addresses, stateless address auto configuration (SAA) makes it easier to configure and maintain IPv6 devices.

Finally, the application layer will have the specification for some application profiles using application (APL) layers to place the responsibility for application development on the user. The application's profile defines the communication method broadcast over the air. Devices having the same application profiles can communicate with one another. The device designer provides the actual application code. The 6LoWPAN protocol allows effective communication between IoT-enabled ZigBee devices and IPv6 nodes.

3.3.2 Integrating the Network Adaptation Layer in the IoT-enabled ZigBee Environment.

The adaptation layer provides services to the network or internet layer by taking the data from the end devices. As shown in Figure 3.9, IPv6 requires a minimum transmission unit of 1280 octets, whereas IEEE 802.15.4 only permits a maximum ZigBee MAC frame size of 127 bytes, including 25 bytes of frame overhead and only 102 bytes for the payload. The link layer enhances the MAC frame with an Auxiliary Security Header for security purposes. In the worst situation, the issue worsens, and just 81 bytes are left for the IPv6 packet. As a result, an IPv6 packet will not fit into a ZigBee frame. Furthermore, the upper layers have just 41 bytes because an IPv6 packet's IPv6 header is 40 bytes long. The User Datagram Protocol (UDP) header is 8 bytes long. The Transmission Control Protocol (TCP), which is 20 bytes long and inserted at the transport layer, is the only two bytes the IPv6 header reserves for application data. The adaptation layer uses the 6LoWPAN protocol (WSN) to connect with all wireless sensor nodes. Therefore, this protocol is

suitable for IP-based, low-power, and low-cost devices and seamlessly binds any device to the Internet. Further, it also provides interoperability between any link-layer technologies supporting IPv6. The 6LoWPAN protocol offers end-to-end communication between IoT-enabled ZigBee devices and the Internet host. Once the 6LoWPAN protocol receives the query from the internet host or ends the user, it performs the three primary services. (i) Fragmentation and reassembly are used to meet the IPv6 minimum MTU requirements. (ii) Header compression: removing fields that may be deduced from link-level information or based on basic shared context assumptions. (iii) Link-layer forwarding is supported to transport IPv6 datagrams over many hops.

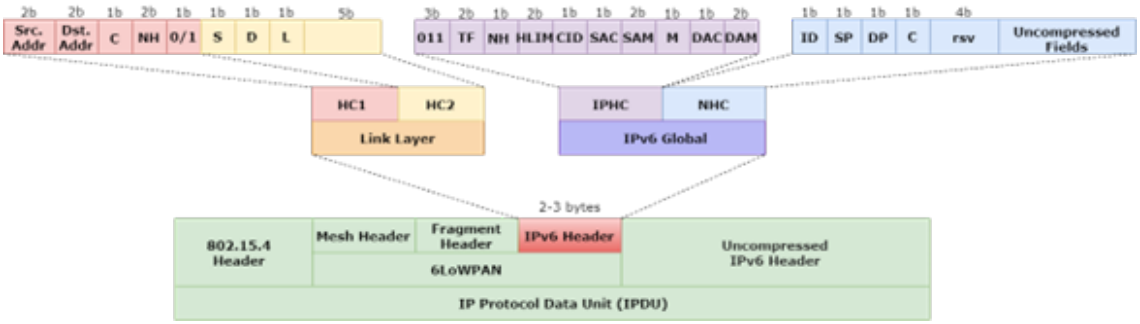


Figure 3.9: 6LoWPAN Header Compression

3.3.2.1 Header Compression of IoT-enabled ZigBee Packet Header

The gateways and edge routers provide end-to-end communication in IoT-enabled ZigBee devices, which poses several challenges, such as end-to-end communication between two endpoints that are far from each other, requiring multi-hop communication. It needs compression and decompression on each hop. The routing protocols employ rerouting (e.g., RPL) to gain receiver diversity, which demands state movement and dramatically affects compression efficiency and incurs overhead in networks with several hops and intermittent transmissions that are continually changing. We used 6LoWPAN protocols that use stateless and shared-context compression, which takes no state and enables routing protocols to identify routes without sacrificing compression ratio dynamically. The 6LoWPAN protocol performs header information via stateless or shared-context compression. The UDP and IP headers may be condensed to a few bytes, as shown in Figure 3.9. The 6LoWPAN employs

encapsulated header stacking and has three self-contained sub-headers (Figure 3.9).

6LOWPAN HC1 and HC2: According to Figure 3.9, the HC1 specifies header compression for such an IP header. It uses the Traffic Class and Flow Label default settings and IP Version (v6) (both are zero). A link layer or fragmentation header can be used to determine the payload length. The interface IDs for the source and destination IPv6 addresses are inferred from the link-layer addresses. The following header field is 2 bits long and shows whether the connection is UDP, ICMP, or TCP. The entire value is in line because the hop limit is not compressed. The HC2 defines the UDP header compression standard. The length, source port, and destination port fields can be shortened. The IPv6 header can be used to estimate UDP length. Four bits can represent the frequently used port numbers F0B0 to F0BF. As the UDP checksum is not compressed, it is delivered in its entirety.

6LoWPAN IPHC: Figure 3.9 also shows "IP header compression" (IPHC) and "next header compression" (NHC) for compressing IPv6 header and UDP header, respectively. IPHC is a global IPv6 address compression technique that reduces communication overhead across nodes separated by more than one IP hop. It includes compression based on the shared states within contexts. If traffic and flow labels are not null fields, a mechanism is defined to compress. IPHC uses the first eight rightmost bits of dispatch type to specify the compressed field of the IPv6 header, independent of addressing compression. IPHC follows the dispatch type, limiting how compact the source and destination addresses are. An additional octet called context identifier extension when communicating with a global address. The destination address is represented by the last four rightmost bits, whereas the stated context and source address are represented by the first four leftmost bits. The Ipv6 address is 16 octets long, which can significantly improve compression efficiency. IIDs for IPv6 addresses are either 16-bit or 64-bit short IEEE 802.15.4 addresses. In link-local communication, the best compression of the IPv6 header (40 bytes) that can be accomplished is two octets. The IPv6 header can be compressed to 7 octets when passing via several IP hops using IPHC.

6LoWPAN NHC: The NHC compresses any subsequent arbitrary header and employs a variable-length identifier to designate the following heading. When compressing UDP headers, the checksum may be deleted if Message Integrity Check (MIC) or another upper-

layer security mechanism is used. The port numbers between F00 and F0FF are compressed. It is identified by the initial 5 bits of a UDP header. If C = 1, the checksum is compressed. Figure 3.9, mentioned above, depicts the NHC format. NHC-IMP offers the following port compression options: When both port numbers are between F000 and F0FF, NHC-IMP compresses one, whereas NHC lowers one to 8 bits. Compared to NHC, which needs 16 bits to be communicated in the line, NHC-IMP reduces well-known port numbers from 0–255 to 8 bits. Under some circumstances, IPHC-IMP can reduce multicast addresses to 48, 32, 8, or 0 bits. In IPHC-IMP, the all-nodes and all-routers multicast addresses can be entirely ignored, while the lowermost 8 bits of the talks must be sent inline in IPHC. In summary, the IPv6 header may be minimized to only (2) two bytes while connecting both ZigBee devices inside the same 6LoWPAN network utilizing link-local addresses. When communicating with a ZigBee device outside the 6LoWPAN network, the IPv6 header can be reduced to 12 bytes if the externally known network's prefix is given. Using the header compression technique can reduce the header size, resolving the header size problem.

3.3.2.2 Fragmentation and Reassembly in IoT-enabled ZigBee Network

The maximum frame length of the 802.15.4 data link is 127 bytes, which does not exceed the MTU of IPv6, which is 1280 bytes. When the payload is too large to fit into a single IEEE 802.15.4 frame, this 6LoWPAN protocol enables fragmentation and reassembly. The amount of data transmission in the single IEEE 802.15.4 payload space is too low. Does the fragmentation process divide a single IPv6 box into smaller fragments, each with its fragmentation header, as shown in Figure 3.10. The fragmentation sequence differs depending on the type of route used. Each stage of the route-over network requires the reassembling of data packets. During reassembly, the additional information sent to data packets is deleted, and the packets' IPv6 structure is restored to its original IPv6 structure. However, fragmentation affects a device's battery life and should be prevented for as long as possible. As a result, it is vital to keep the payload minimal and use header compression. Mesh addressing, fragmentation, and header compression are three sub-header techniques used by the 6LoWPAN. A mesh's layer two (data link) forwarding is made more accessible

by addressing. IPv6 MTU transport is made easier by the fragmentation header.

Fragmentation Header: As shown in Figure 3.10, Datagram size (11 bits), fragmentation type (5 bits), and datagram tag (16 bits) information may be found on the first fragment of a fragmentation header. The first eight leftmost bits are dispatch type; subsequent fragments include the datagram offset (8-bit) area. An IPv6 packet that has not been fragmented has a datagram size of one unfragmented packet. The datagram tag is used to identify the datagram of the particular fragment. The datagram offset is only included in subsequent pieces and specifies that the element offset from the original packet is multiplied by eight octets. The important characteristic of the 6LoWPAN fragmentation header is that fragments must not arrive in the same order when they are fragmented.

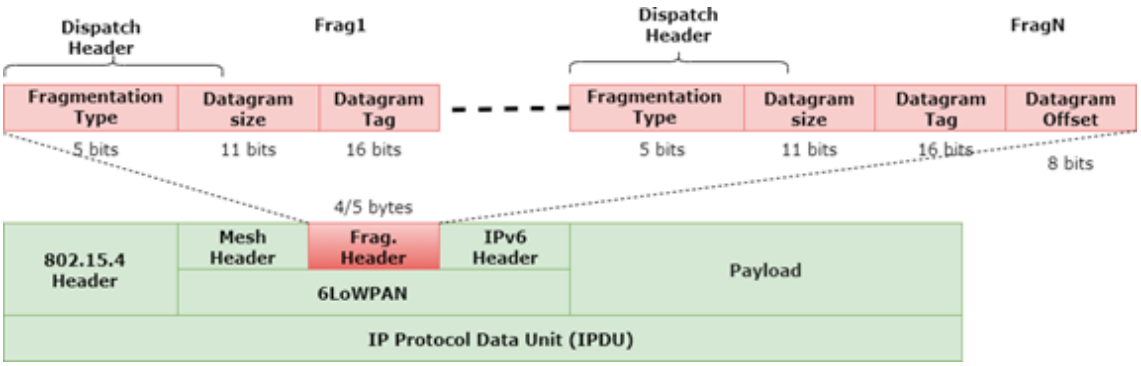


Figure 3.10: 6LoWPAN Fragmentation Header

Mesh Header Compression: As shown in Figure 3.11, the mesh addressing header dispatch type contains '10' (2 bits). The mesh header defines the dispatch type, source, and destination addresses. The V and F bits indicate two 802.15.4 formats for source and destination addresses with 2 to 8 octets. If V is 0, 64-bit extended lessons from the source, and V is 1, short 16-bit addresses. If F is 0, 64-bit advanced addresses of the destination address, and F is 1, a temporary 16-bit address. The next hop receives the packet, checks the routing table for the following hop, decrements the hop count each time, and then sends the data packet with two octets to its next ball and destination address.

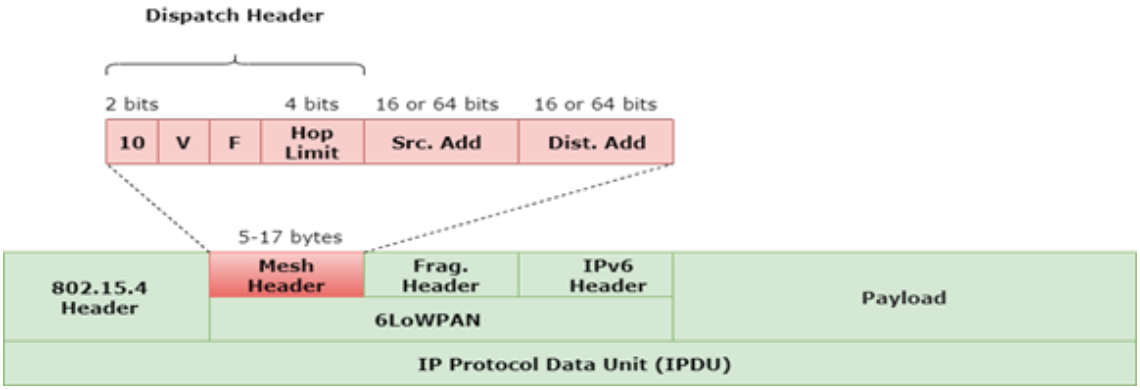


Figure 3.11: 6LoWPAN Mesh Header

3.3.3 Integrating the RPL-AODV Routing Protocol into an IoT-enabled ZigBee Network.

The 6BR connects IoT-enabled ZigBee networks to the Internet. This 6BR integrates IP-based infrastructures with ZigBee sensor devices to route IPv6 packets into regional IoT-enabled ZigBee networks. However, packets must be routed or forwarded via multiple steps. This can be achieved using the mesh address header. This mesh address header has three fields: the hop limit, the source address, and the destination address, as shown in Figure 3.12. The hop limit option restricts the number of hops used for forwarding. This parameter is decremented for each hop. When the count approaches zero, the packet is discarded. The source and destination address parameters specify the ZigBee IP endpoints. These endpoints also contain IEEE 802.15.4 addresses, which can be short or lengthy depending on the requirements of the IEEE 802.15.4 standard. The capability to send data packets from one ZigBee device to 6BR across a number of hops is referred to as the RPL-AODV routing protocol.

3.3.3.1 Overview of RPL-AODV Routing Protocol:

The "Routing Protocol for Low Power and Lossy Networks (RPL)" is the IPv6-based distance vector routing protocol for "IoT Enabled ZigBee Networks" (IEZN) that supports "multipoint-to-point", "point-to-multipoint", and "point-to-point" traffic flows from the root in the "destination-oriented directed acyclic Graph (DODAG)". This traffic will be happen-

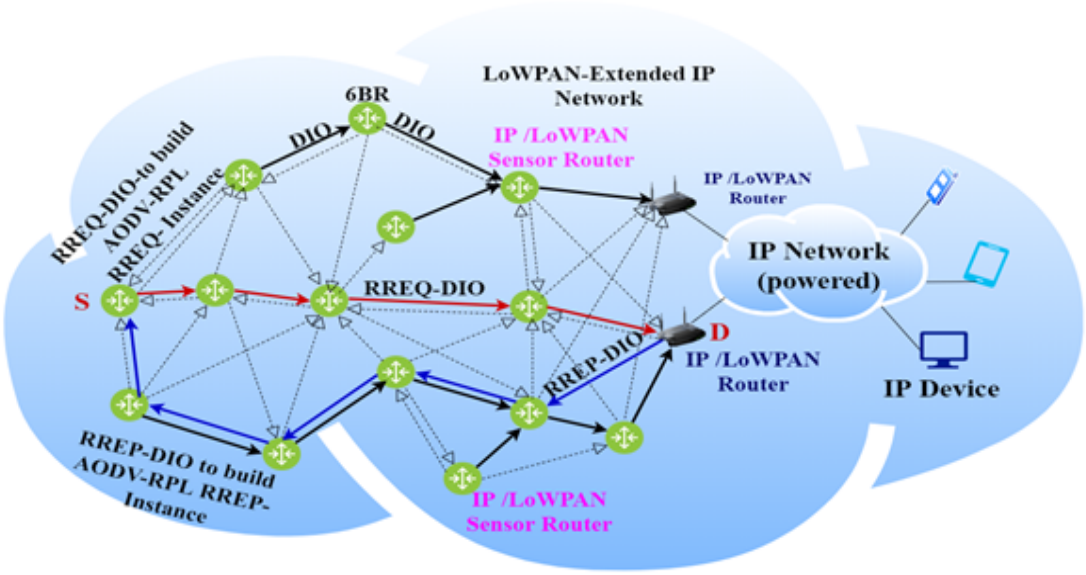


Figure 3.12: RPL-AODV Protocol into Routing Layer on ZigBee

ing between different routers within the DODAG. However, the routers do not contain the information of another network router. Therefore, the traffic flows information in these networks is operated in two modes. One is the non-storing mode and the storing mode. In the non-storing mode, the root of the DODAG will receive every data packet from the routers or the edge nodes. While in the storing mode, the common predecessor node will receive the data packets. But, the data packets need to flow over the longer path, which results in congestion at the root level of the DODAG.

In the RPL network, the originator acts as a local root in the temporary destination-oriented DODAG that introduces the DIO control message to discover a better path. Once the neighbor router receives the DIO message from the originator node, it adds its IPv6 addresses and then multicast these DIO messages to the target node. The process is encapsulated using point-to-point route discovery P2P-RDO options in DODAG, either hop-by-hop or source routing mode. However, both the hop-by-hop and source routing mode adds the extra overhead of the address vector that restricts satisfying the objective function constraint. The RPL-AODV protocol uses point-to-point route discovery features of the RPL protocol with different operation modes. To achieve high route diversity, the RPL-AODV protocol uses two other multicast messages to find the possible asymmetric routes.

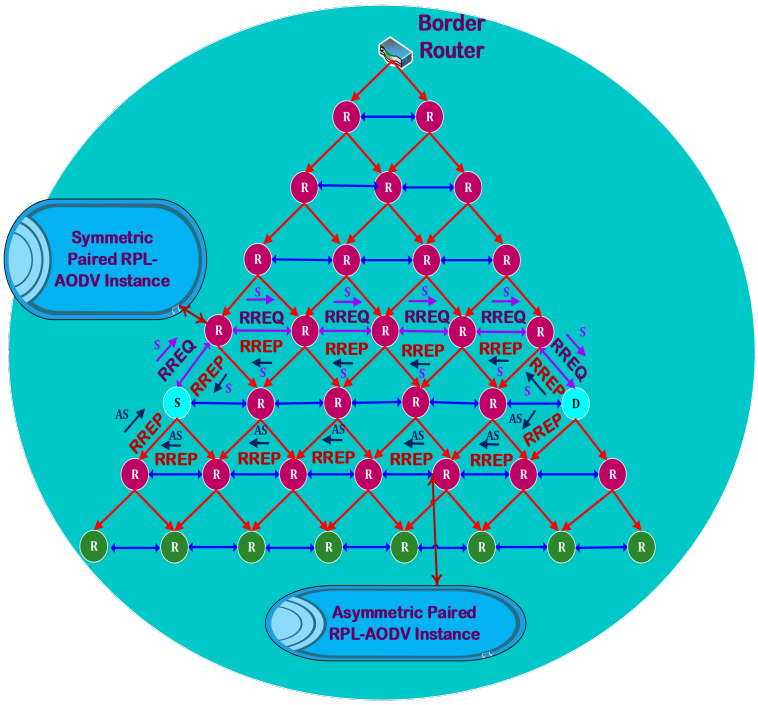


Figure 3.13: Symmetric and Asymmetric Paired Instances in RPL-AODV Protocol

RPL-AODV eliminates the need to address overhead in the case of hop-by-hop mode. Restrictive IEZN networks can benefit from a significant reduction in control packet size.

3.3.3.2 Modeling of RPL-AODV Routing Protocol for IoT Enabled ZigBee Networks (IEZN):

This section proposes an RPL-AODV routing protocol in low power and lossy network (IEZN) that only establishes the path from the origin node to the target node on-demand basis. The route discovery process in the RPL-AODV protocol is reactive when the source node wishes to transmit a data packet to a destination node for which there is no route or an existing route that does not satisfy the requirement. This route discovery process of the RPL-AODV protocol achieves high route diversity with the help of asymmetric communication using bidirectional links for finding the route from the origin node to the target node and from the target node to the origin node. Also, it eliminates the constraints of traversing a common predecessor node, which is there in the original RPL protocol. Further, RPL-AODV facilitates route discovery for symmetric DODAG communication, as shown in Figure 3.13. In discovering the routes, the RPL-AODV uses a route discovery

process containing two control messages, route request (RREQ) and route reply (RREP). The discovery of routes is achieved by forming a temporary DODAG at the origin node. The mode of operation (MoP) in RPL-AODV is the basis for the construction of the paired DODAG Instances. The target node receives the RREQ control message instance from the origin node, and the origin node receives the RREP control message instance back. The DODAG Information Object (DIO), which aids intermediate routers in joining the DODAG instance, is used to compute the rank. The route found in the RREP instance serves as the basis for both the transmission of data from the origin node to the target node and the communication of acknowledgment from the target node to the origin node.

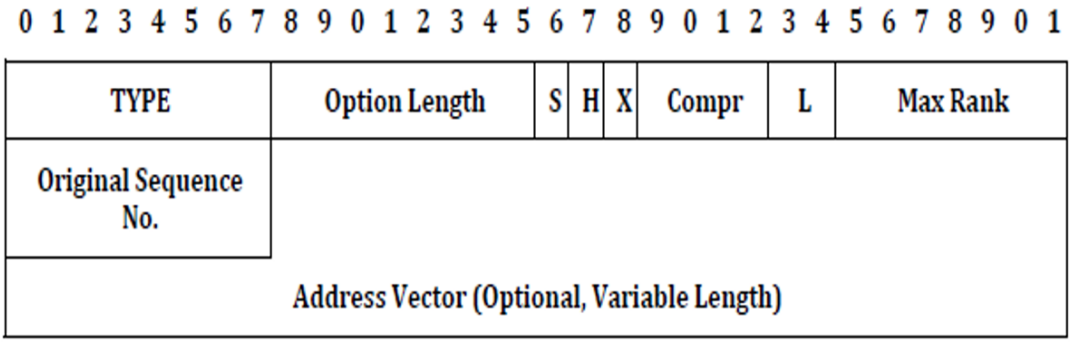


Figure 3.14: Packet Format of DIO RREQ Instance option

The following Figure 3.14 shows the RPL-AODV DIO option, which contains an RREQ-DIO message comprising the DODAG ID field filled by the IPv6 address of the origin node. RREQ-DIO must carry out only one RREQ option in RPL-AODV MoP. In the RREQ option, the origin node forwards the following information: Type: The type assigned to the RREQ option. Option Length: The option length in octets, omitting the length field and type field. Due to the presence of several octets and address vectors, option length is variable. 'S' indicates the symmetric bit representing a symmetric path from the origin node to the router transmitting the RREQ-DIO. 'H' is the value set to zero, indicating source routing, and one represents hop-by-hop routing. This flag controls both the upstream and downstream routes. 'X' is reserved. 'Compr' is an unsigned integer of 4 bits, which is the value field when H=0, i.e., in the case of source routing, and if it is hop by hop routing, i.e., H=1, upon reception, it is ignored and set to zero. 'L' is an unsigned integer of 2 bits

indicating the time duration for a node in the RREQ instance for which it belongs to a temporary DAG, including both the target node and the origin node. Once the time is over, the node has to leave the directed acyclic graph (DAG), and for temporary DODAG, the node has to stop receiving or sending DIO. 'MaxRank' represents the upper limit of the rank. Orig SeqNo is the sequence number of the origin node, which is defined the same as in the AODV protocol. 'Address Vector' is an IPv6 address vector indicating the path that RREQ-DIO has passed. It is present only if the value of H is zero. If a node rank is higher or equal to the max rank, then that node should not join the RREQ instance. When the rank of a target node is similar to the max rank, that node can join the RREQ instance. Upon receiving RREQ, the router must discard it if the rank is higher or equal to the max rank.

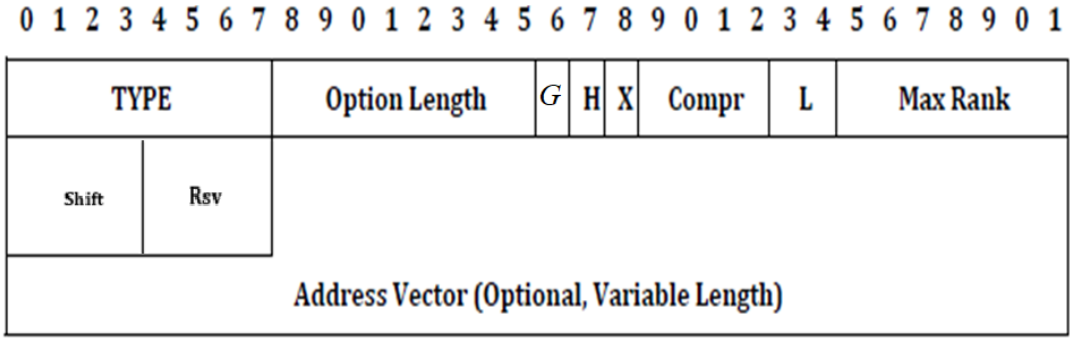


Figure 3.15: Format of DIO RREP option

The following Figure 3.15 shows the RPL-AODV DIO RREP Option containing the RREP-DIO message, which comprises the DODAG ID field filled by the IPv6 address of the target node. RREP-DIO must carry out only one RREP option in RPL-AODV MoP. In the RREP option, the target node forwards the information, as shown in Figure 3.15. Type is the type that is assigned to the RREP option. Option Length is the option length in octets, omitting the length field and type field. Due to the presence of several octets and address vectors, option length is variable. G is Gratuitous route. H is the value set to zero, indicating source routing, and one represents hop-by-hop routing for the downstream route. The H value here is the same as in the RREQ option. X is reserved. Compr is an unsigned integer of 4 bits. This field is useful when H=0, i.e., in the case of source routing, and if it is hop by hop routing, i.e., H=1, upon reception, it is ignored and set to zero. L is an unsigned

integer of 2 bits indicating the time duration for a node in the RREQ instance for which it belongs to a temporary DAG, including both the target node and the origin node. Once the time is over, the node has to leave the directed acyclic graph (DAG), and for temporary DODAG, the node has to stop receiving or sending DIO. Rsv: Initialization of Rsv is set to zero, and upon reception, it is ignored. Orig SeqNo: The sequence number of the origin node is defined the same as in AODV. Address Vector: is an IPv6 address vector indicating the path RREP-DIO passed asymmetrically. It is present only if the value of H is zero.

3.3.3.3 Mathematical Formulation

Consider an IEZN network that consists of both non-storing and storing nodes. In such a network, a large message is divided into multiple segments, and the packet travels from the node.N_i(Origin) to N_j(destination) is cached in a queue at the intermediate locations$N_k$and then transmitted to N_h, which is the next hop of the node. The intermediate nodes act as storing nodes. The requirements for packet flow between nodes are raised randomly, and packets may be of various lengths. In such networks, random variables such as average packet delay that average flow in the channel, from origin to the destination node is represented as $AD = \frac{i}{\gamma} \sum_{i=1}^{NA} \frac{f_i}{c_i - f_i}$

Where $\gamma = \sum_{i=1}^{NN} \sum_{J=1}^{NN} r_{ij}$

AD = Per packet total average delay (sec/ packet)

NA = No.of edges

r_{ij}= It is the average rate of a packet from i to j (packet/second)

f_i= Total bit rate on the channel i (bits/ second)

c_i= Channel (i) capacity (bits/ second) The RPL-AODV protocol is a routing problem in which packets are transmitted from an origin node to some target node through symmetric or asymmetric links in a resource-constrained network. Mathematically, we will represent the RPL-AODV routing problem. Consider a graph $G \in (V, E)$, where V is the set of nodes, and E is the edges in the IEZN network. The costC_{ij} It is associated with each edge $(i, j) \in E$, and each edge has some constraint. U_{ij} On capacity. Let the decision variable by V_{ij} , which is defined per edge $(i, j) \in E$. Each of V_{ij}Denotes a packet distribution from $ItoJ$. $C_{ij} \times V_{ij}$ Is the cost of a flow V_{ij}. Every node j in graph G satisfies the flow

constraint:

$\sum_{k|(j,k)\in E} V_{j,k} - \sum_{i|(i,j)\in E} V_{i,j} = b_j$

b_j Is the flow amount generated by node j. And to find the flow from the source node to the target node and minimize overall cost subjected to capacity and flow conservation constraints.

Minimize $\sum_{i|(i,j)\in E} C_{ij} V_{ij}$

Subject to $\sum_{k|(j,k)\in E} V_{j,k} - \sum_{i|(i,j)\in E} V_{i,j} = b_j \; \forall j \in V(Vertices)$

$0 \leq V_{ij} \leq U_{ij}; \forall (i,j) \in E(Edges)$

Due to the restricted IEZN network, there should be depreciation in the overall link cost and the number of packets distributed, i.e., overall transportation cost should be minimized. Mathematically, we will represent the RPL-AODV routing problem, a flow model for a network with intermediate nodes. Let R be the RPL-AODV routing algorithm, and R(p) be the packet probability that uses path p from the origin node to the destination node. The RPL-AODV routing algorithm R can be represented as:

$\sum_{p\in P_{s,d}} R(p) = 1; \forall s, d \in N$

$\sum_{p\in P_{s,d}} R(p) \geq 0; \forall p \in P$

Where P is the set of all paths of the RPL-AODV routing algorithm, and the Cost Function C(R) should be minimized Subject to $\sum_{p\in P_{s,d}} R(p) = 1$

$\sum_{p\in P_{s,d}} R(p) \geq 0$

In the RPL-AODV routing protocol, the total number of packets sent by the source node is equivalent to the total packet received and is represented as

$\sum_{i=1}^{m} a_i = \sum_{j=1}^{n} b_j$

To minimize the total distribution cost from source node i to target node j

$$Minimize : y = \sum_{i=1}^{n} \sum_{j=1}^{m} C_{ij} x_{ij} \tag{3.1}$$

Such that $x_{ij} \geq 0$ The packets are sent from source node i to all possible target nodes with available routes at that source.

$$Subjectto \sum_{j=1}^{n} x_{ij} = \alpha_i \tag{3.2}$$

The packets that are sent to the target node j from all possible source nodes ought to be equivalent to the received at that target node j

$$\sum_{i=1}^{m} -x_{ij} = -b_j \tag{3.3}$$

Where a_1 =No. of packets sent from the source; b_j = No. of packets received at the destination, c_{ij} =cost from source node i to target node j, where $i = 1, 2, 3, \ldots\ldots, m-1, m$ and $j = 1, 2, 3, \ldots\ldots, n-1, n$ andx_{ij} =no. of packets to be distributed from source node i to target node j. where $i = 1, 2, 3, \ldots\ldots, m-1, m$and $j = 1, 2, 3, \ldots\ldots, n-1, n$.

3.4 Results and Performance Analysis

This section presents the results and performance analysis of the proposed method that uses an IoT-ensemble interface with an adaptive 6LoWPAN communication protocol in the ZigBee network. We tested our proposed work in the network simulator NS3 and conducted experiments ranging from 10 to 500 nodes within IoT-enabled ZigBee networks. We evaluated performance metrics such as throughput, routing overhead, average end-to-end delay, and header compression. To assess the performance of the experimental results of our proposed framework, we utilized the dataset generated by the simulator NS-3. The Table 3.1 shows the simulation parameters.

3.4.1 Hardware setup

The hardware setup has the following components: a Raspberry Pi, a temperature and ultrasonic sensor, a breadboard, Jumper Wire, and a 4.7 k Resistor.

1. **Raspberry Pi:** The Raspberry Pi Foundation created the little single-board computer known as the Raspberry Pi, which has an approximate dimension of 85 mm by 56 mm. The Broadcom BCM2835 SoC, which powers the Raspberry Pi, has a core architecture of a 32-bit ARM11 processor with a 700 MHz operating frequency called the CPU ARM1176JZFS. One Ethernet socket, video output, audio output, a 15-pin

Parameters	**Value**
Simulator	NS (Network Simulator)
Simulator Version	NS-3
CBR Packet Size	512 bytes
Simulation Area	70M*60M
Simulation Time	60 seconds
Routing Protocols	RPL-AODV, 6LoWPAN Protocol
Number of Nodes	500
Performance Metrics	Routing Overhead, End-to-End Delay, Header Compression, Average Throughput
Packet Rate	1Kbps
Net Buffer Size	1000Bytes
Node Deployment	Uniform

Table 3.1: NS-3 Simulation Parameters

MIPI camera serial interface with a microSD card slot, 512 MB of SDRAM, 40 GPIO pins, four USB-2.0 ports, and other features are included with the B+ model. Figure 3.16(a) shows the sensor module has four pins: VCC for voltage (3.3 V to 5 V), GND for ground, DO for digital output, and AO for analog output. As we are interested in ON or OFF signals from the sensor based on the result of the temperature sensitivity adjuster, only DO is connected to GPIO23 (Pin 16) of the Pi instead of AO. Pin 2 and Pin 6 are connected to voltage and ground, respectively. The power pin of the Pi is connected to the first row of the breadboard's positive rail, while the second row will be associated with the sensor's VCC. The ground pin of Pi is connected to the first row of the negative rail, where the second row will be connected with the sensor's GND. Finally, the jumper wire from the DO pin of the sensor and GPIO23 of the Pi is connected to the blank rail of the breadboard. The resistors must be connected in series to link the DO, which outputs 5 V, and the GPIO, which outputs 3.3 V, reducing the voltage to a desirable level after installing the hardware. The IoT-enabled ZigBeeprotocol enables the communication of Pi and thermometer Sensors.

2. **Temperature Sensor:** The humidity and temperature are measured via the DHT11 and DHT22 sensors. One GPIO is utilized. The key factors separating the two are measurement range and precision. The white DHT22 has a 2 percent accuracy range for all humidity calculations from 0 to 100 percent. In contrast, the DHT11 (blue)

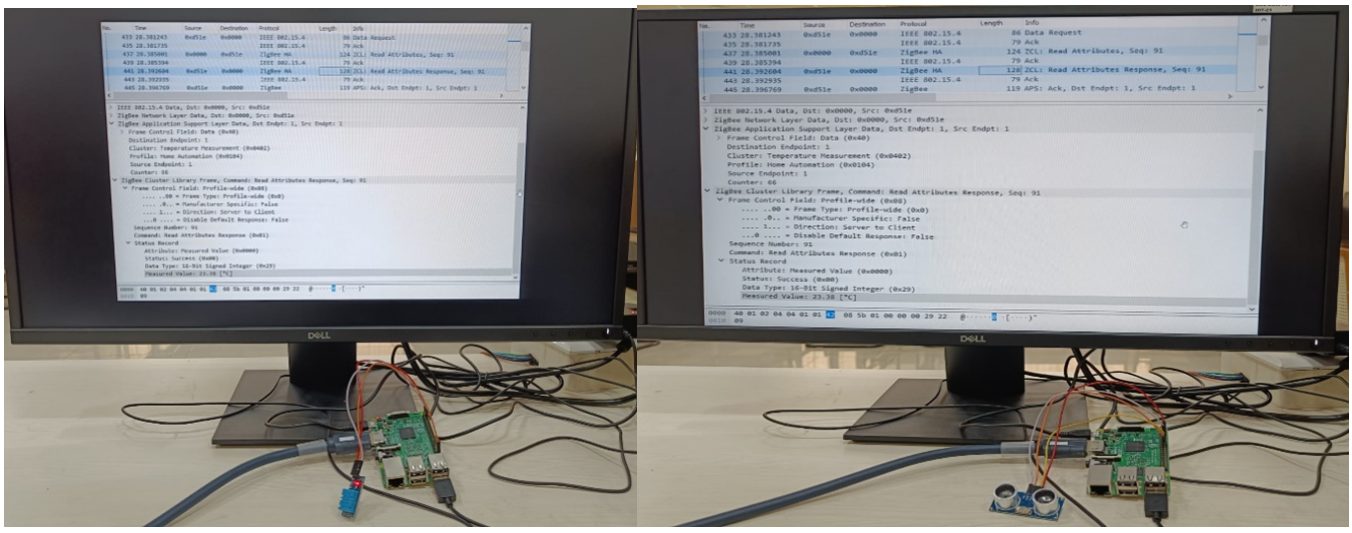
can only monitor regions with humidity levels between 20 and 90 percent, and its accuracy is just 5 percent. The hardware setup is a Raspberry Pi-based Thermistor Sensor Module kit, alerting the user if the temperature and humidity reach a specific threshold. A ZigBee packet fetches a "Read Attributes" request from the ZigBee hub to the multipurpose sensor. We can observe that the packet could be read, and its cluster was identified as "Temperature Measurement.

3. **Ultrasonic Sensor:** The ultrasonic range module HC-SR04 has a 2 to 40 cm range, and its precision is 3 mm. The time will begin when ultrasonic waves are released from the transmitter into the ultrasonic sensor, which distributes the waves in a certain direction. The ultrasonic waves dispersed throughout the air instantly reversed direction when they came into contact with any item in their path. The ultrasonic sensor receiver pauses when the transmitter starts receiving the reflected wave. Since the speed of ultrasonic waves is 340 m/s, the distance between the transmitter and the desired target may be determined using the formula s = 340 t/2. The difference in the time-distance measurement principle refers to this. Ultrasonic distance measurement is based on the known air spreading velocity, measuring the time for the waves from the time of transmission to the time of reception after contact with the target and calculating the distance using the time and velocity of the waves. We can observe in Figure 3.16(b) that shows the read attributes response packet content shows the Ultrasonic Sensor.

3.4.2 Performance Analysis

The section presents the performance analysis of the proposed work with various network metrics such as end-to-end latency, average throughput, and packet delivery ratio (PDR). The following measurement metrics evaluate the proposed interfacing of 6LoWPAN in a IoT-enabled ZigBee Network.

The RPL-AODV combo of the 6LowPAN protocol is tested for performance using the following network metrics. The indicators include end-to-end latency, average throughput,



(a) Content from the Read Attribute Response packet displaying the temperature value

(b) Read Attributes Response packet content showing the Ultrasonic Sensor.

Figure 3.16: Hardware Setup for Performance Evaluation using Raspberry Pi

and packet delivery ratio (PDR). The following measurement metrics evaluate the proposed Interfacing 6LoWPAN in IoT-Enabled ZigBee Network.

i. **Average End-to-End Delay**: The time passed since a data packet is transmitted to the time it is received at the destination. This includes all types of delays in a network.

$$\sum_{i=1}^{n}\sum_{j=1}^{n}(rtp)_i - (stp)_j\sum_{i=1}^{n}(prn)_i \tag{3.4}$$

rtp - Received time of packet

stp - Sent time of packet

prn - Packet received by node

ii. **Routing Overhead**: The total number of control packets each routing protocol produces.

Packets Overhead = the Total number of routing packets transmitted in the network during the simulation.

iii. **Avg Throughput**: It is the amount of data transferred over the period of time expressed in bytes per second in the network during a simulation.

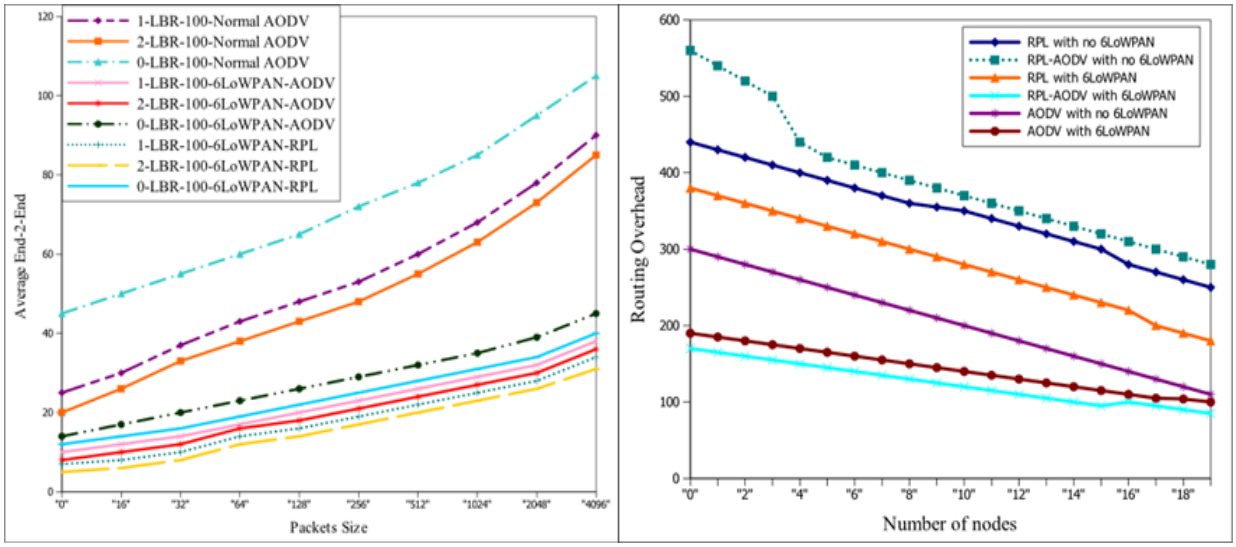
$$AvgThroughput = \frac{\sum_{i=1}^{n} Data\ packets\ received\ by\ node_i}{\sum_{i=1}^{n} Data\ packets\ sent\ by\ node_i} \tag{3.5}$$

iv. **Packet Delivery Ratio:** the proportion of data packets supplied by the origin node successfully received by the target node.

$$PDR = \frac{\sum_{i=1}^{n} packets\ received\ by\ destination}{\sum_{i=1}^{n} packets\ sent\ by\ sources} \tag{3.6}$$

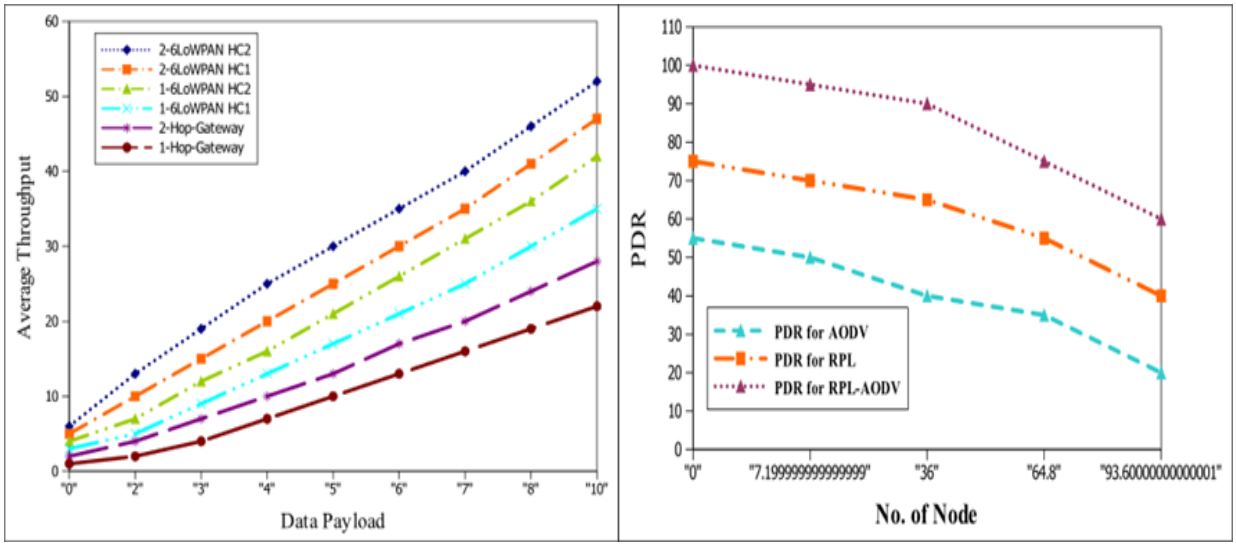
Figure 3.17(a) shows the end-to-end delay of low bit rates in AODV, 6LoWPAN-AODV, and 6LoWPAN-RPL routing protocols within the IoT-enabled ZigBee network. The proposed RPL-AODV protocol has a lower average end-to-end delay due to the shortest path and achieves higher route diversity than the AODV and RPL protocols. The Figure 3.17(b) shows the overhead routing with RPL, 6LoWPAN, AODV, and RPL-AODV with and without the IoT-enabled ZigBee network. The routing overhead varies with RPL-AODV, which has a lower routing load than the AODV and RPL protocols. It also reduces the size of four DIO requests and DIO replies, RREP, and RREQ control messages to two control DIO-RREQ instances and two DIO-RREP instances. Hence, the proposed routing protocol suits various low-power applications.

Figure 3.17(c) shows the average throughput of 6LoWPAN HC1, 6LoWPAN HC2, and Hop-gateway routing protocols with varying pause times. The throughput of 6LoWPAN decreases due to high throughput loss, degrading the IoT network's performance. Figure 3.17(d) shows the packet delivery ratio with varying IoT network nodes. It indicates that PDR is for AODV, RPL, and RPL-AODV protocols and shows that the PDR for AODV is lower than for RPL and RPL-AODV protocols. However, the proposed RPL-AODV protocol achieves better PDR than RPL protocols with varying nodes. Figure 3.18(a) shows routing overhead with varying times. The proposed RPL-AODV protocol has less routing load than the AODV and RPL protocols. It reduces the size of four DIO requests and DIO replies, RREP, and RREQ control messages to two control DIO-RREQ instances and two DIO-RREP instances. Hence, the proposed routing protocol suits various low-power applications. Figure 3.18(b) shows the end-to-end delay of RPL, AODV, and RPL-AODV routing protocols in the IoT network. The proposed RPL-AODV protocol has a lower



(a) Average End-to-End Delay

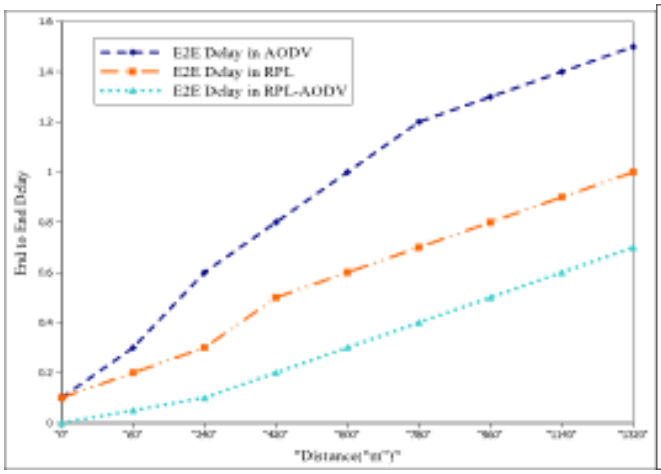
(b) Average End-to-End Delay.



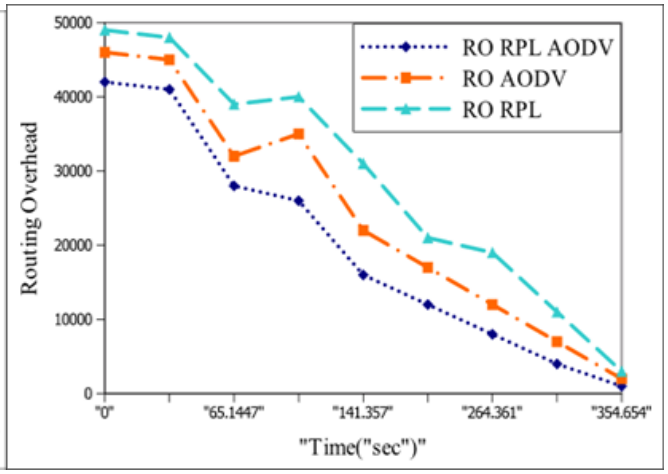
(c) Average Throughput

(d) Packet Delivery Ratio

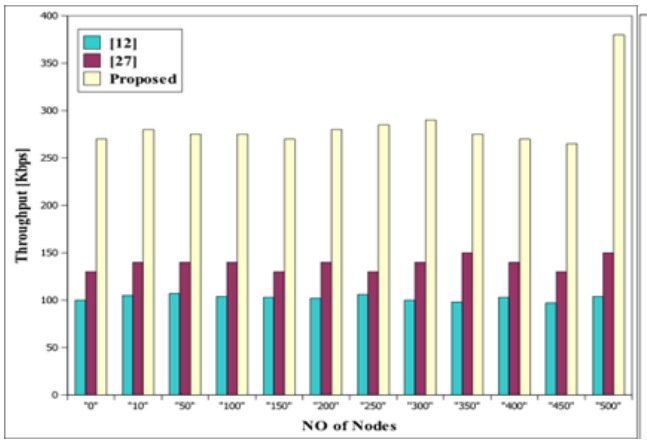
Figure 3.17: Evaluation of proposed framework based on key performance metrics.



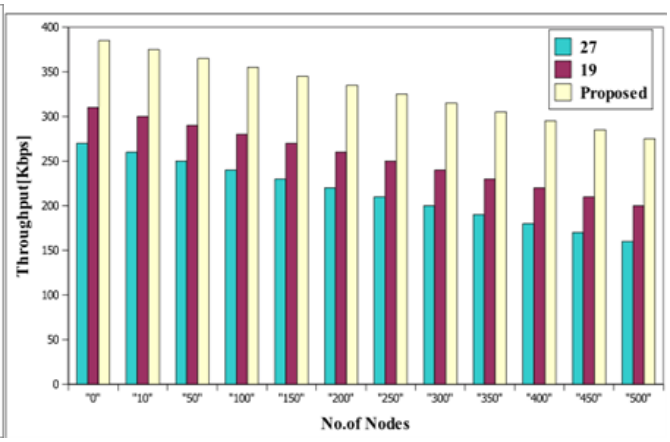
(a) Average Throughput



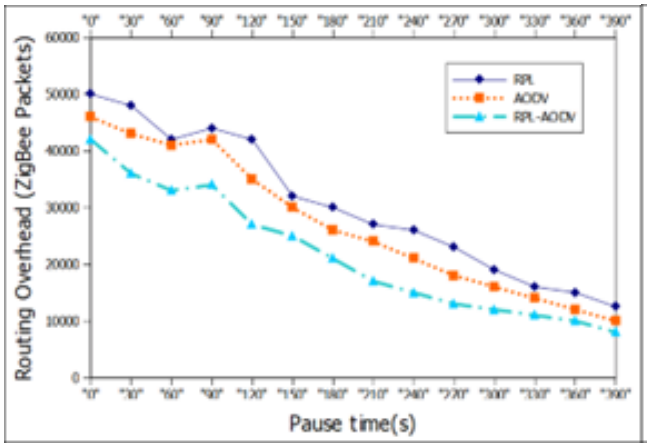
(b) Packet Delivery Ratio



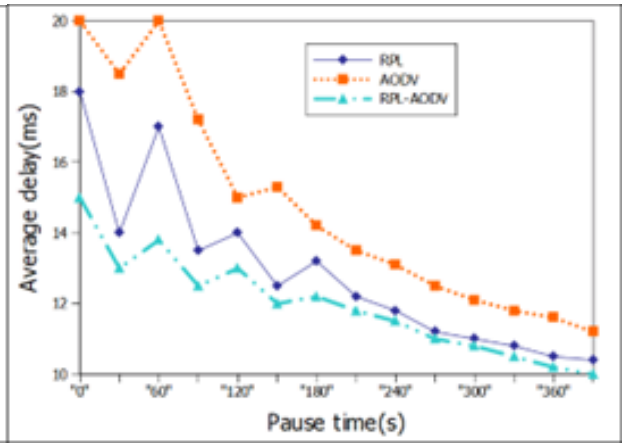
(c) Throughput Comparison with Different ZigBeeNodes



(d) Throughput Study Comparing Nodes in Different WSN



(e) Simulation of Routing Overhead



(f) Simulation of the Data Packet Average Delay Time

Figure 3.18: Evaluation of Proposed Framework based on Key Performance Metrics

average end-to-end delay due to the shortest path and achieves higher route diversity than the AODV and RPL protocols. Figure 3.18 (c) and (d) show the throughput with various IoT network nodes. It shows that the throughput for AODV and RPL is less than the proposed RPL-AODV protocol. Moreover, the proposed RPL-AODV protocol achieves better throughput than the RPL protocol with varying nodes compared with other existing methods. figure-3.18 shows the average end-to-end delay of the RPL, AODV, and RPL-AODV routing protocols in the IoT network. The proposed RPL-AODV protocol has a lower average end-to-end delay due to the shortest path and achieves higher route diversity than the AODV and RPL protocols. Moreover, the RPL-AODV protocol achieves less latency than the RPL protocol with varying nodes compared with other existing methods presented in [16] [34] [40].

Figure 3.18 (a) and (b) show that the delay of RPL and AODV is greater than RPL-AODV and increases with decreasing node pause duration. The higher the mobility of mobile nodes in this experiment, the quicker the network changes. The figure clearly shows that the AODV and RPL protocol delays are higher than the RPL-AODV protocol delays.

3.5 Summary of the Chapter

This chapter presents the proposed framework to provide an efficient end-to-end communication protocol by interacting with an adaptive 6LoWPAN communication protocol in an IoT-enabled ZigBee network. The adaptation protocol offers services to the network or internet layer by taking the data from the end devices. Once the 6LoWPAN protocol receives the query from the internet host or ends the user, it performs the three primary services. (i) Fragmentation and reassembly are used to meet the IPv6 minimum MTU requirements. (ii) Header compression: removing fields that may be deduced from link-level information or based on basic shared context assumptions. (iii) Link-layer forwarding is supported to transport IPv6 datagrams over many hops. Next, route the IPv6 packets into regional IoT-enabled ZigBee networks. We proposed an RPL-AODV routing protocol and the mesh address header to transfer Zigbee packets among multiple 6BR nodes. We tested our proposed work and evaluated the performance metrics, such as throughput, routing

overhead, average end-to-end delay, and header compression. The proposed work's performance showed better results than the existing work. However, enabling efficient IPv6 communication over ZigBee networks requires high end-to-end security rules that will be discussed in the next chapter.

Chapter 4

Cooperative IDS Mechanism to Detect Collaborative Attacks against RPL-AODV Routing Protocol in the IoT-Enabled ZigBee Networks

In recent years, the number of devices in our environment that are connected to the internet has exploded. The Internet of Things (IoT) [76] [84] is one of the vital technology integrators in Industry 4.0, contributing to the large-scale deployment of IoT networks that enable networked connections among people, processes, data, and things[49]. However, all the nodes in the IoT are connected through lossy links, which are generally unstable and support low data rates. Many battery-operated restricted devices have low processing and capacity, limited memory, and limited energy[23]. In addition, the significant inconveniences of these IEZN networks mainly depend on the "security" of the devices. The fact that there are so many businesses that produce them and so many different protocols based on the many existing standards is one of the main reasons why there is still no standardised strategy to fixing these difficulties. The "routing protocol for low-power and lossy networks" [45] [104] (RPL) is one of the standardized protocols designed for efficient communication of smart devices with optimal energy and transmission specifications

[72] [115] [12] [33]. The RPL protocol itself has many security risks and possibilities for attacks. Most efforts have been put into a mechanism to defend against individual attacks against the RPL routing protocol[11] [14]. Intrusion detection fails to handle a high detection rate, early detection of known attacks, the ability to detect novel, unknown attacks, and a low false-positive rate[118][119].

IoT-enabled ZigBee Networks (IEZN) cooperative IDS mechanism that detects collaborative attacks against the "RPL-AODV" routing protocol[14][116]. To do this, we first looked at how well the RPL-AODV routing protocol performed at combining the benefits of both RPL and AODV routing protocols, which coexist in the resource-constrained, low-power IoT-enabled ZigBee Networks covered in the previous chapter. Next, we modeled the collaborative attacks[98], such as the wormhole and black attack, which exploit the vulnerability of the AODV protocol, and the rank attack and sinkhole attack, which exploit the vulnerability of the RPL protocol[13]. Specifically, we modeled the collaborative attacks (wormhole, black attack, rank attack, and sinkhole attacks) against the RPL-AODV routing protocol. The RPL-AODV routing protocol, which effectively keeps an eye on the IoT-enabled ZigBee Networks, is vulnerable to coordinated attacks. To detect these attacks, we suggested cooperative IDS, which combines specification-based and signature-based IDS[71] [37][120].

4.1 Challenging Issues

Some of the following challenging issues are addressed in this chapter:

1. The AODV [32] and "RPL routing" protocols in the "LLN network" are resolved by resolving the above limitations of the AODV and RPL protocols, where the AODV protocol uses a flooding mechanism[50]. In contrast, the RPL protocol is mainly used in the restricted network[17].

2. The AODV and RPL protocols themselves have many security risks and possibilities for attacks [12], [[44]], and [69]. Most such efforts have been put into a mechanism to defend against individual attacks [34], [16] against the AODV and RPL routing

protocols.

3. Intrusion detection [47], [37] fails to handle high detection rates, early detection of known attacks, the ability to detect novel, unknown attacks, and a low false-positive rate[94].

This chapter addresses the above challenging issues with the following solutions:

1. We modeled collaborative attacks such as wormhole and blackhole[99] attacks, which exploit the vulnerability of the AODV protocol, and rank attacks and sinkhole attacks, which use the vulnerability of the RPL protocol[43][63]. This collaborative attack may have a more devastating impact on IEZN networks than an uncoordinated attack[9][60]. The collaborative model was developed to investigate the weaknesses of the AODV and RPL protocols in LLN networks that exploit the LLN environment's vulnerabilities[20]. From a security perspective, these collaborative attacks use the combined efforts of more than one attacker against the target victim[61][96].

2. A hybrid IDS[32] has been proposed by combining signature and specification-based techniques to overcome the limitations of signature and anomaly-based approaches[26] [71]. This combination enables the hybrid IDS to detect signature or specification attacks, consuming less energy[22]. The proposed cooperative IDS is a hybrid-based intrusion detection[92] system using an ensemble machine learning approach that combines specification-based and signature-based IDS as a cooperative IDS to detect "collaborative attacks" against the "RPL-AODV routing protocol" that effectively monitors the IEZN network[80][89][94].

4.2 Modeling of Collaborative Attacks against the RPL-AODV Routing Protocol

This section presents the "collaborative attacks" against the "RPL-AODV routing protocol" discussed in the section of Chapter 1. The most prominent and well-known attacks against this RPL-AODV routing protocol are sinkholes, rank attacks, black holes, and wormholes

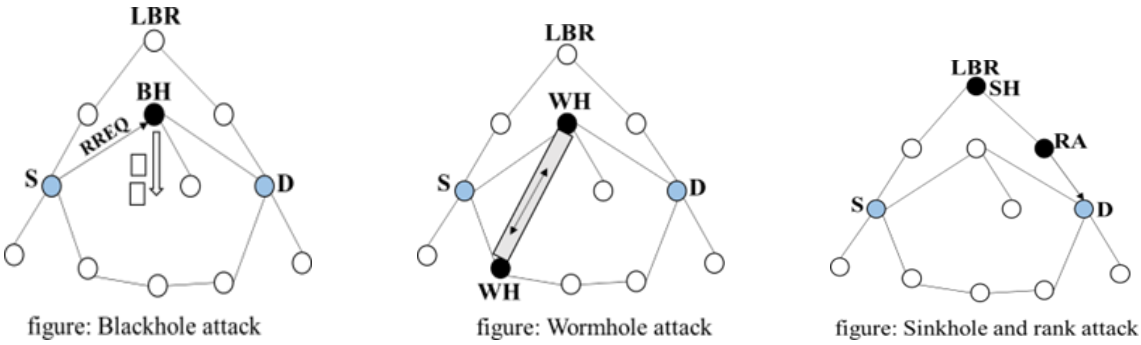


Figure 4.1: Collaborative attacks against RPL-AODV routing protocol

against the AODV and RPL routing protocols in a collaborative fashion. Most such efforts have been put into a mechanism to defend against isolated attacks in state-of-the-art work. The attack can be described as any process, method, or means to maliciously attempt to compromise the "AODV and RPL routing protocol" nodes in the IoT-enabled ZigBee Networks[62][95]. The attackers perform malicious activities in the network, including data stealing, damage to data, modification of data, denial of service, or depleting network bandwidth and resources. First, we present the attacks against the AODV and RPL routing protocols. Existing literature shows that Wormhole and Blackhole Attacks are more vulnerable to the AODV routing protocol, as shown in Figure 4.1.

4.2.1 Wormhole and Blackhole Attacks Against AODV Routing Protocol

The wormhole attack is caused by two or more attackers or malicious nodes that can communicate with one another. One node is kept around the router, and the other is held somewhere else in the IEZN network. When one of the nodes receives a data packet without sending it to its standard path, it sends it out to the other node directly through the tunnel. So in this way, the attacker can do packet manipulation and cause network routing disruption since routing data does not reach every node. The wormhole attack can also be carried out using one malicious node, which transmits incorrect information to two legitimate nodes at different locations, convincing them they are neighbors.

The other is a black hole attack that will work with the perception of intercepting all

the messages; an attacker can broadcast false information to all other nodes in the IEZN network with the shortest path[112]. A black hole node attracts all packets using a forged RREP packet (route reply), which claims to have the shortest path to the destination and drops all of the data packets without sending them. Once the attacker tries to access all the packets and can drop a few or all of them, this can be done according to the packet data. It assumes that the malicious node has complete information about the data content transmitted on the IEZN network.

4.2.2 Rank Attack and Sinkhole Attack Against RPL Routing Protocol

The Rank Attack and Sinkhole Attack will exploit the vulnerability of the RPL routing protocol; the rank attack will exploit the weakness of the RPL protocol, which is mainly used to provide the optimized routing topology and prevention of loops in IEZN networks, as shown in Figure 4.1. The mechanism to prevent loops is based on the rank concept to show the nodes' relationship. Every node in the network needs to calculate its rank depending on the data collected from neighboring nodes. Each node must select a preferred parent except the sink node, and the parent node rank should not be greater than the children's rank. The node's rank is calculated based on the RPL rule, which states that "in downward direction rank of a node is strictly increasing and in upward direction rank of a node is strictly decreasing." The attackers will exploit this security flaw.

Specifically, when a source $node-1$ transmits a packet through intermediate nodes $(i.e., node-2,3,4.\ldots..N-2,N-1$are the intermediate nodes) to the target node N. Consider $R_1, R_2R_3.\ldots..R_n$ Be the rank of nodes from 1 to N, respectively. According to the rank rule, if node-1 transmits a packet in the upstream direction to node N, the condition $R_n \leq R_{(n-1)}.\ldots..R_{(2)}[\leq R]_{(1)}$must be satisfied, or if the packet travels in a downward direction, then $R_n \geq R_{(n-1)}.\ldots..R_{(2)}[\geq R]_{(1)}$ must be satisfied. Along the route, every sender and receiver of the packet must check these conditions. If the state is not satisfied, the node must inform by setting the bit rank error in the information of the RPL packet. The attackers will easily exploit this issue by omitting the checking function for rank in the

compromised nodes. This attack is hard to disclose because it does not require anything to spoof and looks normal in the behavior of the compromised nodes. The attackers will exploit the following issues to degrade the performance of the network: (in terms of delay and throughput)

1. Creation of an unoptimized path.
2. Disruption in the optimized paths, which results in an undiscovered path.
3. Undetected creation of loops.

Sinkhole Attack: The other attack against the RPL routing protocol is a sinkhole attack. Intruders launch a sinkhole attack with the help of their rank. Intruder sends out better rank to the other nodes in the network to make them a neighbor in the destination-oriented directed acyclic graph for choosing it as a node which is the preferred parent. This attack focuses on controlling packet traffic through the compromised or malicious node to a great extent in the network. The attacker cheats the authorized node to establish the link with the unauthorized or malicious node by showing it has the optimal routes. The attacker forwards incorrect information to some legitimate node using a wormhole attack or directly. A sinkhole attack behaves like a wormhole, black hole, and selective forwarding attack.

4.3 Detection of Collaborative Attacks against RPL-AODV Using Hybrid-Based Intrusion Detection System

This section presents the "hybrid-based intrusion detection" system proposed to address the aforementioned complex issues by combining the benefits of signature-based IDS, which offers an effective attack detection scheme of known attacks with improved detection rate, and low "false-positive rates", with the ability of the anomaly detection system to detect novel, unknown attacks [93]. Hence, the sequence-based fusion of these two approaches should theoretically provide an effective Intrusion detection system that enhances the overall performance of collaborative attack detection, shortening the detection delay, increasing detection accuracy, and reducing false-alarm rates.

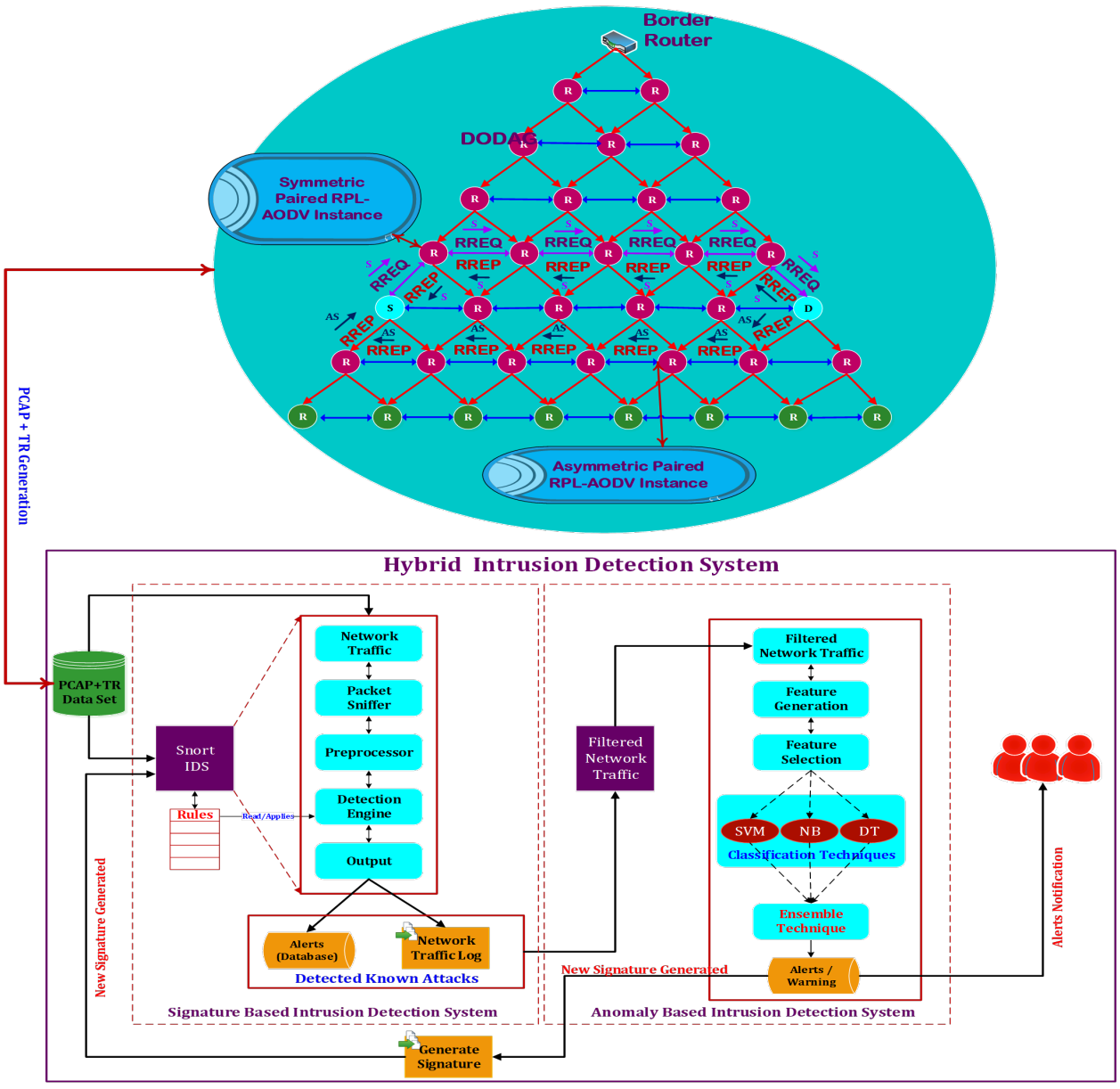


Figure 4.2: figure-Based Intrusion Detection System against RPL-AODV Protocol

The hybrid intrusion detection system employs both IDS techniques in two stages to detect both known and undiscovered assaults, as shown in Figure 4.2. In the initial phase, we employ Snort IDS, a lightweight signature-based detector, for misuse detection. A database of known detection behaviors has been developed and updated over time. In this stage, the system compares the network traffic with an intrusion behavior database in real time. Based on the matched rules, the alerts will be generated upon attack detection without any learning mechanisms. During the second phase, the anomalies are detected. This stage is used to compensate for the first stage's shortcomings and can detect novel attacks. After the signature-based identification, the network features are extracted through the feature extraction module. To identify abnormal network behaviour from typical network activities, significant non-redundant features are retrieved and picked. By combining the Adaboost Ensemble methodology with machine learning classification methods like Decision Tree, Naive-Bayes, and Support Vector Machine, malicious packets are more accurately detected. The hybrid intrusion detection system measures various tokens to detect the misbehaving aspect of these collaborative attacks. The measures include the received strength of a signal, the packet's sending rate, the packet's receiving rate, the packet's delivery ratio, the packet's acknowledgment, the sending ratio of the packet, the forwarding rate of the packet, and the channel sensing time. Some of the parameters were considered while simulating the proposed RPL-AODV protocol.

1. The received strength of the signal is the power measure enclosed in the radio signal received.

2. The sending rate is the number of packets transmitted in a predefined duration.

3. The receiving rate is the number of packets received in a predefined duration.

4. The delivery ratio of the packet is the packet ratio delivered successfully and based on the number of packets the sender transmits.

5. Packet acknowledging rates are numbers defined for the acknowledgments a node sent to another node.

6. Sending ratio of the packet is defined as the number of packets sent successfully and the number of packets that must be transmitted.

7. The dropping rate of the packet is the number of packets dropped in a predefined duration.

8. The forwarding rate of the packet is the number of packets received by some node to forward it in a predefined duration.

9. The time a node waits to access the channel is called channel sensing time.

4.3.1 Hybrid-Based Intrusion Detection System Using Ensemble Machine Learning Approach:

A hybrid IDS has been proposed by combining signature and specification-based techniques to overcome signature and anomaly-based weaknesses. This combination enables the hybrid IDS to detect signature or specification attacks by classifying correct and incorrect feature vectors in the dataset with less energy consumption. The datasets contain flow-based and packet-based network features. The performance of the hybrid IDS can be measured in terms of statistical metrics (mean, packet size), protocol information, and direction identifiers.

The AODV-RPL protocol performs leveling of the network using a tree created using the child-parent relationship, and at a high level, it places a border router that acts as the tree base. To decrease the use of node resources, rather than the monitoring node monitoring all its neighbors, it only monitors the node with an immediate relationship with the nodes, i.e., its child node or its parent node. Based on the analyzed and statistical data, The monitored node data can be forwarded to the operator at the border router to compare them and output the final result to revoke the suspicious node.

This method employs ensemble machine learning techniques by integrating Support Vector Machine, Naive-Bayes, and Decision Tree classifier techniques for network record classification into regular or malicious traffic records. To achieve high accuracy, the proposed method uses Adaptive Boosting (AdaBoost) classifier to improve classifier accuracy,

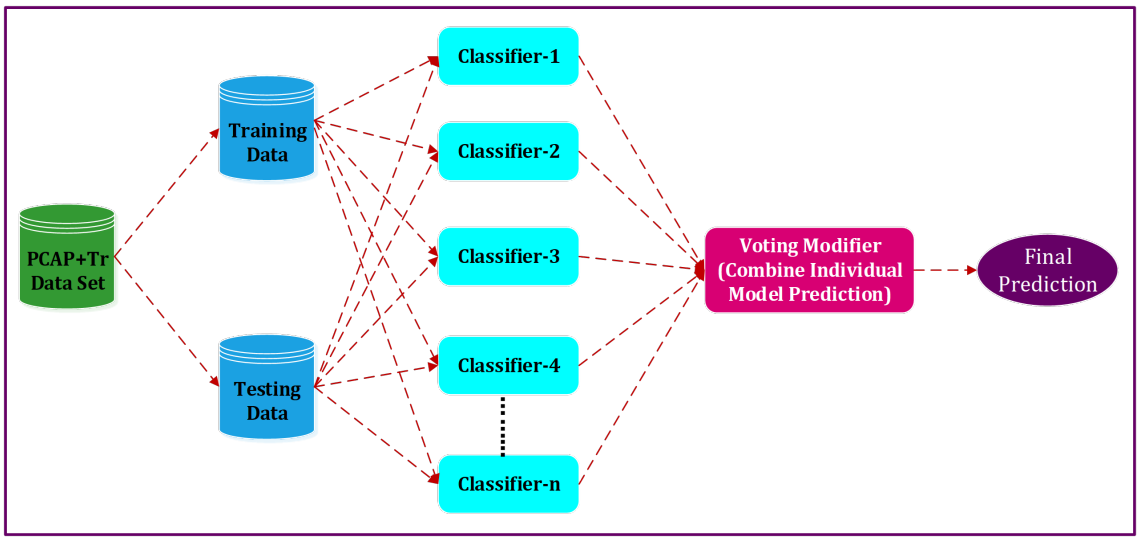


Figure 4.3: Ensemble Machine Learning Technique

an "iterative ensemble method" as shown in Figure 4.2. To make them robust classifiers, boost their performance, and produce models with high precision, this classifier incorporates decision trees, Naive Bayes, and Support Vector Machines. It won't be as vulnerable to the over fitting problem. This approach's main goal is to give each instance in the training set a weight. All weights are first regarded as being equal. Nonetheless, the consequences are increased for all cases incorrectly predicted in each iteration so that these cases have a high likelihood of classification in the subsequent epoch.

In contrast, cases that are accurately classified have their weights reduced. Repeat the iterations until the maximum number of estimators or efficient classifier is found. Every iteration lowers training mistakes and improves how well the model fits the supplied data. As shown in Figure 4.3 the ensemble machine learning technique acts as the **Voting Classifier** by selecting the best classification results among the three classifiers as mentioned above. Based on the average of the estimated probability distribution of output label classification, this soft voting mechanism is performed.

Alert/Warnings: Alerts are generated when malicious instances are identified, and the "false positive rate" is discovered to assess the performance. The main advantage of the proposed hybrid IDS is that

1. It is effective in spaces of considerable size.

2. It is effective in memory because the decision-making function selects a set of training samples known as support vectors.
3. It uses probability to produce predictions.
4. It can deal with material that is both discrete and continuous.
5. It is easy to deal with numbers that are missing.
6. It is easy to change as new information comes in.
7. It makes things easier to understand and less complicated.
8. It takes into account every possible result of a choice. So, it follows each link all the way to the end.
9. It has a high detection rate, finds known threats early, and has a low rate of false positives.

4.4 Results and Performance Evaluation

This section presents results and performance analysis for studying the feasibility of our proposed work. We have implemented the proposed AODV-RPL protocol along with its attacks in network simulator NS3 [33], Whitefield, and Contiki-Cooja [32] has been utilized and conducted a series of experiments ranging from 10 to 1000 nodes on AODV, RPL, AODV-RPL Protocol, and proposed collaborative attacks against AODV-RPL Protocol for generation of high-trustworthiness attack data within IEZN networks. Table 4.1 shows the simulation parameters of the proposed work.

4.4.1 Performance Analysis

The performance of AODV-RPL protocol is analysed using a set of metrics including packet delivery ratio (PDR), average end-to-end delay, routing overhead, precision, accuracy, recall or detection rate, false-positive rate, and F1- score. The proposed "Intrusion Detection System (IDS)" assessment is based on the following.

Parameters	**Specifications**
Operating System	Ubuntu-18.08
No of Nodes	Contiki-3.0
Simulation Duration	250m
Physical Topologies	Variable Grid-Center Topology and Random Topology
Traffic Type	UDP
Data Payload Size	127Bytes/ Packet
Routing Protocol	RPL-AODV Protocol

Table 4.1: NS-3 Simulation Parameters

1. Packet Delivery Ratio (PDR): the ratio between the data packets received correctly by the target node and data packets sent by the origin node

2. Average End-to-End-Delay: Average time taken by the packet correctly to deliver from the origin node to the target node

3. Routing Overhead: Number of data packets received correctly by the target node within the time duration

4. The proportion of correctly identified samples to all samples is used to calculate accuracy.

5. Precision is the percentage of genuine positive samples used to forecast successful models. It provides the guarantee of DDOS attack detection.

6. The recall is also known as the "Detection Rate (DR)" or "True Positive Rate (TPR)" and is calculated as the ratio of true positive samples to total positive models.

7. The ratio of "false-positive" samples to positive model predictions is known as the false-Positive Rate (FPR).

8. $F1_Score$ (F1) is the Harmonic average of precision and recall.

9. The recall is also known as the detection rate (DR) or "true positive rate (TPR)", and it is calculated as the ratio of real positive samples to total positive models.

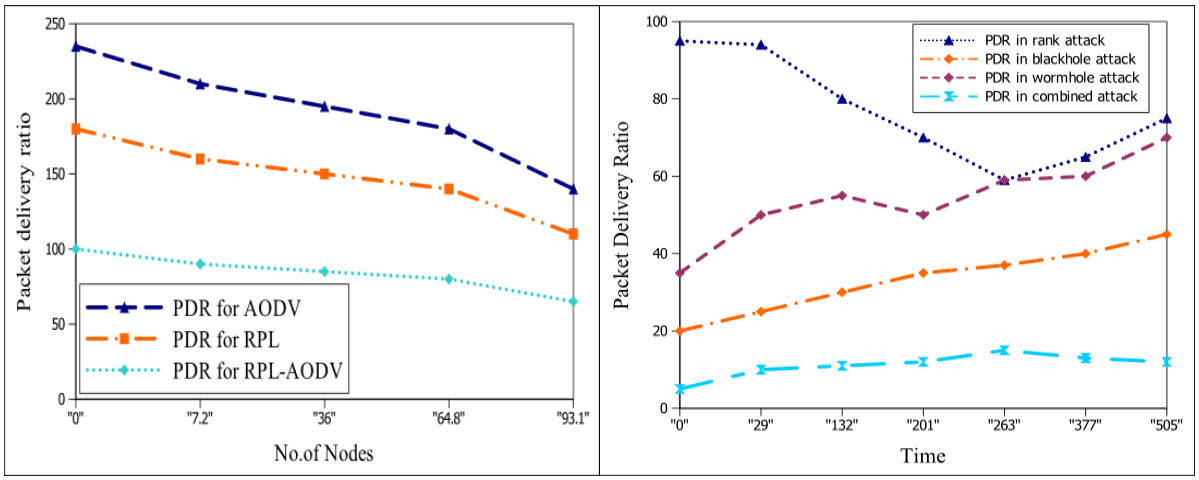
10. The ratio of "false-positive" samples to positive model predictions is known as the "false-Positive Rate (FPR)".

11. $F1_Score$ (F1) is the precision and the recall harmonic average.

Figure 5.11 (a) shows the packet delivery ratio with various IEZN network nodes. It indicates that PDR for AODV is less than for RPL and RPL-AODV protocols. However, the proposed RPL-AODV protocol achieves better PDR than RPL protocols with varying nodes. Figure 5.11 (b) shows the packet delivery ratio with collaborative attacks in the IEZN network. The PDR is decreasing because the attacks become active at 132.1 ms. It is observed that collaborative attacks will cause high packet drops that incur a denial of service to the application layer, as it gets only 12.5% of the application data to the border router. Figure 5.11 (c) shows routing overhead with varying times; the proposed RPL-AODV protocol has less routing load than the AODV and RPL protocols. It reduces the size of four DIO requests and DIO replies, RREP, and RREQ control messages to two control DIO-RREQ instances and two DIO-RREP instances. Hence, the proposed routing protocol suits various low-power applications.

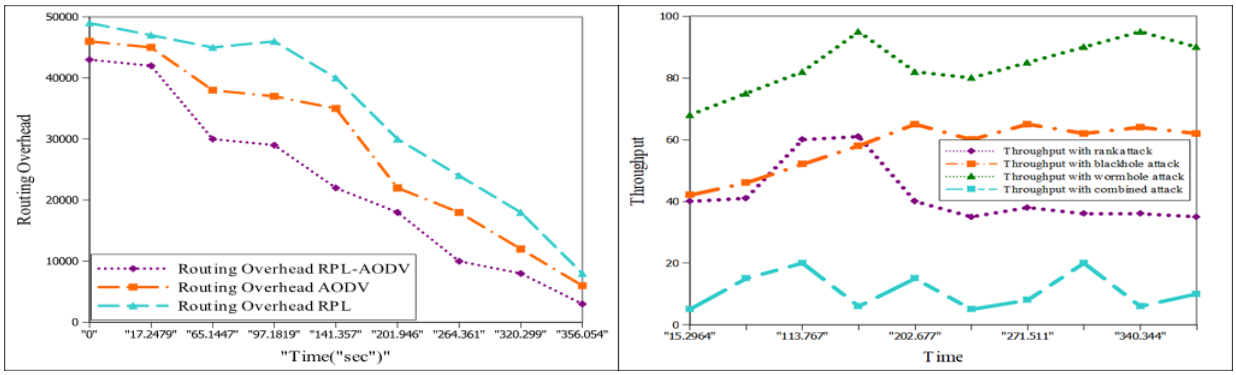
Figure 5.11 (d) shows the throughput of RPL, AODV, and RPL-AODV routing protocols with varying pause times. It is observed that the throughput of RPL-AODV is decreasing because the attacks become active at 15.1 ms. It is also observed that collaborative attacks cause high throughput losses, degrading the IEZN network's performance.

Figure 5.11 (e) & Figure 5.11 (f) show the end delay of RPL, AODV, and RPL-AODV routing protocol with and without attacks in the IEZN network. The proposed RPL-AODV protocol has a less average end-end delay due to the shortest path and achieves high route diversity compared to the AODV and RPL protocols. Further, Figure 5.11 (f) The more end-to-end delays in the presence of collaborative attacks in the RPL-AODV protocol. The proposed method also uses an ensemble machine learning-based attack detection methodology that takes various tokens for detecting the misbehaving aspect of these collaborative attacks with high accuracy and precision. We evaluated and contrasted the experimental performance of the proposed "hybrid IDS", which combines "Signature-based" and "Anomaly-based" detectors, using various performance metrics as mentioned earlier. To evaluate the efficacy of the experimental outcomes of our proposed framework, we employ the simulation NS-3 and Cooja-generated PCAP raw packet capture and Trace (tr) files. This data source contains both routine network traffic and recent collaborative attacks. Nor-



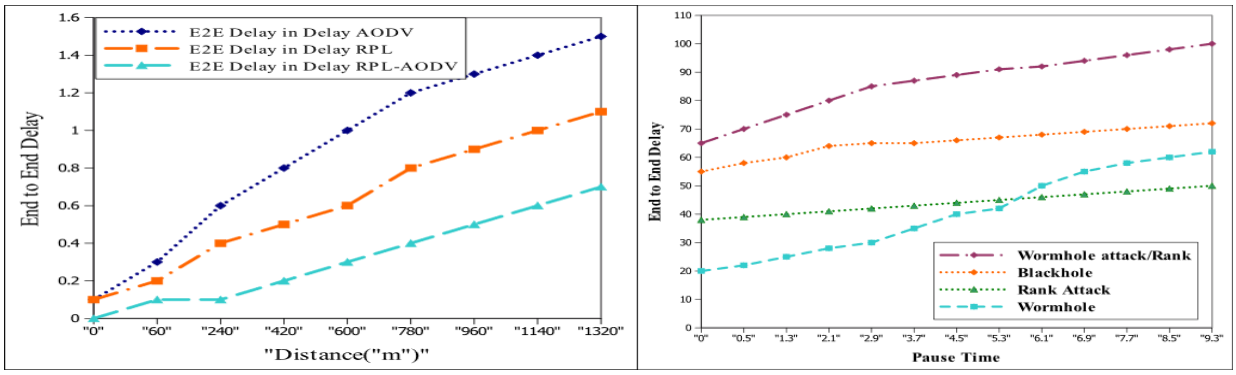
(a) Packet delivery ratio for different routing protocols

(b) Packet delivery ratio with different attacks



(c) Routing Overhead Ratio for Different Routing Protocols

(d) Throughput with Different Attacks



(e) End-to-end delay for different routing protocols

(f) End-to-end delay with different attacks

Figure 4.4: Visualization of Communication Among devices ZigBeeNetwork

mal is the class labelled for normal vectors; for malicious vectors, the class is labelled as an attack. All of the raw network packet data was gathered using tcp dump, and 43 features with the class label were generated using Argus, Bro-IDS, and twelve other methods. Each data record's notional data type or class classification is given a numeric value, such as 0 for typical occurrences or 1 for an attack. There were approximately 2,76,232 training records and 122,332 test records in the training set. Each classifier was trained with the help of a train set and validated with the test set. Normal and assault forms in the data set used to train the model are listed in Table 4.2

Traffic Type	**Training**	**Testing**	**Total**
Normal	174,217	75,332	2,49,549
Collaborative attacks	102,015	47,000	93,000
Total	2,76,232	122,332	3,42,549

Table 4.2: Proportion of Normal and Attack data records for training the proposed framework

The following category features from the dataset are of nominal data type: services (HTTPS, HTTP, CoAP), protocols (UDP, RPL, AODV, RPL-AODV, and ICMP), and so on. These categorical fields are encoded into numerical data types, each having a unique value, such as$TST = 1, URN = 2, RTA = 3$, etc. But the chosen categorization models cannot yet fit the dataset. It includes quantitative and qualitative features that could include extraneous or redundant parts that aren't appropriate for statistical technique models. However, the suggested machine learning algorithms classify the input data affected by the qualitative features available in the data source using numerical statistics. In order to create a machine-learning model that is well-trained, high-quality input data is necessary. Therefore, data must be cleaned up and prepared for fitting into the employed classification models before being visualised for quality and pre-processed before training the suggested model. The data set's features are displayed to check for correlation. When two characteristics have a high degree of correlation, they have the same impact on the dependent

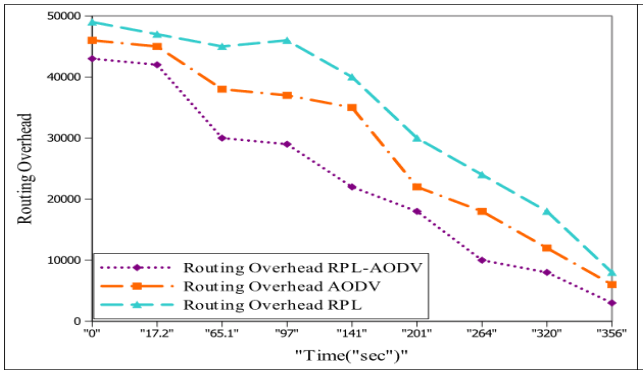
variable. To save back on computation and other expenditures, we can eliminate one of the two features. The software Pandas and Matplotlib were used to plot the data correlation. The features are ranked within the $[-1, 1]$ interval. The confusion matrix, which compares the predicted class predicted by a model with the actual class (the ground truth), is used to derive the performance metrics mentioned above. The procedure of displaying the outcomes of binary classification is known as the confusion matrix whose outcomes Table 4.3

- "True-Positive (TP)": Attacks or abnormalities that were successfully identified as attacks.
- "False-Positive (FP)": Number of Normal recordings that were mistakenly labelled as assaults.
- "True-Negative (TN)": How many records were correctly classified as normal
- "False-Negative (FN)": Attacks or abnormalities classified as normal in number.

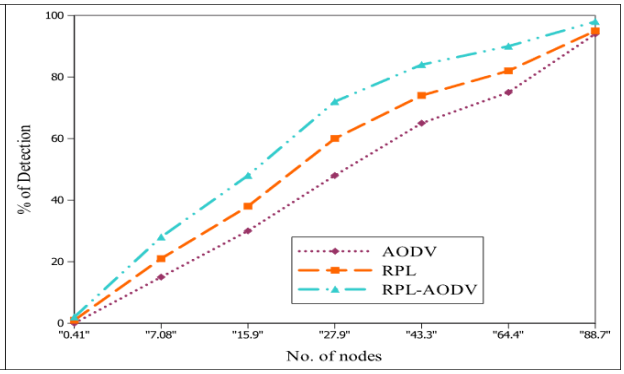
Proposed Method	**Measures (%)**			
	Packets	**ACC**	**DR**	**FPR**
Snort IDS	25,000	97.12	89.13	0.7
	97332	97.65	92.34	0.9
	122,332	98.70	89.67	1.3

Table 4.3: Comparison of Performance Metrics using Snort IDS

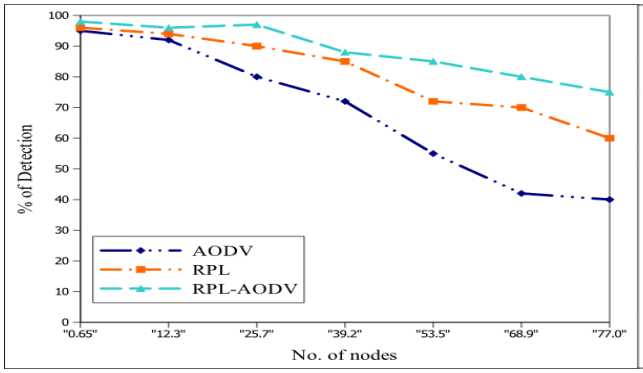
In the first step, we assessed the effectiveness of the experimental findings of the Signature-based IDS. We examined 122,332 UDP, ICMP, HTTP, RPL, AODV, and RPL-AODV control and data packets. Snort captures these UDP, ICMP, HTTP RPL, AODV, RPL-AODV control, and data packets based on the rules/signatures. These guidelines/signatures were created as group attacks to identify invasions. The output module contains a log of



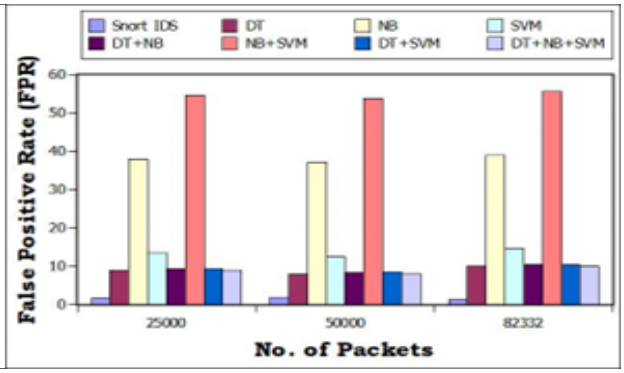
(a) Signature-based intrusion detection with one node



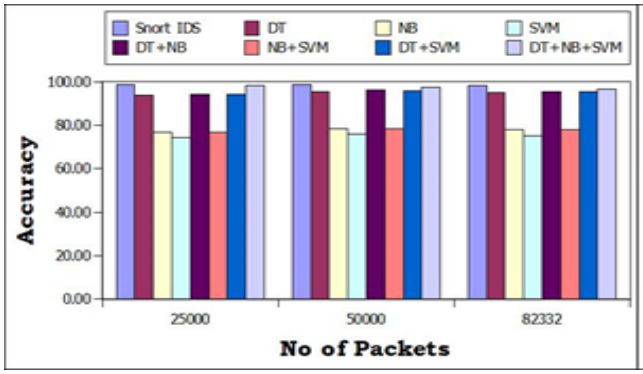
(b) Signature-specification-based intrusion detection with multiple nodes



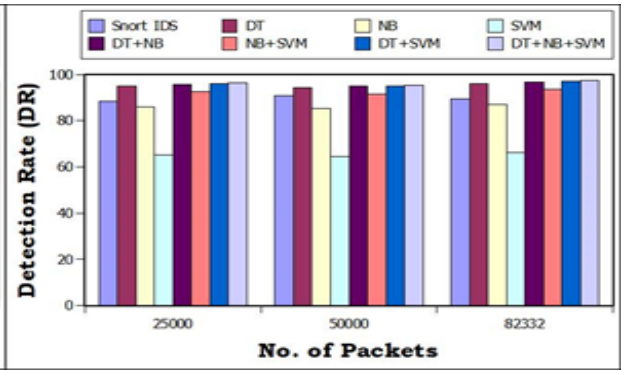
(c) Comparison of different IDS



(d) False-Positive Rate using Hybrid IDS



(e) Accuracy using Hybrid IDS



(f) Detection Rate using Hybrid IDS

Figure 4.5: Proportion of Normal and Attack data records for training the proposed framework

each and every alert that Snort IDS has produced. All these modules are tested and compared with different IDS, and results are achieved, as shown in Figure 5.11(a).

The importance of the Detection Rates of 89.13% for 25,000 packets, 92.34% for 97332 packets, and 89.67% for 122,332 packets is depicted in Table 4.3 , Figure 5.11(a). Additionally, the suggested IDS offers a low false-positive rate of 0.7% for 25,000 packets, 0.9% for 97332 packets, and 1.3% for 122,332 packets, as shown in Table 4.2. The suggested IDS also achieves great accuracy, with rates of 99.12 percent for 25,000 packets, 97.65 percent for 97332 packets, and 98.70 percent for 122,332 packets, respectively.

The data set is split into training and testing subsets in order to assess the performance of each classifier and Ensemble Method. Figure 5.11 (b), (c), and (d) depicts the performance of SVM with as accuracy of 74.1% and a detection rate of 65.3% and an FPR of 13.5%. The DT-based classification result in an accurayc of 93.7%, a detection rate of 95%, and an FPR of 8.9%. For NB-based approach, the accuracy, detection rate and FPR are 76.6%, 86% and 37.9% respectively. When the DT and NB based techniques are combined, the accuracy, detection rate and FPR are 94.2%, 95.7%, and 9.3% respectively. The combination of NB and SVM based approaches result in 76.7%, 92.4% and 54.5% of accuracy detection rate and FPR respectively. The ensemble approach of three techniques achieves the accuracy, attack detection, and FPR of 94.3%, 96.3%, and 9% respectively. As a conclusion, the proposed ensemble method outperform the DT, SVM and NB classification techniques interms of these significant performance metrics.

Detection Rate significance in which are 88.56% for 25,000 packets, 90.72% for 97332 packets, and 89.43% for 82,332 packets, respectively. Additionally, the suggested IDS offers a low false-positive rate of 0.7% for 25,000 packets, 0.9% for 97332 packets, and 1.3% for 122,332 packets, as shown in table-4.2. A high accuracy of 98.67% for 25,000 packets, 98.70% for 97332 packets, and 98.17% for 122,332 packets is finally achieved by the suggested IDS.

4.5 Summary of the Chapter

In this chapter, we proposed a cooperative IDS mechanism that detects collaborative attacks against the RPL-AODV routing protocol in LLN networks of the IEZN networks. First, we modeled the collaborative attacks that cause a more devastating impact on LLN networks than uncoordinated attacks. The collaborative model was developed to investigate the weakness of AODV and RPL protocols in IEZN networks that exploit the IoT environment's vulnerabilities. These collaborative attacks use the combined efforts of more than one attacker against the target victim. Next, a hybrid IDS has been proposed using an ensemble machine learning approach that combines specification-based and signature-based IDS as cooperative IDS to detect collaborative attacks against the RPL-AODV routing protocol that effectively monitors the IEZN network. However, security concerns will still arise with IoT-enabled ZigBee devices, which are more prone to several issues and infiltration hazards because of their limited memory complexity and processing speed, addressed in chapter-5.

Chapter 5

Keys Distribution among End Devices Using Trust-Based Blockchain System for Securing IoT-Enabled ZigBee Networks

A routing approach is needed to enable communication over greater distances in IoT-enabled ZigBee devices is discussed in chapter-3. The existing ZigBee network uses an AODV routing protocol with a flooding mechanism unsuitable for IoT networks[70]. The IoT routing protocol uses the RPL routing protocol, a unique standardized protocol that efficiently uses smart devices' energy and compute resources. It builds flexible topologies and data routing to address the properties mentioned above and the constraints of IoT networks. But this routing protocol is only used on the restricted network[39]. In chapter-3, we proposed "RPL-AODV" protocol for multi hop communication among Zigbee devices and 6BR. The IoT-enabled ZigBee network uses the 6LoWPAN protocol to communicate efficiently between ZigBee devices and the internet host [38][41]. However, security concerns arise with this protocol[1] [97]. It presents many potential security issues and avenues open to attacks and infiltration hazards because of their limited memory complexity and processing speed, as discussed in chapter-4.

5.1 Challenging Issues of IoT-Enabled ZigBee Networks

The IoT-enabled ZigBee protocol has many flaws relating to security

- The distribution of keys, as they are insecurely installed on devices or transferred over the air[77].
- All nodes share the same" master key" or" network key." If this key is compromised on one single node, it jeopardizes the entire network[1] [35]..
- Key secrecy and key distributions are vulnerable to attacks. (active and passive) [68].
- Existing protocols are based on a faulty adversary model in which all benign devices share (hard-coded symmetric keys in end devices) some secret master key that leads to worm attacks in Philip Hue lights. The use of asymmetric cryptography is power hungry, and there is a chance of security attacks such as Denial of service (DoS), Man in the middle, false data injection, etc[66].

Hence, enabling efficient IPv6 communication over ZigBee networks requires high end-to-end security rules[44].

In this chapter, we proposed the key management mechanism for the distribution of keys among IoT-Enabled ZigBee Networks utilizing a trust-based Blockchain system [23], which enables end-to-end application key establishment, Securing joining the network, Network-wide key distribution, Network key update, network access control and authentication of routers & end Devices, and storage of key credentials utilizing the Trust Security Service Provider[117]. Network-wide key distribution is more effective and efficient, as demonstrated in the implementation and validation of the proposed work compared to the current state of the art[2]. This chapter addresses the above challenging issues with the following solutions.

1. To design efficient end-to-end security among IoT-enabled ZigBee Devices by reusing the same cryptographic credentials among the ZigBee IP protocol stack using a trusted-based PBCS [29].
2. To identify and authenticate IoT-enabled ZigBee Devices using a trusted-based PBCS[2][103].

3. To securely distribute the key pairs and secure communication among the ZigBee nodes with trusted storage using a Physically Unclonable Function (PUF).

4. To enable "end-to-end application key establishment", "Securing joining the network", "Network-wide key Distribution", "Network Key Update", "network access control and authentication" of routers, End ZigBee Devices, and storage of key credentials using the Trust Security Service Provider [75] [117] [54].

5. Secure IoT-enabled ZigBee against ZigBee chain worms (duplicate symmetric keys) using a proposed PBCS.

5.2 Preliminaries and Basic Building Blocks

This section outlines the preliminary information and fundamental building elements needed for the proposed system in the form of ZigBee IP Protocol Stack Architecture, the foundation for cryptographic primitives.

5.2.1 Review of ZigBee IP Protocol Stack Architecture

This section reviews the ZigBee IP Protocol Stack Architecture, which is discussed in chapter-3. The ZigBeeIP protocol stack architecture, as shown in Figure 5.1, consists of "the IEEE 802.15.4 standard", ZigBeeIP alliance, and Applications[1][2]. "The IEEE 802.15.4 standard" consists of 802.15.4 PHY and Link Layer 802.15.4 MAC. ZigBee IP alliance provides Network Adaptation Layer, Network Layer, Routing Layer, Transport Layer, Application Support Sub Layer, Service Provider, and Application Layer[121]. When sending IPv6 packets across ZigBee networks, the IEEE 802.15.4 standard performs the necessary tasks and offers the facilities required[88]. The IEEE 802.15.4 PHY Layer provides services to the top layer, including modulation and demodulation of different transmitted and received signals, energy detection, connection quality indicator, channel selection, and clear channel evaluation[102][113]. The Link Layer of "IEEE 802.15.4 MAC" is responsible for developing beacons and syncing the device; collision-free, CSMA/CA,

Frame buffering, and polling mechanisms are employed for frame transmissions, encryptions, authentication, and reply protection [116]. The next protocol stack layer is the 6LoWPAN protocol, an adaptation layer that provides the services to the internet layers. This protocol takes the data from the ZigBee end devices(ZED) via the MAC and PHY layers and transfers the data to the upper layer[36][67]. The 6LoWPAN protocol offers various services, including neighbor discovery to the top layer, fragmentation and reassembly, stateless auto-configuration, and header compression[1] [48]. Given that the IEEE 802.15.4 protocol has a maximum frame length of 127 bytes and that the MTU of IPv6 is 1280 bytes, the 6LoWPAN protocol enables successful communication between IoT-Enabled ZigBee Networks and IPv6 nodes utilizing a fragmentation and reassembly technique that manages the improved payload[55].

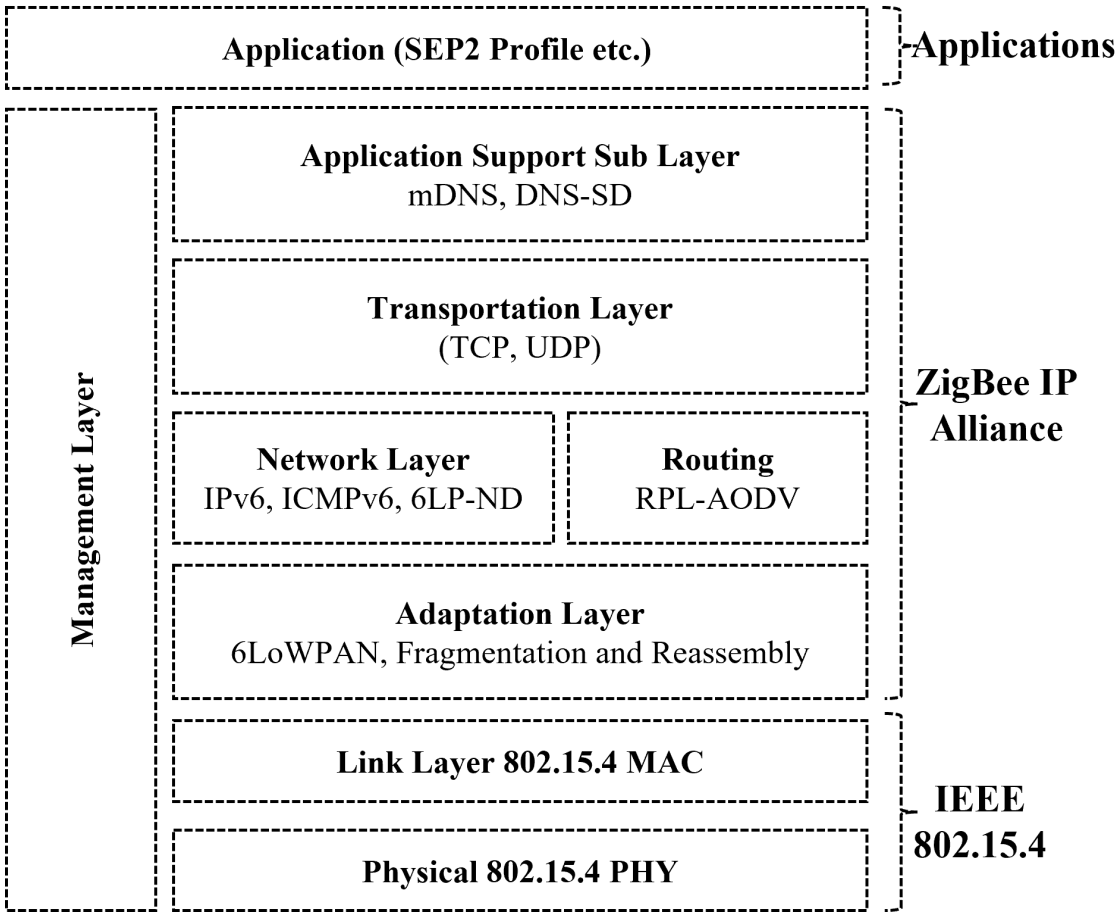


Figure 5.1: ZigBee IP Protocol Stack Architecture

The Network Layer provides a wide range of services to the IoT-enabled ZigBee De-

vices, including IPv6 addressing, packet framing, messaging through ICMPv6, neighbor discovery, and duplicate address detection. Further, this layer propagates 6LoWPAN configuration information and forwards IPv6 packets and multicast [56]. The Internet Control Message Protocol for IPv6 (ICMPv6) is a fundamental IPv6 protocol that reports errors and data generated during packet processing using error or informational messages. Link-local scoped multicast is used by the "Neighbour Discovery (ND)" and other essential IPv6 components for router discovery, duplicate address detection (DAD), and address resolution. By enabling nodes to issue meaningful addresses, "stateless address auto configuration (SAA)" simplifies the configuration and upkeep of IPv6 devices[42] [34]. "The Routing Layer uses AODV-RPL protocol," a reactive peer-to-peer route discovery protocol that can find routes for symmetric and asymmetric network flows. This routing protocol permits point-to-multipoint traffic from a 6BR to ZigBee devices and multipoint-to-multipoint traffic from ZigBee devices to a 6BR [57]. A destination-oriented directed acyclic graph with a root-based architecture handles the various traffic flows [46].

The Application support sublayer is the Management entity, a conceptual function that manages the various protocols to accomplish the required operational behavior by the node. The application support sublayer (APS) offers services to the application and network layers. In Application support, the sublayer controls node bootstrapping, node power management, non-volatile storage, and restoration of critical network parameters[21][47]. The definition for various application profiles employing Application (APL) layers will be included in the application layer, letting users take on the burden of developing applications. The over-the-air communication mechanism is specified in the application profile. Communication [27] [86][107]across devices is possible if they have the same application profiles [65].

5.2.2 Cryptographic Primitives Used in Proposed Work

This section discusses the ECC cryptographic primitives used in the proposed work. Elliptic curves over finite fields are the foundation of Elliptic curve cryptography (ECC), a technique for Public-Key Cryptography (PKC), which is used in this part to secure our

suggested system [87]. Compared to PKC, ECC employs more small keys while keeping the level of security the same. This enables encryption and decryption techniques to be used by "ZigBee devices(ZD)" with little memory and computing capacity. In our proposed system, digital signatures and key negotiations are denoted by "ECC." The ZigBee Coordinator will make "the public-private key" pair available to edge devices via ECC to let them sign messages and blocks published in the anticipated PBCS[55][51]. The suggested "Blockchain architecture" employs the "Elliptic Curve Digital Signature Algorithm (ECDSA)." ECDSA is a PKC technique that guarantees the authenticity and integrity of communications sent from fog nodes to edge devices[52], [40]. Before adding blocks, the distributed ledger verifies them using a threshold digital signature technique[20] [21].

5.2.2.1 ECDSA Signature Scheme:

Consider the EC $E : y^2 + ax + b$ where Zp is a finite field, $b \in Zp$ and $4a^3 + 27b^2 \neq 0$ a generator of prime order $'n'$; where $G \in E(Z_p)$; "The ECDSA" algorithm makes use of the hash function $H : Me \rightarrow Z_p$. Messages are inserted into fields that start with "p" in this manner. The three practical algorithms that make up the ECDSA Signature Scheme are:

1. **Key Generation Algorithm** A point on the EC and an integer are used as the private key $PrivK$ and public keys - $PubK$, respectively, in the "ECDSA" key-pair:$PubK = PrivK * G$.

   - $PrivK$ is a [0...n-1] random integer.
   - $PubK \in EC$ point multiplication used to calculate the EC - $PubK = PrivK * G$.

2. **Sign Algorithm** The message (Me), private key $PrivK$, and a signature (q, t) are the input and output, respectively, of ECDSA Sign the Algorithm. The ECDSA Sign Algorithm employs the ElGamal signature technique, which functions as follows:

   - $h = Ha(me)$ - Using a cryptographic hash algorithm, determine the message's hash value.

- securely produce the random integer $'l' \in [1..n-1]$
  $Ra = l * G, q = Ra.x$- determine the X-coordinate of the random point.
- $t = l - 1 * (h + q * PrivK)(modn)$ - the signature proof calculation
- Output q, t.

where $[1...n-1]$ is the range for the integersq, t. The random point is encoded using the Sign technique. $Ra = l*G$, along with a proof t, demonstrates that the signature is knowledgeable of the message and the private Key $PrivK$. The Public Key, $PubK$, may be used to validate the proof $'t.'$

3. **Verify Algorithm** The signed message is used as the input for the ECDSA Verify Algorithm. $'m'$, the ECDSA Sign algorithm's signature of the form q, t, and the signer's public Key $PubK$, that is matched to the signer's private Key $PrivK$. A valid or incorrect value is the output. As seen below, the ECDSA verification algorithm follows:

   - $h = Ha(m)$ - compute the message's hash
   - $sig = s - 1(modn)$ - the inverse modular proof of the signature.
   - $R' = (h * Si) * G + (q * Si) * PrivK$ - recovering the signing-related random point
   - $q' = R'.x$ - determine R's x-coordinate.
   - If $q' == q$, genuine signature

5.3 Trust-based Permissioned Blockchain System pBCS to Distribute Keys across IoT-enabled ZigBee Devices

This section presents the proposed trust-based permissioned Blockchain system pBCS to distribute keys across IoT-enabled ZigBee devices. The proposed pBCS, called Blockchain: The "Trust Security Service Provider (B-TSSP)," provides the open trust model that allows end-to-end security among IoT-enabled ZigBee devices by reusing the same cryptographic

credentials among the ZigBee IP protocol stack on the ZigBee edge device with trusted storage using a Physically Unclonable Function (PUF) mechanism as shown in Figure 5.2.

The Trusted Blockchain will create the signed certificates using a private validator key commonly used as a root of trust. All the ZigBee coordinators, Routers, and End Devices must be enrolled with a BCS before their operations are performed. The ZigBee IP Coordinator is the full-function device that can initiate a new ZigBee network and maintain the Blockchain system. According to the ZigBee Alliance Specifications, each ZigBee network must have a single coordinator. The End user will communicate with any ZED only through the ZigBee IP Coordinator when an existing ZigBee network needs to accommodate adding a new end device. Then the user must change the network's status through Blockchain DApps from closed to open state and send the exact request (available form) command to the coordinator. Then the smart contract of the Blockchain system will verify the state and change the system's state. When the ZigBee network switches to an open state, the coordinator authorizes the broadcast of a join response message, telling all ZD that the network is now accepting new joining requests and is in an open state. On the other hand, the ZigBee network cannot accept any new devices once it has reached the closed state. Only the trusted, Permissioned Blockchain can create authentically signed certificates.

Any router or edge device that holds the validator's public key can validate the signed certificate and guarantee the public key's integrity. Finally, the Secure Communication Protocol is designed to transfer the data between the ZED and the coordinator via a registered ZR. This Secure Communication Protocol derives the shared secret key between the coordinator and edge devices in the untrusted field for authenticated and encrypted communication . In this Secure Communication Protocol, we performed mutual authentication with less Non-volatile memory (ROM). The Blockchain validator and ZED must be enrolled in the BCS before performing the mutual authentication. This proposed BCS solves the problem of less usage of Non-volatile memory and improved key management. The Blockchain validator will access the shared ledger that stores the digital key credentials of all the enrolled ZED and ZigBee Routers (ZR), including the ZigBee Coordinators.

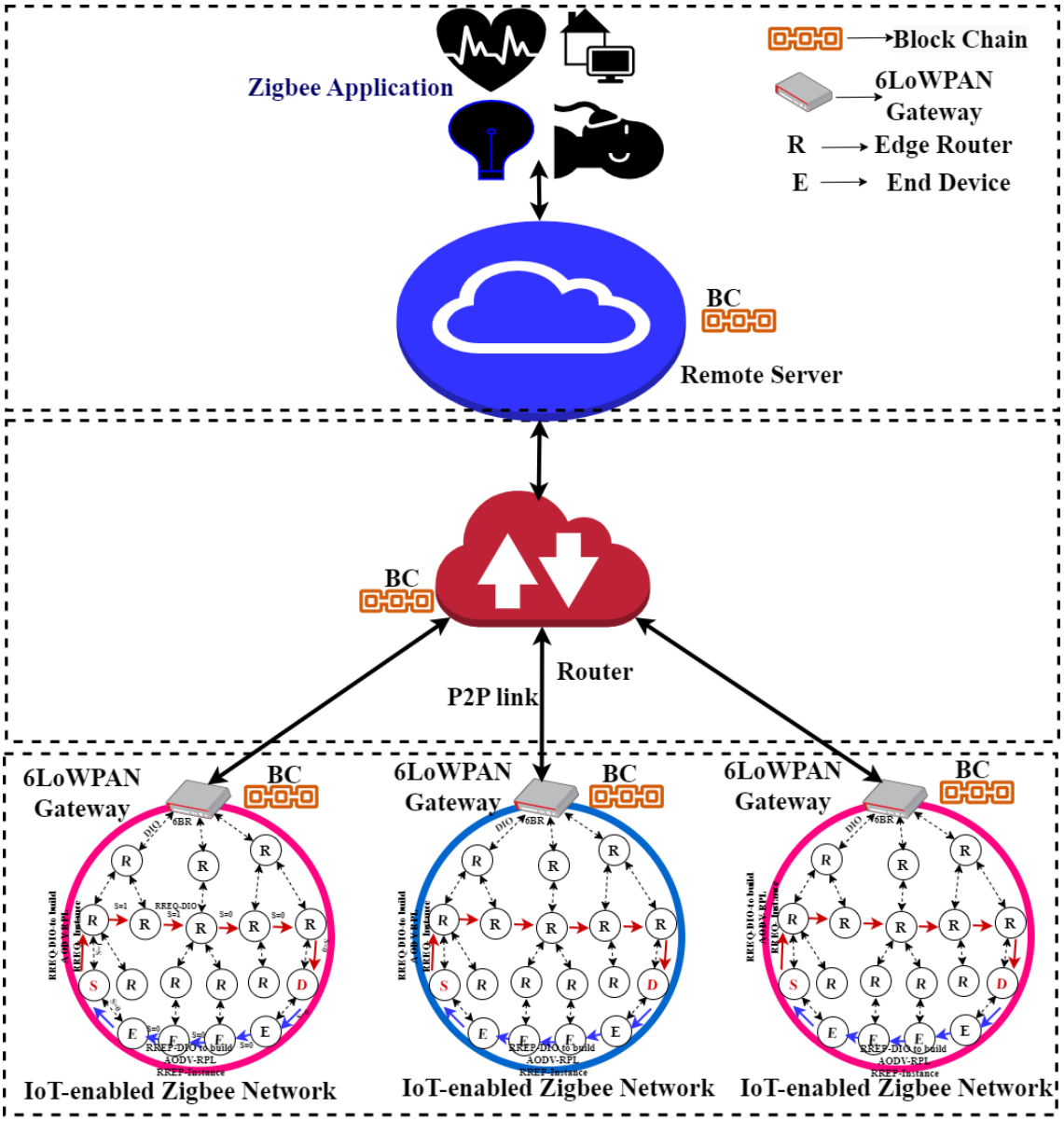


Figure 5.2: Proposed Architecture of Permissioned Blockchain System pBCS

5.3.1 ZigBee IP Protocol Stack Security Architecture

The proposed ZigBeeIP protocol stack security architecture, as seen in Figure 5.3, is made up of the "IEEE 802.15.4 standard Security", "ZigBeeIP alliance Security," and "Applications Security." The IEEE 802.15.4 standard supports the Link Layer (MAC) and PHY (802.15.4) security. The ZigBeeIP Alliance offers Network Adaptation Layer Security, Network Layer Security, Routing Layer Security, Transport Layer Security, Application Support Sub Layer Security, Application Layer Security, and Blockchain Service Provider. All the layers are discussed in the following subsections.

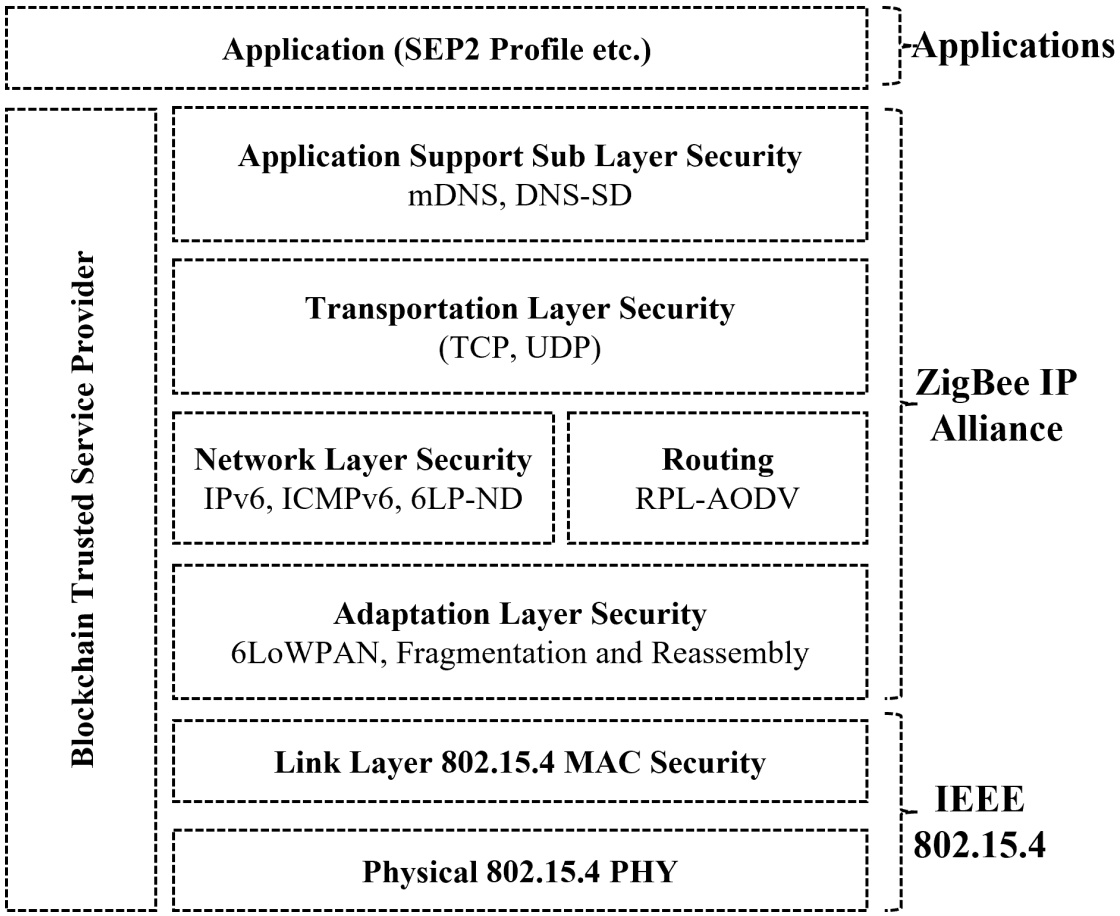


Figure 5.3: ZigBee IP Protocol Stack Security Architecture

1. **Blockchain – The Trust Security Service Provider:**

   The proposed Blockchain system called Blockchain-The Trust Security Service Provider (B-TSSP) provides an open trust model that allows end-to-end security among IoT-

enabled ZigBee Devices by reusing the same cryptographic credentials among the ZigBee IP protocol stack on the same ZigBee edge device. In other words, this proposed BCS provides the trust security service to the ZigBee IP protocol stack. This B-TSSP enables the security procedures by providing various security services such as end-to-end application key establishment, joining a secured network, network leave, Network-wide key distribution, Network Key Update, network access control and authentication of routers, end ZigBee Devices, frame protection, storage of key credentials, restoration of critical security and network configuration information, and security mechanisms for the Network APS Security sublayer. Figure 5.3 shows the Proposed ZigBee IP Protocol Stack Security with Attack Landscape.

2. **The Physical Layer Security:**

   PHY security confronts several obstacles, and typical wireless physical layer security solutions are difficult to implement in ZigBee contexts. Most ZigBee devices have modest data rate needs, periodic data traffic arrivals, minimal hardware, signal processing capabilities, and sensor levels. Various aspects must be considered, including multi-path effects, fading, unpredictability, the sensors' geographically scattered nature, and heterogeneity. Furthermore, basic PHY assumptions include the adversarial model, the heart of the wireless channel, and practical considerations during implementation. As the IEEE 802.15.4 standard implies, the PHY offers no security services.

3. **The MAC Layer Security:**

   Communication devices must often share a standard secret key to use upper-level security services. A pre-shared private key is already pre-installed on each device on the network. PHY should work with upper layers to provide various security levels if security services are requested. Secure Communication between ZigBee devices is made possible by the security of the IEEE 802.15.4 MAC layer protocols. These MAC-layer protocols use AES-CCM encryption to maintain data integrity and guarantee data secrecy. AES is the most commonly used technique for encrypting data on the MAC layer. MAC-layer protocols offer decent security services. However,

there are still specific, important issues that are not covered. Since it may safeguard MAC layer data and higher layer headers, MAC layer security is typically seen as more secure than the upper layers. Deposits at higher levels are unnecessary if MAC layer security is enabled.

4. **The Adaptation Layer Security:**

   The adaptation layer provides services to the network or internet layer by taking the data from the end devices. As shown in Figure 5.1. IPv6 requires a minimum transmission unit of 1280 octets, while IEEE 802.15.4 only allows for a maximum ZigBee MAC frame size of 127 bytes, with 25 bytes for frame overhead and just 102 bytes for the payload. Suppose the link layer adds an Auxiliary Security Header to the MAC frame for security reasons . In the worst-case scenario, the problem worsens, leaving only 81 bytes for the IPv6 packet. As a result, an IPv6 packet will not fit into a ZigBee frame. Furthermore, the upper layers have just 41 bytes because an IPv6 packet's IPv6 header is 40 bytes long. The IPv6 header allows only a few bytes of space for application data by reserving either the 8-byte "User Datagram Protocol" (UDP) header or the 20-byte "Transmission Control Protocol" (TCP) header added at the transport layer. The Adaptation layer uses the "IPV6 over Low Power Wireless Personal Area Networks" (6LoWPAN) protocol with IP communication capabilities to communicate with all ZigBee-enabled sensor nodes. The 6LoWPAN protocol provides end-to-end Communication between IoT-Enabled ZigBee Networks and the Internet host. Once the 6LoWPAN protocol receives the query from the internet host or end user, it performs the three primary services: (i) To meet the IPv6 minimum MTU requirements, fragmentation, and reassembly are used. (ii) Header compression: removing fields that may be deduced from link-level information or based on basic shared context assumptions. (iii) Link-layer forwarding is supported to transport IPv6 datagrams over many hops.

5. **The Network Layer Security:** : Network Layer Security provides a wide range of services to ZigBee-enabled devices. When an "NWK layer" frame needs to be secured, it uses "AES encryption/authentication" in the Enhanced Counter with a

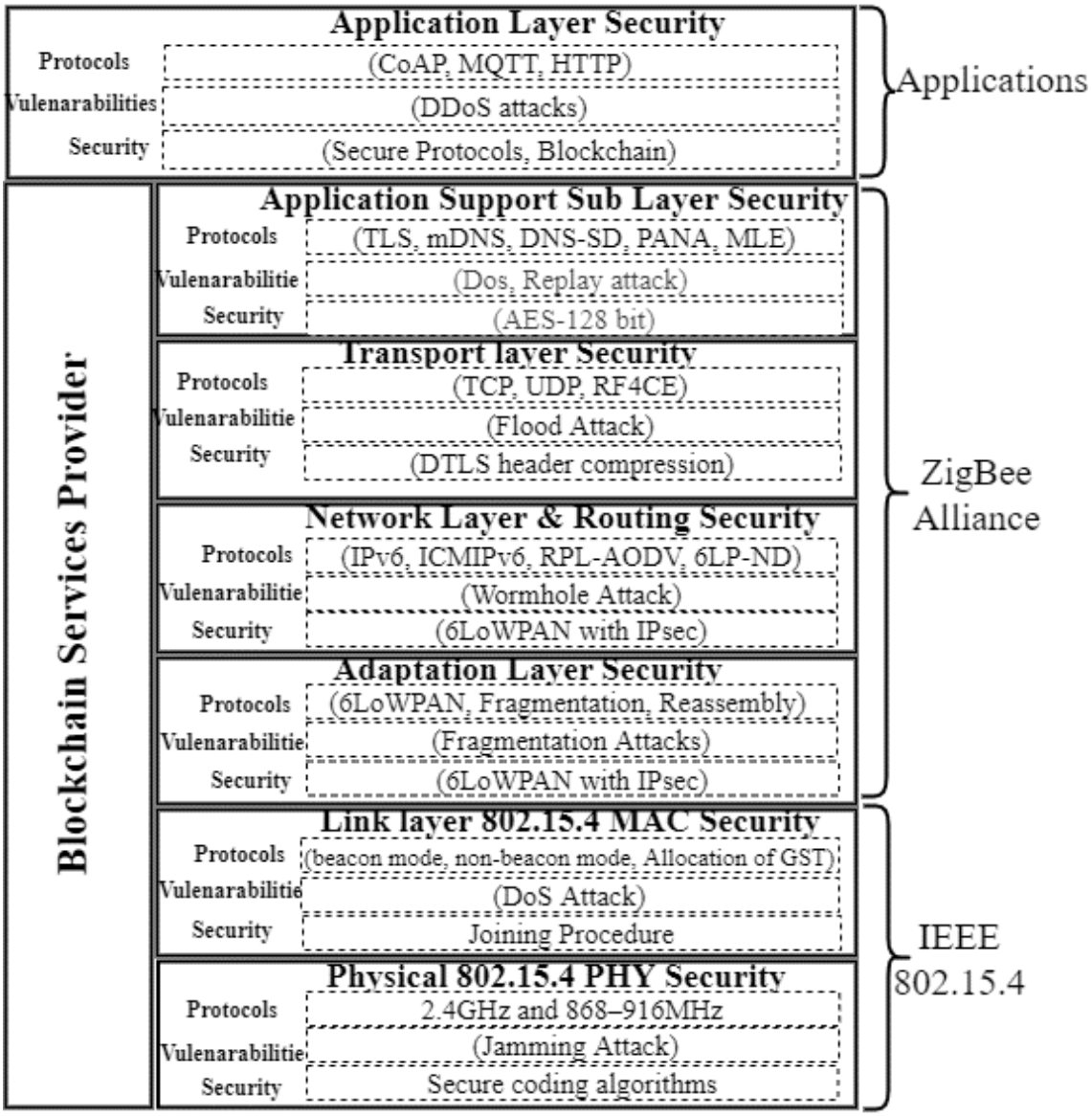


Figure 5.4: Proposed ZigBee IP Protocol Stack Security with Attack Landscape

"CBC-MAC (CCM*)" mode of operation. The "NWK layer" secures the transmission and reception of outgoing and incoming frames. The upper layers manage security processing operations by establishing security keys. The Routing Layer uses the AODV-RPL protocol, a reactive peer-to-peer route discovery protocol that can find routes for symmetric and asymmetric network flows. This routing protocol permits point-to-multipoint traffic from a 6BR to ZigBee devices and multipoint-to-multipoint traffic from ZigBee devices to a 6BR. A destination-oriented directed acyclic graph with a root-based architecture handles the various traffic flows (DODAG).

6. **The Transport Layer Security:** The Datagram Transport Layer Security (DTLS)" protocol is based on the TLS protocol. It can provide similar security guarantees while maintaining the datagram delivery model as shown in Figure 5.4. The DTLS provides authenticity, including "data origin authentication," "identity authentication," "integrity," and "confidentiality." DTLS operates on top of the "unreliable transport protocol UDP." DTLS is used with PANA and EAP to authenticate a joining node and the "Authentication Server."

7. **The Application Support (APS) Sublayer:** The "Application Support (APS)" sublayer interfaces the NWK and APL levels through a wide range of services provided by APS data and management entities. The APS sublayer handles incoming and outgoing frames to establish and manage the cryptographic keys and enable safe transmission and reception of the frames. The APS sublayer receives primitives from the above levels to access its services. Entity Authentication, Permission Config Table, Establish Key, Transport Key, Updating Device, Removal Device, Request Key, Switch Key, and Device Update and Removal are among the services that comprise APS Layer Security. Support for Application Security protocols, service discovery protocols, encryption methods, and authentication procedures are all integrated to provide sublayer security.

8. **The Application Layer Security:** This layer offers direct end-to-end security at the application layer. The Constrained Application Protocol (CoAP) is one of ZigBee's most popular application layer protocols. The Internet Engineering Task Force's

working group on constrained RESTful environments (CoRE) has suggested CoAP (IETF). The CoAP, however, does not offer any security services. To protect CoAP messages concerning secrecy, integrity, authentication, and non-repudiation, it integrates with DTLS. CoAP specifies four security levels that vary in how key negotiation and authentication are accomplished.

9. **Physically Unclonable Function (PUF):** We assumed the IoT-enabled ZigBee devices support PUF and have trusted storage. The characteristics of the IoT-enabled ZigBee device are based on the manufacturing phase, as every ZigBee device will have unique features. So, it can generate key pairs based on the device's physical characteristics. The proposed BCS distributes the key teams and securely communicates among the nodes. Network Key (NK) and Unique Link Key (ULK) are the two types of keys used by the ZigBee alliance, serving many objectives, including joining the network and ensuring nodes can communicate securely. Suppose the ZD with the PUF model supports underground storage. This enables keys based on the device's physical properties to be generated.

5.3.2 Registration Phase: IoT-enabled ZigBee devices in pBCS Network

All the ZigBee coordinators, routers, and end devices must first be enrolled with a pBCS before their operations are performed. The trusted Blockchain will create the signed certificates using a private validator key commonly used as a root of trust. Only the trusted, permissioned Blockchain can create authentically signed certificates. Any router or edge device that holds the validator's public key can validate the signed certificate and guarantee the public key's integrity. Figure 5.5 shows the node joining procedure in a secure Blockchain network.

The following registration phase is discussed below.

1. The APUF response of the ZED is enrolled with the Cryptographic Key Generation (CKG) function. With the help of the CKG Function, the ZED will reconstruct the key pair.

2. The ZED Identifier, called Device ID, is a unique identifier performed by incrementing the global counter of the manufacturer.

3. The ZED ID and its Public Key are sent to the permissioned Blockchain System (pBCS).

4. The pBCS network binds the ZED ID and PUF Public Key and creates the signed certificate using the coordinator/Validator private key.

5. If the ZED enrollment succeeds, the same secure procedure will be performed with the coordinator/validator registration process.

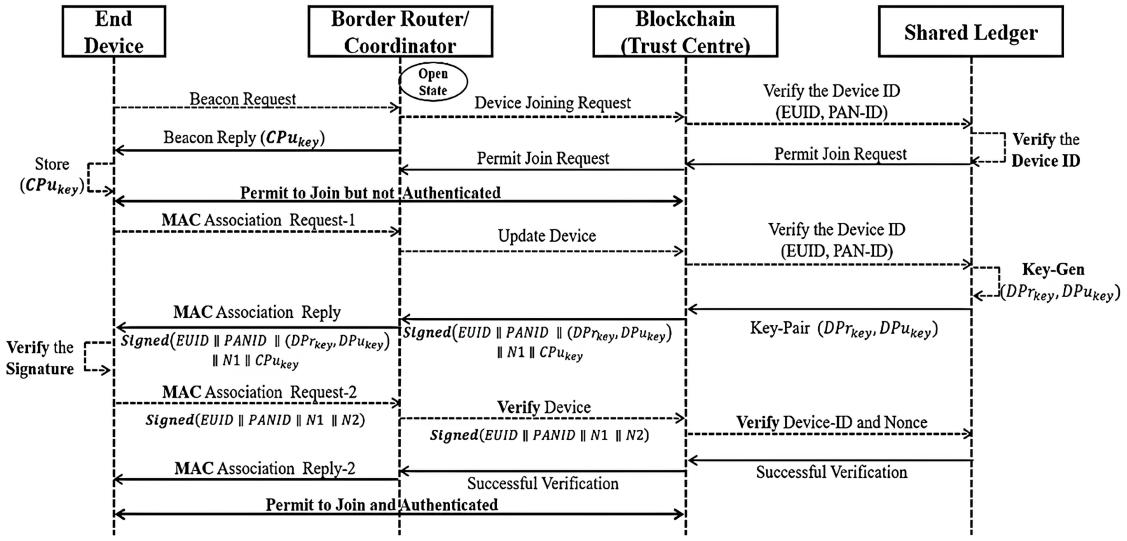


Figure 5.5: Node Joining Procedure in a Secured Blockchain Network

5.3.2.1 Joining a Secured Blockchain Network.

The ZigBee IP coordinator is the full-function device that can initiate a new ZigBee network and maintain the Blockchain system. As per the ZigBee alliance specification, there must be a single coordinator for each ZigBee network. The end user will communicate with any ZED only through the ZigBee IP coordinator. If a current ZigBee network has a new end device that the end user wants to add, Then the user must change the network's status through Blockchain DApps from closed to open state and send the exact request (open

state) command to the coordinator. The Blockchain system's smart contract will then confirm the status and modify the system's state. The coordinator authorizes the broadcast of the join response message, telling all ZD when new joining requests are allowed and when the ZigBee network has shifted to an open state. On the other hand, once the ZigBee network is closed, no new devices are allowed to join it. Figure 5.5 shows the Secure Key Exchange and Authentication Protocol Using APUF and the Blockchain system. The process for adding a node to a secure Blockchain network is as follows: Each new joiner device must follow the process to connect to a secure Blockchain network using a ZR.

- The Joiner end device continuously broadcasts, beginning the joining procedure by broadcasting an unencrypted beacon request frame and waiting for the reply message, as shown in Figure 5.6. The coordinator will verify the joining device's Device ID (EUID, PAN-ID) through a smart contract on the Blockchain. After verification of the smart contract, issue the permit join request to the coordinator.

- The coordinator provides the unencrypted beacon acknowledgment for routers to join the ZigBee network. The ZR's MAC address, Personal Area Network (PAN) ID, and unencrypted beacon message coordinator public key

- The Joiner end device is declared to have joined the network but is unauthenticated.

- The Joiner end device initiates a connection with the ZR by sending an association request message 1. The ZR requests the Device Update from the coordinator. Once again, the smart contract will verify the Device ID (EUID or PAN-ID) and generate the Key pairs using Gen-Key from the Blockchain system.

- The smart contract will create the signature. Send the ZR. The ZR replies with an association response message to the joining end device.

- The Joiner end device will validate the signature with the coordinator's Public key.

- The coordinator's Public Key The joiner, ZED, will use it to validate the signature.

- The Joiner end device sends a signed association request message 2 to the ZR. The ZR requests the Device Update from the coordinator. Once again, the smart contract will verify the Device ID and Nonce from the Blockchain system.
- After successfully verifying the signed association request message 2, The smart contract will send the Successful Verification notification to the ZR. The ZR replies with an association response message backing the Permit to Join and Authenticate to the joining end device.

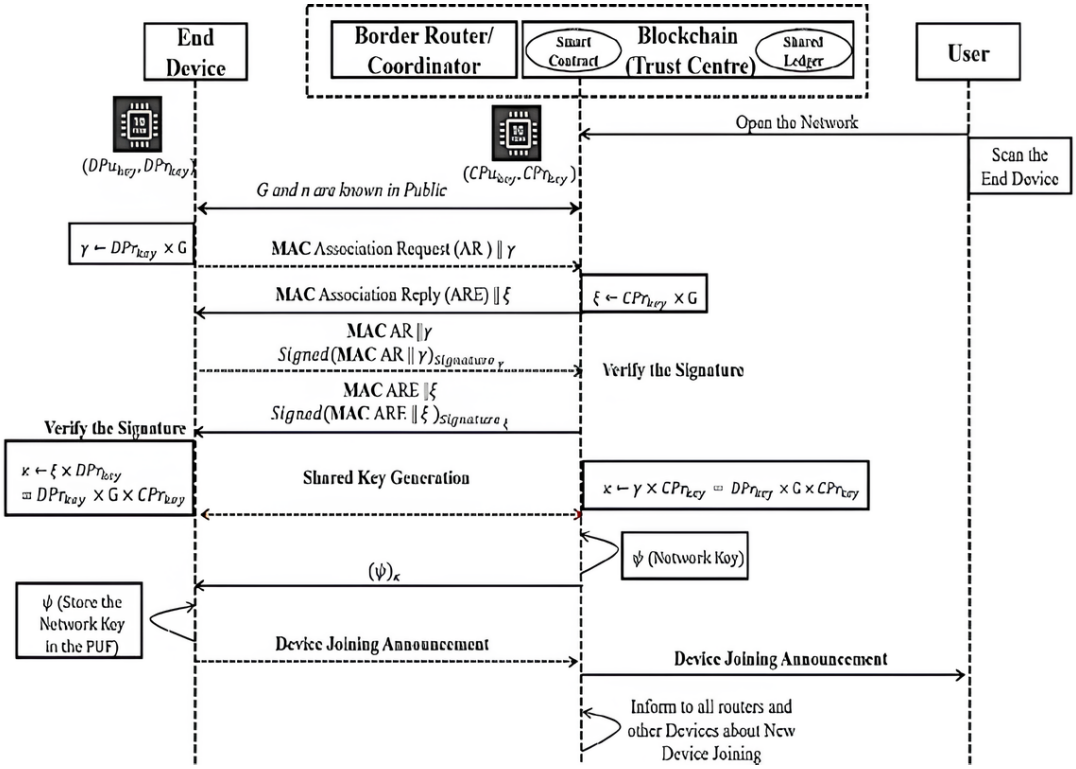


Figure 5.6: Using the APUF and Blockchain systems, a secure key exchange protocol

5.3.3 Authentication and Secure Key Exchange Protocol

A secure communication protocol is required to transfer the data between the ZED and the coordinator via a registered ZR. This protocol derives the shared secret key between the coordinator and edge devices in the untrusted field through authenticated and encrypted communication. In this secure communication protocol, we performed mutual authentication with less Non-volatile memory (ROM). The Blockchain validator and ZED must

be enrolled before performing mutual authentication. This proposed Blockchain system solves the problems of less usage of Non-volatile memory and improved key management. The Blockchain validator will access the shared ledger that stores the digital key credentials of all the enrolled ZED and ZR, including the ZigBee coordinators. The following key exchange and authentication occur whenever communication is needed between the ZED and the coordinator via a registered ZR in a secure and authenticated manner.

10. Coordinator secure, shared Key G

5.3.4 Keys Updation:

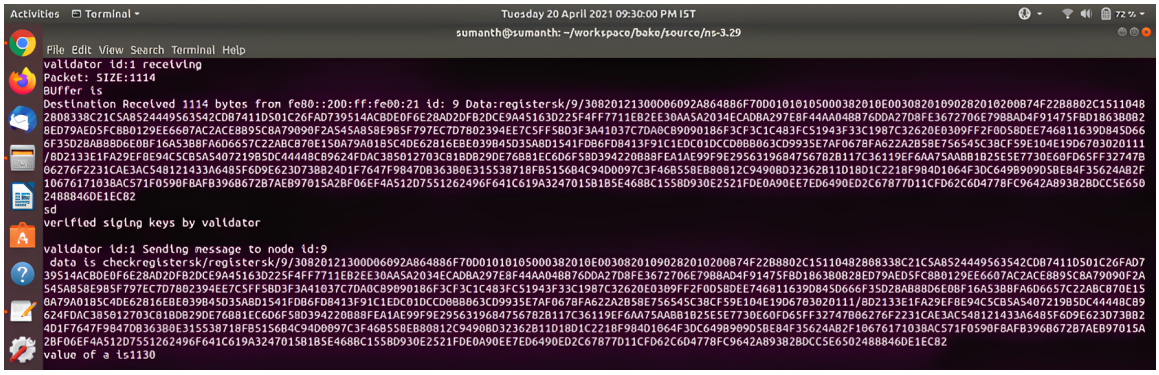
If ZED wants to update the keys, The APUF response of the ZED will generate the Cryptographic Key Generation (CKG) Function. With the help of the CKG Function, the ZED will update the key pair. The update of the key pairs will be sent to the ZC. The ZC will verify the request through a smart contract, and after proper validations, the same agreement sends the updated confirmation back to the ZED. Otherwise, it will discard the transaction (request).

5.3.5 Implementation and Performance Analysis

This section presents the proposed protocol and its attacks implemented in the network simulator NS3, which has been tested on a network of 10 to 500 nodes that enable the IoT-enabled ZigBee network. The findings are provided together with a performance analysis to assess the feasibility of our proposed work with various performance metrics such as Throughput, Transaction Delay, Authentication, Encryption, and Decryption. The simulation parameters are shown in Table 5.1. Further, we utilize the dataset generated by the simulation NS-3 in the form of PCAP raw packet capture and Trace (tr) files. We use Wireshark in and Response packet content shows the temperature value. Table 5.1 shows the simulation parameters.

The figures from Figure.5.7 (a) shows the results of information processed within the pBCS network. The proposed work's GUI front-end results, evaluated in NS3, are shown in the Figure.5.7 (b). The following Figure.5.7 (c) shows the implementation results of the


Activities
Terminal
Tuesday 20 April 2021 09:25:00 PM IST
sumanth@sumanth: ~/workspace/bake/source/ns-3.29
File Edit View Search Terminal Help
node id:5 Sendlng message to validator id:1
data is reglstersk/S/30820120300D06092A864886F70D01010105000382010D0003082010820820101 0C6F28C93AD4AB49AD3DBDE10F34BEE996194BE1E59B449E07E82FACB87B77D38889DCFD7B92A8918 05BEF17D062C3FB4F22E5FAB30F729A15AD1369230377E5B193FFDB2784F3BD3DA6586F2CA0BD3981C623F3D0B59760E63SDB681C908EF38B026EEF4AB11B42CD02209471FBCB604D16DD0E5F7D96122S3O2D2F E567ED284F78FAC6E8BCC6FAAC457528FC35FAFE8C85CEF8903627CBD2S04979F7C66B8782F750E28BE79A583DDDF55361B1E1B7AEF963B84D2CE2115F32D53CD7EC0BCD322E575DC1F3AF57892F31B28D38F76 347F98DF69634A60BFF37E762CA94947FBC375274661 42FE084A2A599722D877B2E13DAF70130092BA920633EF63B4E6B8F020111/02D927ECF8D42758EE46B6621E7AA3BA1E513A702C4479614032995D75F619 2832AB034F838F638B25B5664B47ADF037D3D1646566829CAFEA135B66A67C0FBBF03DAA58044DEB03148A69293FC3A2172FEB20477D0220C252B7EAEB8CF2DF76DB9FA5F2F169B0B19BD9E378BDD51FC23F012 6EAD33862D8A9D0A3D172S6DD1A41F34B0632FDC98E4BCEE9EE9BAB073B57B6B147B6055S2E6B760201B1E198BEB2F0B84AAF8BDF3C45372D5F161BB2AD49BC1BB34D457641E9DB777ED6250FABE23289EE489D1 0AEB43CB7F411E2273EDFDAB3C9C18006E7BF852E24E723F7C882D07B033FF9A09EBD339S4FA292454A70DFB11C5D4387421785CB9782780AAB1E9D
value of a is1112
node id:5 Sendlng message to validator id:1
data is reglstersk/S/30B2011F300D06092A864886F70D0101010500038201 0C003082010702820100060 43C111AD85 1D4F6CAE59DC069A1AF2C3C3C826AFB69B1EB6CF545C52F70C78842AD5B1A3C26EE6D 366S6B48932164F0357DCAB3C7075B8D6A4269E6C914BAEF63EC4D9DCBC7480A732567BBCAA80795S3FD1C3821B2C43DE7B359241 19E488C1F6207936942049D1924312B84DED1F937C1FEF8630C413A765959 7 0FCE45607D188393FEB9DC36344D662135B898E2083D14028F31FA2EDFCC1943351E964F6853E3063DFA7791CADFB802E74FA40C8B413C0DEDDDEE60AF828E2D37A610A237E449FA07CCB4C36080AF16581FE1 0E85A240BC5B50E831BE613738B39F0983D4B09826E4D434CD5F326E5BFBE24B1CC605F636DE29EFD00426ACCEB8C49D1020111/0306A066BC6FC0B03F9E1D79FD2BAAB08C8376ED07A910BE713A174EB21EE2B ABF4B202DF8949E2F4D77A591541DC888B974E0A7F3D76F27F6A13BE385C85544893688774C969B834B169F4CC9D6DBE542EB0607182B4526C8347A1A30B24BCC14B4C9DB035DD1350D288E53AC72C79A24D993 F7876622B3EE956BDF231674CFE44B99C4F5D5914661 7B3CA66BD6D032B7ECF5D52DC219DDFE33D0F0EDE746DF40865497E0D2E21F033705 2D19E1374BFAAFBDB1266F702B2542308F3A37EBA994E922DEB19BC CA2FBBE0A5DD61272FCC05B80E3CF1F6846D1BAA69B6736C9AABAB25B5F1F9D865DBA8BABCE5F4A85F1079E6C0C6D1BA4E68D97A93ACODC112719
value of a is1110
node id:6 Sendlng message to validator id:2
data is reglstersk/6/30B20120300D06092A864886F70D0101010500038201 0C003082010802820101148B725A3AE538FA6026CA6F790F9C7BE3C269F2CD27872AEBDC1971100F7E16D3C1940A7A1DDC27E D9F24F7E573B718EBF6B6899B135AE13C8DE93ED9511620ADED156D009B2FDD33B6768 1CEESA6408C43C5756C448SEASSD51E173F9D27470FEBB00A2EC3SD3EE4AB4AFFBEEE5E50774097E9174D21BCC0E2A11C 489087B128192389D9791F1B250B31749DA5B814A64E4D48FC6D8CB88C242F1CF709B440B5D287EE9E77S80247D7B53A30EF1F5720532B9FE44BDC22606ADBEEAEDC31539F948F9EDAE92274577FA046B5SECAC 7CACDE0695716A616FF692B8CA59AE045F2F73E45452D092781ED43D3SF019A0027F4C23360933A3E074AF373S62BB387E1020111/04EA94C71BCFD25439EA3465B8B8BAD4E6C422C98FF8F6E50E353376A017D 41ED4BDA7450BE7S83CS31AEE1E859771B0AAC41866B73C42E731C9A1D96160636CAFED87E9BD79AF672D98F8FA1914BAB1E9D7F25D940SDDB6ES4118EC4614B6319CC8C13883F559E2F0A2FA667E0SCBF37B9 F71F0A0648AE6C4F618046C0EA58F5A50E2C488A3BFCC085C9A29DF9FCB417688CDF109D0CC9F6130CDA81C52AA58C7AAC6A15SD80CEF719AF0CE4D6A6D0CC7E7988BEC26200223D542D89B606B5SE327F92A37 DE22F62C3AD0E91F23178SFD7FB998BC0S30C5E64BCFFB0S1769335EA17BC97DA2A59893A2DA6F45SC5446EF27C9BD8C0868C19472C2CAE07293C6
value of a is1112
node id:6 Sendlng message to validator id:2
data is reglstersk/6/3B2011F300D06092A864886F70D0101010500038201 0C003082010702820100032C6407F163DC96C1B801A05DCE5B5CEC2278SAED945B5F1BAFF76716SE4657SB1FD91F265D1838 5ABB04FE56E75D96FCEC22FAC92BEDEB0C410D3FE93D68876BDB017DDFA7A7429EA763CC69ECE9F2F2012AD9EF739F2470192S3F1F6D5OA0886C436BBF983C3D2067BFB16DA6DA3FC59A7946 3C50F7AA1F3584E 40E62745770F9F236AF714CA46126412A629FA1372156A34AAA6E65BAB9D1D11C36FF2E18C4ABB044FE97D45E3BA3BC85FAE561F6B5C552D189C0B1CE69AEC8152BA899AE96FC3E79ABBFB90D57E4CB5A5718B3 C5B65826CEC32A06211AB1D4A1BAFF393708A9E2C509003F3B6746B71F8EA94F676792BD5F58213D997A66CA0BB7F2AS5020111/083925FE88C4E54186B0D22814AB1B30B509230F64CE19F1A7C6940FAB2AAB2 D46678D5E89BA7FF38SBA1108E233BDEB7B22ADBEC7480C10B6466C69F0DFB620F0D370553C83CC59FEBB10AB74D6B06AB0EDBD67A6F9466D710D8A017744243 8FAAE6F923SDBA19BDBBAB9BA0C8EFEBE879E1A F4587D10B283B1A47CBA24E1BB869216D6E545F4FE6B457A74C90F1DDF531F7D52CA762F098C97AB3BC0SD997EBBEE544BDDCCD44ABC9F6747E447EA089AA410A95E1SA52E653C6637ADCC022CBA9CB77292DF4 4D665S07DA3C4A516F146D42DS9B1BDA9008E8E2F68E16D4C63FC7D97E52E371E8FF2C01D7925G3667606488786E1D9DC4E36BF706D22F906DFBD
value of a is1110
node id:7 Sendlng message to validator id:3
data is reglstersk/7/30820120300D06092A864886F70D0101010500038201 0D003082010802820101343AEF50136E413A5F46E2406B0154F888DDFDD6C3B007F683024FA0DA8BF793C7501E0E19337B8B4 9C00984B50EF1E30171A34AE94D8265SEED60CED2ED40B5775B04D92F9127C29DA7D391E3C855B3356162305E7CBA4C4CF35D9BF33174A991C931BA34D24ABC957DE740E03687FA8FF37080C6B409DA7DFE08B 94E60E5F4E1B7089BSDCA2014E0CDF88FE15275E92F815BDD357B0C4ACA0F31F148C4563E00C77F418E32E6B213C575BB84A9A4B0CC704CD4CAE4BC415B165AC3D787B5529DD6D080D8564FD20EA54961773E6E
(a) Registration Response Communication from Validator in Blockchain System


Activities
Terminal
Tuesday 20 April 2021 09:30:00 PM IST
sumanth@sumanth: ~/workspace/bake/source/ns-3.29
File Edit View Search Terminal Help
validator id:1 receiving
Packet: SIZE:1114
BUffer is
Destination Received 1114 bytes from fe80::200:ff:fe00:21 id: 9 Data:registersk/9/3082012130OD06092A864886F70D0101010500038201 0E0030820109028201020B74F22B8802C1511048 28D8338C21CSAB52444956354 2CDB7411D501C26FAD739514ACBDE0F6E28AD2DFB2DCE59A45163D225F4FF7711EB2E3DAA5A2034ECADBA297E8F44AA04BB76DDA27D8FE367270E79B8AD4F91475FBD186380B2 5D79AED5FCBB8329EE6607AC2AC8895C8A79090F2A545A85BE985F797ECD7B02394EE7C5FF5BD3F3A41037C7DA0C89090186F3CF3C1C483FC51943F33C1987C32620E0309FF2FD058DEE7686116390B45D66 6F35D2BAB88D6E0BF16A53BBFA6D6657C22ABCB70E15DA79A01B5C4DE62816EBE039B45D35A8D1541FDB6FD8413F91C1EDC01DCCD0B8063CD9935E7AF0678FA622A2B58E756545C38CF59E104E19D6703020111 /8D2133E1FA29EFBE94C5CBSA5407219B5DC4444BC8964 2FDAC385012703C81BDB29DE76B81EC6D6F5BD39422OB88FEA1AE99F9E295631968475670B117C36119EF6AA75AABB1B25E5E7730E60FD65FF32747B 06276F2231CAE3AC548121433A6485F6D9E623D73BB24D1F7647F9847DB363B0E31553B718FB5156B4C94D0097C3F46B558EB80812C9490BD32362B11D18D1C2218F984D1064F3DC649B909D5BEB4F35624AB2F 10676171038AC571F0590FBAFB396B672B7AEB9701SA2BF06EF4A512D7551262496F641C619A324701SB1BSE468BC155BD930E2521FDE0A90EE7ED6490ED2C67877D11CFD62C6D4778FC9642AB93B2BDCC5E650 2488846DE1EC82
sd
verlfled slging keys by validator
validator id:1 Sending message to node id:9
data is checkregistersk/registersk/9/3082012130OD06092A864886F70D0101010500038201 0E0030820109028201020B74F22B8802C1511048280833 8C21C5A852444956354 2CDB7411D501C26FAD7 39S14ACBDE0F6E28AD2DFB2DCE9A45163D225F4FF7711EB2EE30AA5A2034ECADBA297E8F44AA04BB76DDA27D8FE3672706E798BAD4F91475FBD1863B0B28ED79AED5FC880129EE6607AC2ACE8895C8A79090F2A 54SA85E9B5F797EC7D7B02394EE7C5FF5BD3F3A41037C7DA0C89090186F3CF3C1C483FC51943F33C1987C32620E0309FF2FOD5BDEE74681163 9D845D666F35D28A88D6E0BF16A53BBFA6D6657C22ABCB70E15 0A79A0185C4DE62816EBE039B45D35A8D1541FDB6FD8413F91C1EDC01DCCD0BB063CD9935E7AF0678FA622A2B58E756545C38CF59E104E19D6703020111/8D2133E1FA29EFBE94C5CBSA5407219B5DC44448C89 624FDAC385012703C81BDB29DE76B81EC6D6F5BD39422OB88FEA1AE99F9E295631968475670B117C36119EF6AA75AABB1B25E5E7730E60FD65FF32747B06276F2231CAE3AC548121433A6485F6D9E623D73BB2 4D1F7647F9847DB363B0E31553B718FB5156B4C94D0097C3F46B558EB80812C9490BD32362B11D18D1C2218F984D1064F3DC649B909D5BEB4F35624AB2F10676171038AC571F0590FBAFB396B672B7AEB97015A 2BF06EF4A512D7551262496F641C619A324701SB1BSE468BC155BD930E2521FDE0A90EE7ED6490ED2C67877D11CFD62C6D4778FC9642AB93B2BDCC5E650248B846DE1EC82
value of a is1130
(b) Registration Request Communication from ZigBee Device in Blockchain System

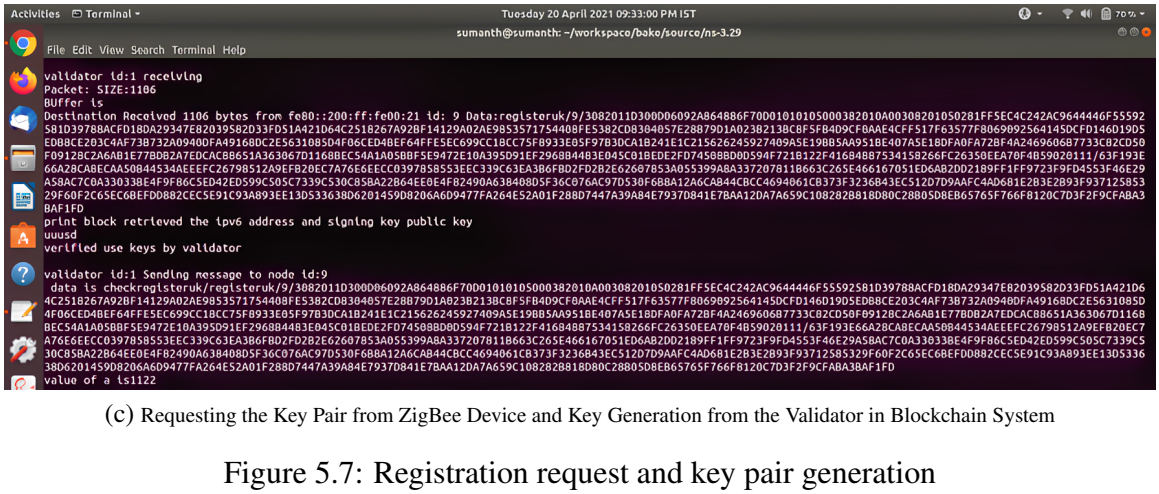
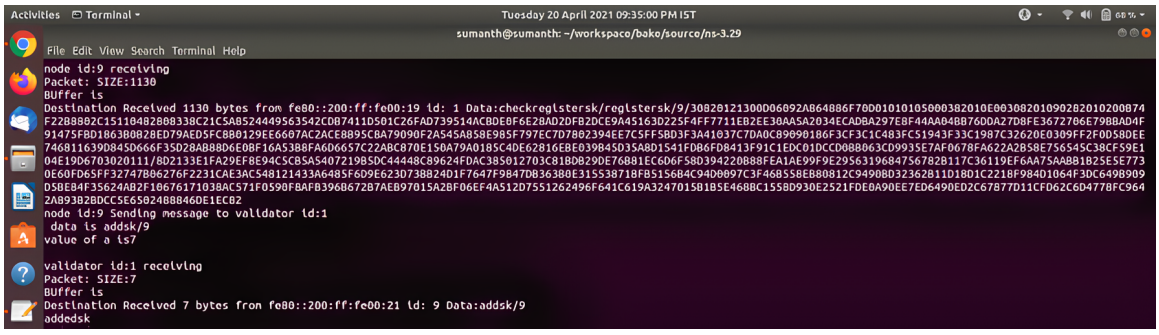

Activities
Terminal
Tuesday 20 April 2021 09:33:00 PM IST
sumanth@sumanth: ~/workspace/bake/source/ns-3.29
File Edit View Search Terminal Help
validator id:1 receiving
Packet: SIZE:1106
BUffer is
Destination Received 1106 bytes from fe80::200:ff:fe00:21 id: 9 Data:registeruk/9/3082011D300D06092A864886F70D0101010500038201 0A00308201050281FF5EC4C242AC9644446F55592 581D39788ACFD18DA29347E82039582D33FD51A421D64C2518267A92BF14129A02AE9853571754408FE538 2CDB304057E28B79D1A023B213BCBF5FB4D9CF0AAE4CFF517F63577FB0690925641 45DCFD146D19D5EDBBCE203C4AF73B732A0940DFA49168DC2E5631085D4F06CED4BEF64FFE5EC699CC1BCC75F8933E05F97B3DCA1B241E1C215626245927409ASE19BB5AA951BE407A5E1BDFA0FA72BF4A2469606B7733CB2CD50 F0912BC2A6AB1E77BDB2A7EDCAC88651A363067D116BBEC54A1A0SBBF5E9472E10A395D91EF2968B44B3E045C01BEDE2FD7450BBD0D594F721B122F41684B875341582 66FC26350EEA70F4B590201 11/63F193E 66A28CABECAA5084453AEEEFC26798512A9EFB20EC7A76E6ECC03978585 3EEC339C63EA3B6FBD2FD2B2E626078S3A055399ABA3372078118663C265E466167051ED6AB2DD2189FF1FF9723F9FD455 3F46E29 A58AC7C0A330338E4F9F86C5ED42ED599C505C7339C530C85BA22B64EE0E4F82490A63B408D5F36C076AC97D530F6B8A12A6CAB44CBCC4694061CB373F3236B43EC512D7D9AAFC4AD681E2B3E2B93F937125853 29F60F2C65EC6BEFDD882CECE91C93A893EE13D53363BD621459D206A6D9477FA264E52A01F288D7447A39A84E7937D841E7BAA12DA7A659C108282B18DB0C2B805D8EB65765F766F8120C7D3F2F9CFABA3 BAF1FD
print block retrieved the ipv6 address and signing key public key
uuusd
verlfled use keys by validator
validator id:1 Sending message to node id:9
data is checkregisteruk/registeruk/9/3082011D300D06092A864886F70D0101010500038201 0A00308201050281FF5EC4C242AC9644446F55592S81D39788ACFD18DA29347E82039582D33FD51A421D6 4C2518267A92BF14129A02AE9853571754408FE538 2CDB304057E28B79D1A023B213BCBF5FB4D9CF0AAE4CFF517F63577FB0690925641 45DCFD146D19D5EDBBCE203C4AF73B732A0940DFA49168DC2E5631085D 4F06CED4BEF64FFE5EC699CC1BCC75F8933E05F97B3DCA1B241E1C215626245927409ASE19BB5AA951BE407A5E1BDFA0FA72BF4A2469606B7733CB2CD50F0912BC2A6AB1E77BDB2A7EDCAC88651A363067D116B BEC54A1A0SBBF5E9472E10A395D91EF2968B44B3E045C01BEDE2FD7450BBD0D594F721B122F41684B875341582 66FC26350EEA70F4B590201 11/63F193E66A28CABECAA5084453AEEEFC26798512A9EFB20EC7 A76E6EECC0397858553EEC339C63EA3B6FBD2FD2B2E626078S3A055399ABA3372078111B663C265E466167051ED6AB2DD2189FF1FF9723F9FD455 3F46E29 30C85BA22B64EE0E4F82490A63B408D5F36C076AC97D530F6BBA12A6CAB44CBCC4694061CB373F3236B43EC512D7D9AAFC4AD681E2B3E2B93F937125853 29F60F2C65EC6BEFDD882CECE91C93A893EE13D53363 8BD620145 9D8206A6D9477FA264E52A01F288D7447A39A84E7937D841E7BAA12DA7A659C108282B818DB0C2B805D8EB65765F766F8120C7D3F2F9CFABA3BAF1FD
value of a is1122
(c) Requesting the Key Pair from ZigBee Device and Key Generation from the Validator in Blockchain System

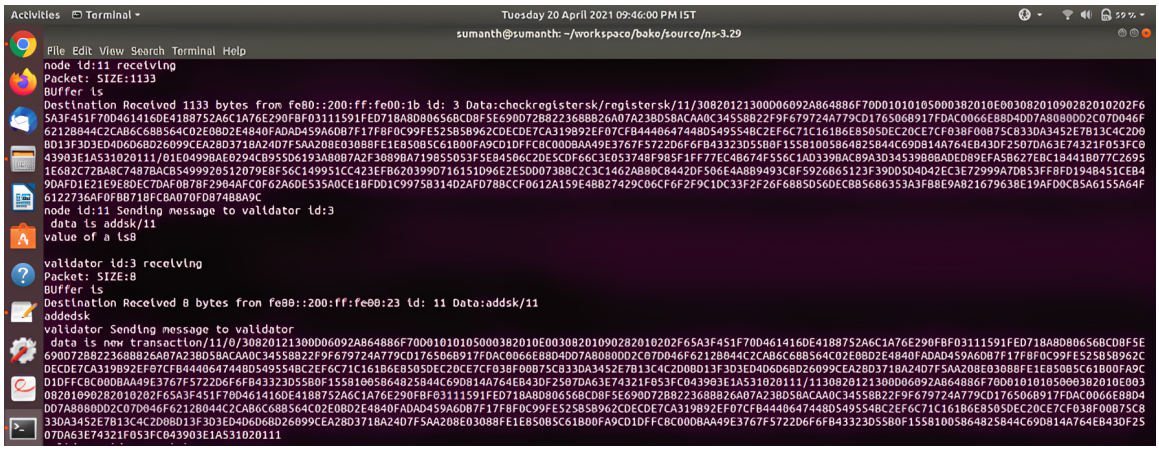
Figure 5.7: Registration request and key pair generation

Parameters	Value
Simulator	NS-3 (Network Simulator-3)
CBR Packet Size	512 bytes
Simulation Area	70M*60M
Simulation Time	60 seconds
Routing Protocols	RPL-AODV, 6LoWPAN Protocol
Number of Nodes	500
Performance Metrics	Routing Overhead, End-to-End Delay, Header Compression, Average Throughput
Packet Rate	1Kbps
Net Buffer Size	1000Bytes
Node Deployment	Uniform

Table 5.1: NS-3 Simulation Parameters



(a) Shows the received confirmation message (Key Pairs) by the ZigBee Node from the validator



(b) shows the registration confirmation message between the validator and ZigBee Node

Figure 5.8: Confirmation messages

pBCS network that creates the signed certificates using the ZigBee Coordinator (Validator) private key commonly used as a root of trust. Only the trusted permissioned Blockchain (Via ZigBee Coordinator) can create authentically signed certificates. Any router or edge device that holds the validator's public key can validate the signed certificate and guarantee the public key's integrity.

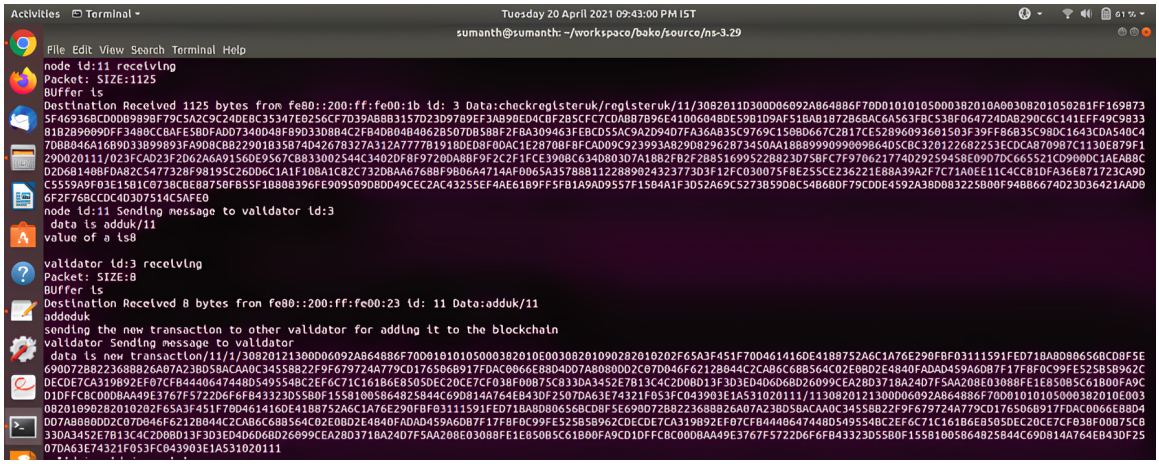
The Figure.5.8(a) The associated validator receives the Registration Request from the ZN and validates the transaction request before sending a confirmation response message to the ZN. The Figure.5.8 (b) Demonstrates that the relevant validator will submit a Link key request to the ZigBee Node, and the validator will then send a Key pair to the ZigBee Node after verifying the transaction request. Figure 5.9(a) shows the confirmation message (Key Pairs) received by the ZigBee Node from the validator.

Figure 5.9(b) shows the registration confirmation message between the validator and ZigBee Node after both sides verify the process. Consider the possibility that the validator chooses against adding the block to the Blockchain. The validator will then forward the registration request to the suitable validator (selected randomly using a round-robin approach) so that they may add the block to the BCS. Figure 5.9(c) shows the communication message between the group of validators for Blockchain creation.

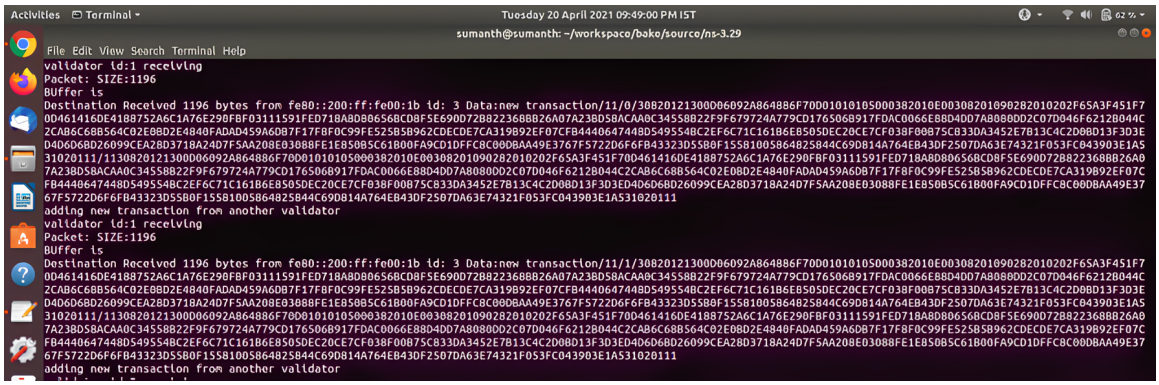
The Figure 5.10(a) & Figure 5.10(b) Show that after validation and verification, the validator (leader) produces the block after receiving requests to register new transactions from other validators. Finally, the newly created block with all new transaction registration requests is

The following Figure 5.10(c) and Figure 5.10(d) Show the secure Communication between ZigBee devices or ZigBee devices to the application profiles Figure 5.10(e). If any ZigBee node wants to communicate with other ZigBee node, their messages are encrypted with a network key and sent to the validator. The Figure 5.10(f)validator will retrieve the information of another node from the BCS Figure 5.10(g). The validator will verify it and send it to the validator of another node if it's not in the same network Figure 5.10(h). After that, the validator of a different node will check it before sending it to the appropriate node.

The implementation outcomes of the pBCS network, which generates the signed certificates using the ZigBee Coordinator (Validator) private key frequently used as a root



(a) Shows the communication message between the group of validators for Blockchain creation



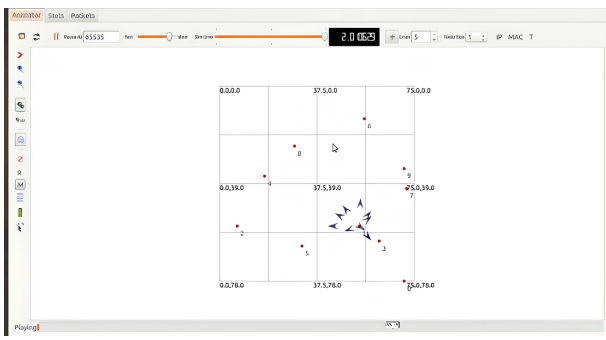
(b) Shows block creation with validation and verification

(c) Shows adding new blocks to the Blockchain system

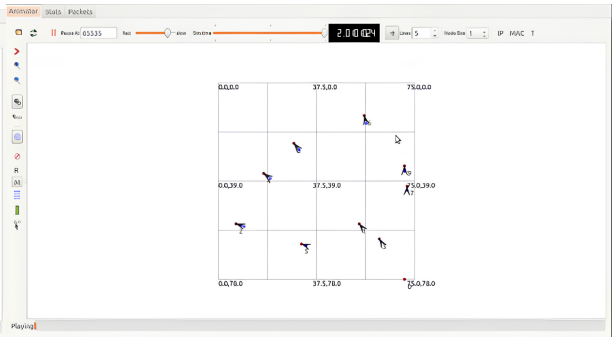
(d) Secure Communication between Node and Validator

(e) Secure communication from one Validator to another Validator

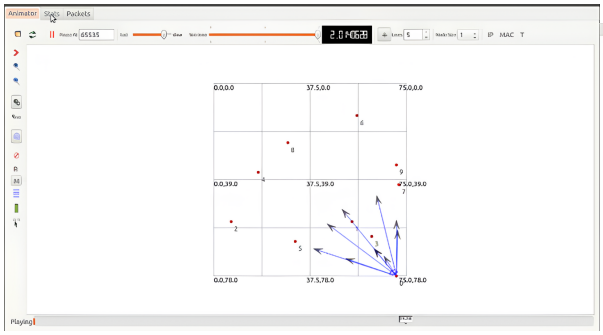
Figure 5.9: Block creation and secure communication



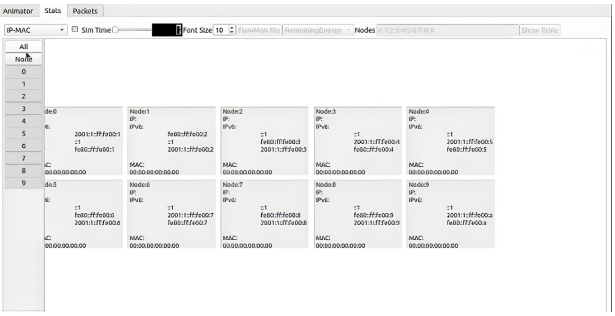
(a) IoT-Enabled ZigBee Network Creation



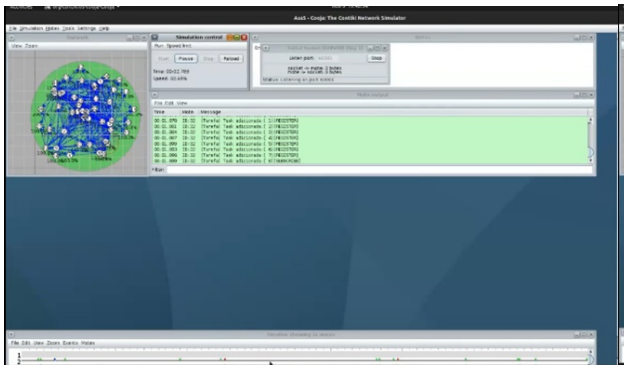
(b) IoT-Enabled ZigBee Setup



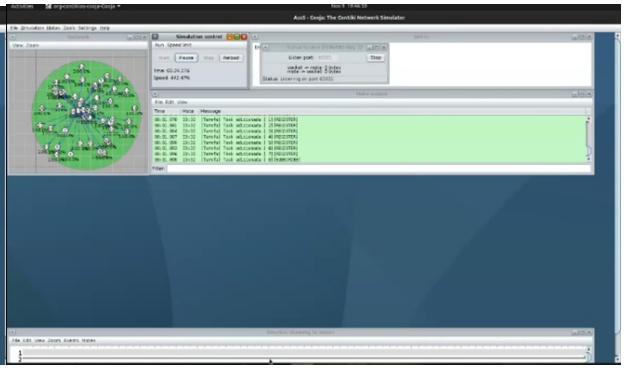
(c) Message Communication from the ZigBee Coordinator to the ZigBee Nodes



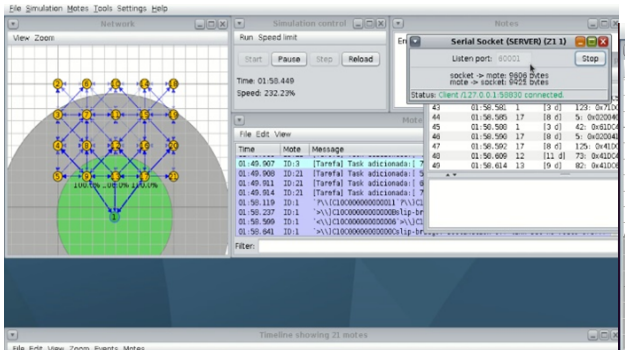
(d) ZED Internal Attributes



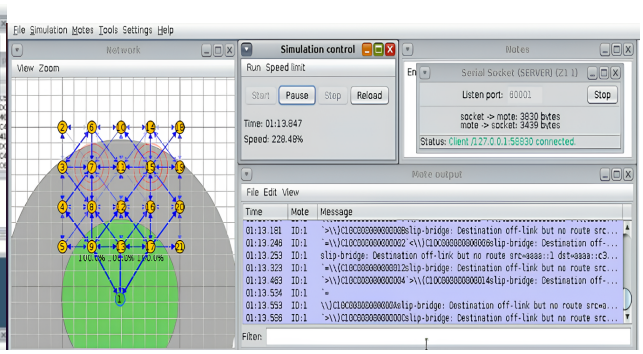
(e) IoT Enabled ZigBee Network Message Communication with 100+ nodes



(f) message from validator to ZigBee Nodes

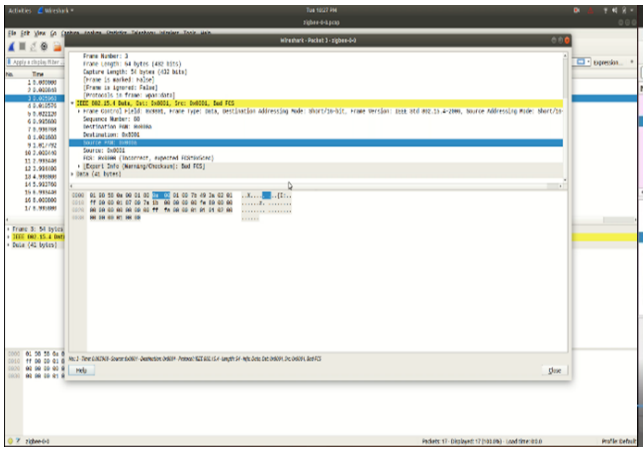


(g) ZigBee Network with IPv6 Enabled

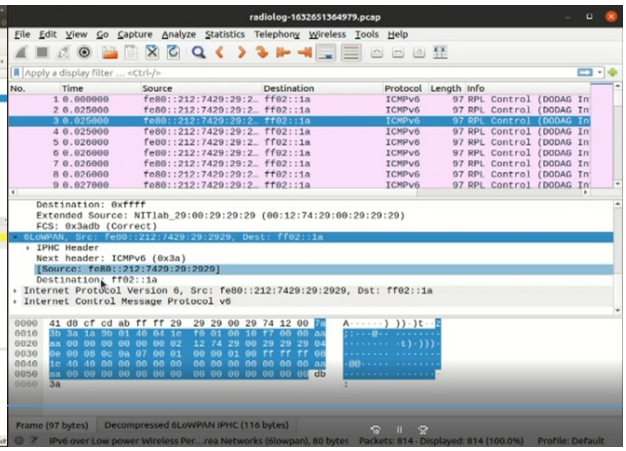


(h) ZigBee Network with IPv6 Enabled

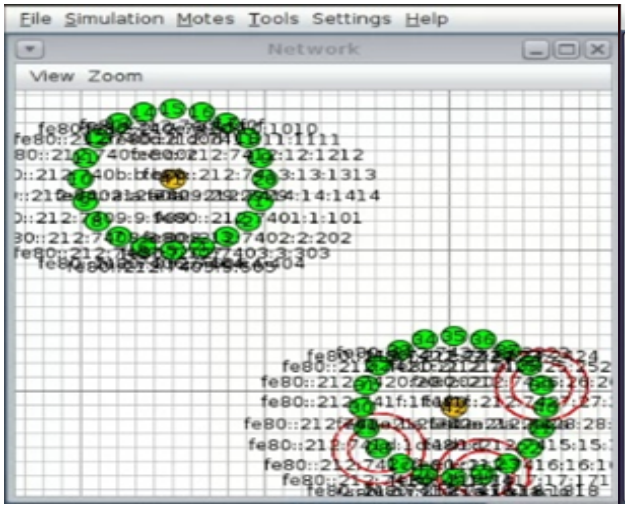
Figure 5.10: Ipv6 enabled ZigBee Network creation



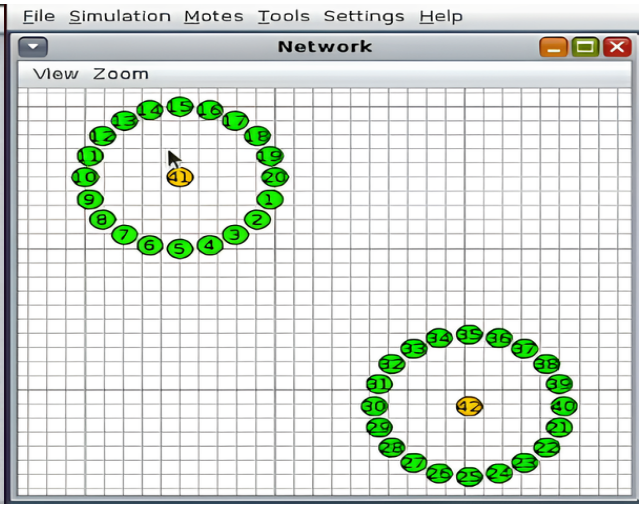
(a) Packet Capture of ZigBee



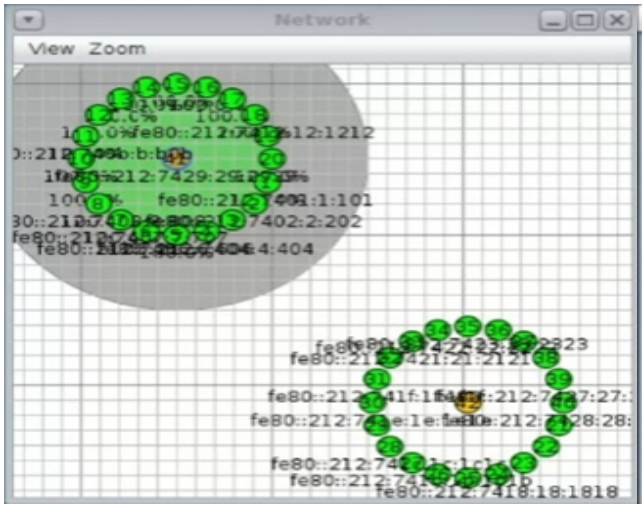
(b) Packet Capture of ZigBee



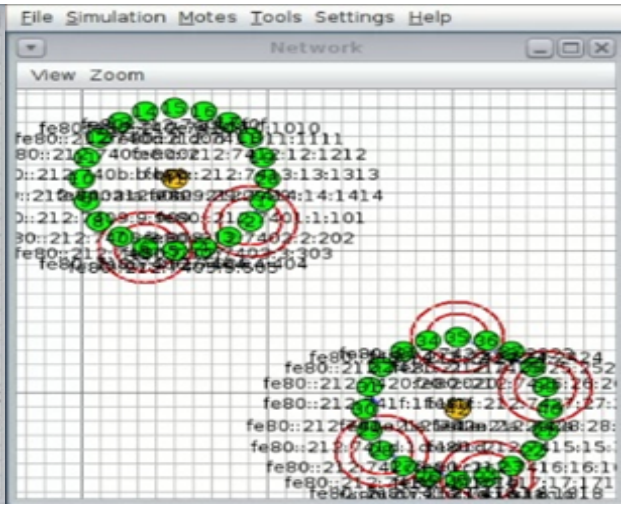
(c) Captures Packet information Stored in Blockchain System



(d) Captures Packet information Stored in Trace Format



(e) Captures Packet information Stored in Blockchain System



(f) Captures Packet information Stored in Trace Format

Figure 5.11: Visualization of Communication among devices ZigBee Network

of trust, are shown in Figure.5.11 below. The only system that can produce authentically signed certificates is the trusted permissioned blockchain (via the ZigBee coordinator). The signed certificate can be verified and the integrity of the public key ensured by any router or edge device that has access to the validator's public key.

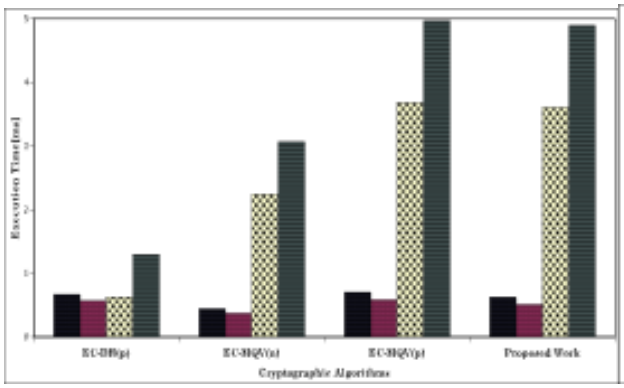
5.3.6 Performance Evaluation

This section provides an evaluation of the proposed framework's performance. It contrasts them with the current mechanisms. Visualization of Device-to-Device Communication The ZigBee Network These network metrics are used to evaluate IEZN networks. Included in the measurements are the number of transactions per second, the average response time of keys, the amount of routing is shown in Figure 5.12 (a) and (b) The creation of a ZigBee Network enabled by IPv6.

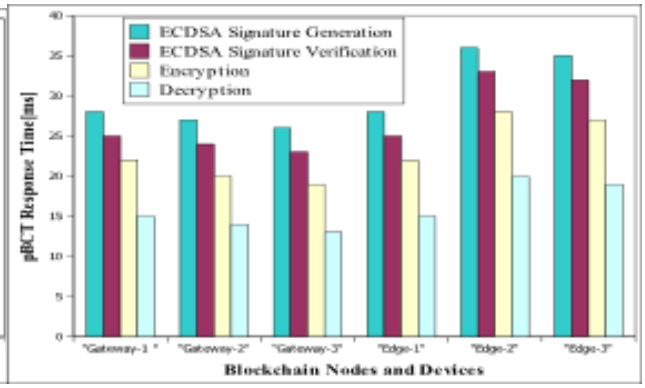
Figure 5.12(c) shows the average time the gateways and edge devices take to write to the pBCT network. It is observed that the gateway handles the minimum 8.67 ms response time to process the request and send the response back to the edge devices. However, the gateways do not store the transaction blocks. The figure also shows the average 57.43 ms response time for registering the edge devices, creating a new block, and adding to the pBCT network.

Figure 5.12 (d) shows the average response while generating the keys from the pBCT network. The maximum response time to develop the key pair for the gateways is 12.45ms, signature creation is 28.17ms, and signature verification is 26.89ms by the gateways. While edge nodes take the maximum response time for signature creation is 32.45ms, and signature verification is 30.29ms. These edge nodes must wait for proper validation for edge devices from other edge devices.

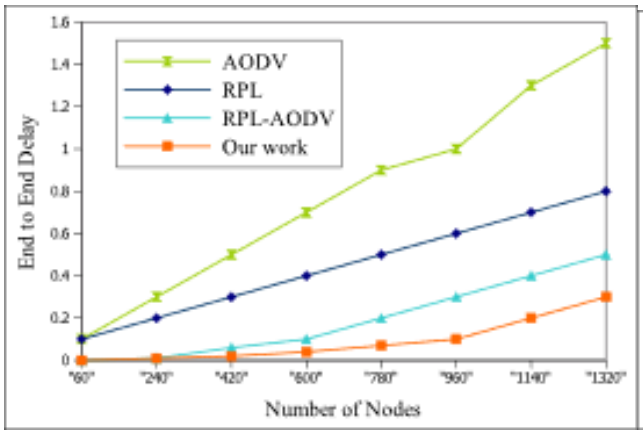
Figure 5.12 (e) shows end-to-end delay with varying times in the presence of DoS attacks over IPsec and Proposed Routing Protocols with and without attacks in the IEZN network. The proposed method has a lower average end-end delay due to the shortest path and achieves high route diversity without DoS Attacks and IPsec. Further, the figure shows that the proposed work incurs more end-to-end delays in the presence of DoS attacks.



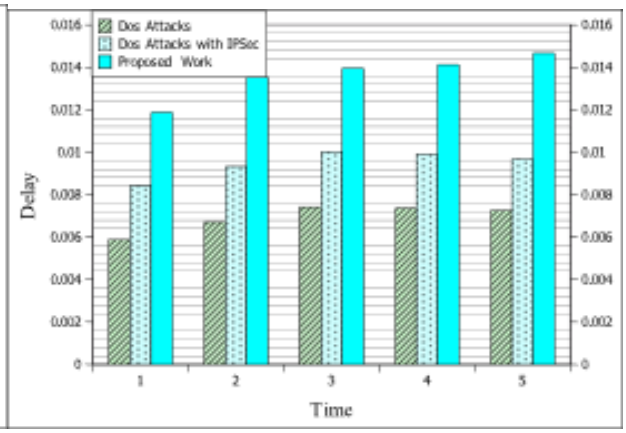
(a) Average Execution time of IoT Devices to register in the pBCT network.



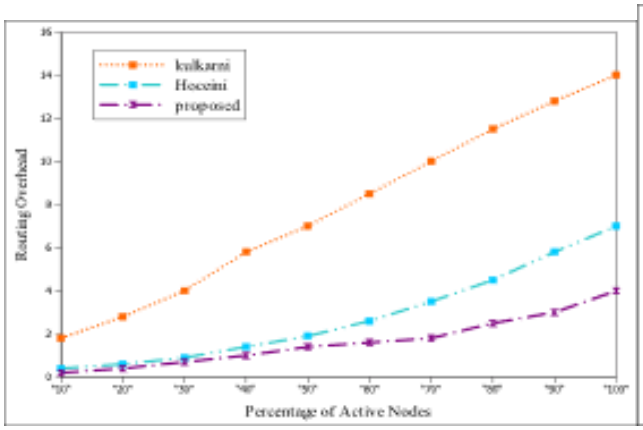
(b) Figure-22 Average Response of Keys Generation in the pBCT network.



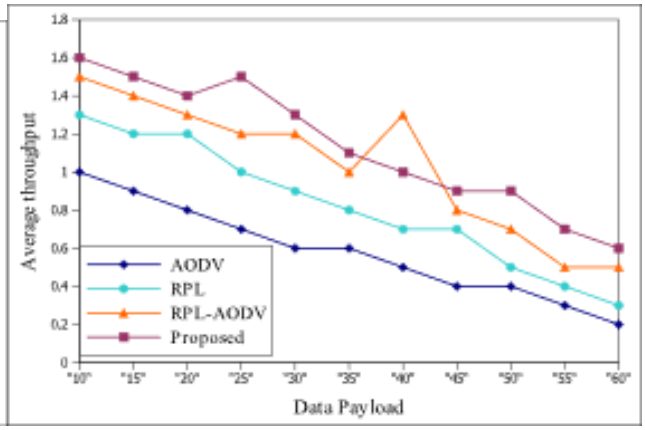
(c) Figure-23 End-to-End Delay Without DoS Attacks



(d) Average End-End Delay With DoS Attacks



(e) Figure-24 Routing Overhead



(f) Average Throughput

Figure 5.12: Performance analysis of Blockchain based Keys Distribution

Figure 5.12 (f) show the End-to-End Delay of RPL, AODV, and RPL-AODV routing protocols with attacks in the IEZN network. The proposed work protocol has a lower average end-end delay due to the shortest path and achieves high route diversity compared to the AODV, RPL, and RPL-AODV protocols.

Figure 5.12 (e) shows routing overhead with varying times; the proposed system has less routing load than the Kulkarni and Hoceini methods. It reduces the size of four DIO requests and DIO replies, RREP, and RREQ control messages to two control DIO-RREQ instances and two DIO-RREP instances. Hence, the proposed routing protocol suits various low-power applications. Figure 5.12 (f) shows the average throughput of AODV, RPL, and presented RPL-AODV routing protocols with varying pause times. The throughput of AODV decreases due to high throughput loss, degrading the IEZN network's performance.

Computational Overhead : Standard cryptographic algorithms like public key systems have a high computational cost and need large memory space. Therefore, these methods are unsuitable for very ZigBee-enabled IoT devices. Our proposal uses a lightweight ECDSA and a hash function. The ZigBee devices and the Blockchain node have enough computational power to handle cryptographic operations based on a symmetric key cryptosystem. However, If the number of devices increases, computation overhead increases for authenticating the ZigBee edge devices and routers. The overall computation cost to complete the authentication transaction in the proposed blockchain network exhibits a bit higher computation overhead in secure communication phases.

5.4 Security Analysis

In this section, we have presented the informal security analysis of the proposed framework. The evaluation is performed in terms of various attacks on IoT enabled ZigBee networks as follows:

1. DOS Attack- This attack may put a victim device on an unending retransmission cycle. The blockchain validators are the distributed coordinator, eliminating the single point of failure, and the proposed scheme can prevent these DoS attacks.

2. ZigBee Network Key Sniffing Attack- Vulnerability in the ZigBee network's key transportation issue while utilizing the minimum-security level. The blockchain prevents the sniffing attack as all the packet data gets encrypted.

3. Network Discovery and Device Identification Attack- ZigBee devices send beacon request frames on a specific channel during the network discovery process. ZigBee Router and coordinators will react by exchanging sensitive information. The anonymity property hides the real identity of Zigbee devices in the blockchain network, so the probability of attacking the device through its unique identity is prevented using the proposed blockchain framework.

4. Worm Attack- The malicious and compromised ZigBee devices spread the worm that causes undesirable activities in the IoT network. The proposed blockchain framework initially registers and authenticates the devices so that worm attacks can be prevented.

5. IoT Worm Hack on Philips Hue Light Bulbs- An assault against Philips Hue Light Bulbs was published in November 2016 to illustrate the attack using Zigbee standards. Attackers utilized a Philips Hue light drone and infected the light bulbs with a worm/virus to turn attackers on and off. The proposed work provides Secure Communication to transfer the data between the End Devices and the coordinator via a registered ZigBee Router. This Secure Communication Protocol derives the shared secret key between the coordinator and edge devices in the untrusted field, authenticated and encrypted communication. This shared secret Key (AES-CCM) will differ for different end devices.

6. Key Search Attack – The attacker uses the user's matched public key to determine the user's Private Key. The coordinator uses a secure channel during the Key-Generation stage, preventing the leakage of the private keys. When an attacker tries to determine the "private keys" from the relevant public key, they face the challenge of solving "the Elliptic Curve Discrete Logarithm Problem." According to "ECDLP," it is impossible to calculate the discrete logarithm of a random number concerning a previously

known base point. The difficulty of computing a point multiplication determines the security of ECC, considering the original and product issues and the impossibility of calculating the multiplicand. The number of discrete integer pairs that meet the curve equation entirely is known as the EC size, which influences how complex the assignment is.

7. Man in the Middle Attack - In this type of assault, a person tries to listen in on a conversation between two people while stealing or altering the information being exchanged. The communication between the two parties creates a separate link between them. Since every letter sent between two parties in our suggested model is signed using ECDSA, the attacker must access one of the parties' private keys to steal or alter the messages. Creating a fake private key is computationally impossible and as complex as solving the ECDLP. Because of this, our suggested model is resistant to Man in "the Middle Attacks."

5.5 Summary of the Chapter

In this chapter In this paper, we proposed the key management mechanism for the distribution of keys among IoT-Enabled ZigBee Networks utilizing a trust-based Blockchain system, which enables end-to-end application key establishment, Securing joining the network, network-wide key Distribution, Network Key Update, network access control and authentication of routers and IoT devices that have different radios, and Storage of key credentials using the trust security service provider. This proposed Blockchain system solves the problem of less non-volatile memory usage and improves key management. The Blockchain validator will access the shared ledger that stores the digital key credentials of all the enrolled routers, devices, and gateways, including the ZigBee coordinators. We implemented and validated the proposed work and showed its performance for securing the network; network-wide key distribution is more effective and efficient than the current state of the art.

Chapter 6

Conclusion and Future Scope

In this thesis, we proposed a framework to interact with an adaptive 6LoWPAN communication protocol in an IoT-enabled ZigBee network to offer an efficient end-to-end communication protocol. This adaptation protocol provides services to the IoT-enabled ZigBee network or internet layer using data from the end devices. When the internet host or end user submits their query, the order to route IPv6 packets into ZigBee networks that support the Internet of Things, the 6LoWPAN links ZigBee devices with IP-based infrastructures, enabling end-to-end communication. The capacity to forward or route data packets from a ZigBee device to a 6LoWPAN Boarder Router (6BR) over several hops is what the RPL-AODV routing protocol, which we designed, is all about. This proposed routing protocol incorporates the benefits of RPL and AODV routing protocols in ZigBee devices of IoT networks to establish the path from the source node to the destination node on demand. Furthermore, we evaluated this protocol's efficacy using various metrics and found that its results were superior to those of existing protocols.

Next, we proposed a cooperative IDS mechanism to detect coordinated attacks against the RPL-AODV routing protocol in the IoT-enabled ZigBee network. First, we modeled coordinated attacks, which significantly impact IoT networks more than uncoordinated attacks. The proposed cooperative IDS combines specification-based and signature-based IDS to detect collaborative attacks against the RPL-AODV routing protocol, effectively monitoring and securing IoT-enabled ZigBee networks.

Finally, we enhanced the security of an IoT-enabled ZigBee network using a Blockchain

system. We investigated the key distribution and secure communication among nodes using RPL-AODV protocols in this method. This proposed Blockchain solution addresses the issues of decreased non-volatile memory utilization and enhanced key management. The Blockchain validator will access the shared ledger that maintains the digital key credentials of all enrolled ZED and ZR devices, including ZigBee coordinators. Finally, we implemented and validated the all-proposed work using state-of-the-art techniques and demonstrated the performance of these works for IoT-enabled ZigBee security; network-wide key distribution is more effective and efficient.

In future work, we can extend a Blockchain-based framework for the secure allocation of IPv6 addresses in IoT-enabled ZigBee networks while interfacing ZigBee devices with IPv6 using the 6LoWPAN protocol. We can also extend the certificate Aggregate signature scheme to enhance the security of the AODV-RPL protocol. This aggregate signature scheme helps highly resource constraint IoT-enabled ZigBee networks. In future work, secure routing paths can be provided by detecting malicious adversaries using Blockchain systems.

Bibliography

[1] A. Haka, V. Aleksieva, H. Valchanov, Enhanced simulation framework for visualisation of IEEE 802.15. 4 frame structure on beacon enabled mode of ZigBee sensor network, in: 2020 International Conference on Biomedical Innovations and Applications, BIA, IEEE, 2020, pp. 109–112.

[2] A. Senthil Kumar, G. Suresh, S. Lekashri, G. Babu Loganathan, R. Manikandan, Smart agriculture system with E–carbage using IoT, Int. J. Mod. Agric. 10 (1) (2021) 928–931.

[3] A. Verma, V. Ranga, Security of RPL based 6LoWPAN networks in the Internet of Things: A review, IEEE Sens. J. 20 (11) (2020) 5666–5690.

[4] A.D. Aguru, E.S. Babu, S.R. Nayak, A. Sethy, A. Verma, Integrated industrial reference architecture for smart healthcare in Internet of Things: A systematic investigation, Algorithms 15 (9) (2022) 309.

[5] A.K. Sangaiah, A.S. Rostami, A.A.R. Hosseinabadi, M.B. Shareh, A. Javadpour, S.H. Bargh, M.M. Hassan, Energy-aware geographic routing for real-time workforce monitoring in industrial informatics, IEEE Internet Things J. 8 (12) (2021) 9753–9762.

[6] A.K. Sultania, F. Mahfoudhi, J. Famaey, Real-time demand response using NB-IoT, IEEE Internet Things J. 7 (12) (2020) 11863–11872.

[7] A.K.M. Al-Qurabat, H.M. Salman, A.A.R. Finjan, Important extrema points extraction-based data aggregation approach for elongating the WSN lifetime, Int. J. Comput. Appl. Technol. 68 (4) (2022) 357–368.

[8] A.K.M. Al-Qurabat, S.A. Abdulzahra, An overview of periodic wireless sensor networks to the Internet of Things, IOP Conf. Ser.: Mater. Sci. Eng. 928 (3) (2020) 032055.

[9] A.K.M. Al-Qurabat, Z.A. Mohammed, Z.J. Hussein, Data traffic management based on compression and MDL techniques for smart agriculture in IoT, Wirel. Pers. Commun. 120 (3) (2021) 2227–2258.

[10] A.M.K. Abdulzahra, A.K.M. Al-Qurabat, A clustering approach based on fuzzy C-means in wireless sensor networks for IoT applications, Karbala Int. J. Modern Sci. 8 (4) (2022) 579–595.

[11] Abdel Hakeem, S. A., Hady, A. A., & Kim, H. (2019). RPL routing protocol performance in smart grid applications based wireless sensors: Experimental and simulated analysis. Electronics (Basel), 8(2), 186. doi:10.3390/electronics8020186

[12] Al-Hadhrami, Y., & Hussain, F. K. (2021). DDoS attacks in IoT networks: A comprehensive systematic literature review. World Wide Web (Bussum), 24(3), 971–1001. doi:10.1007/s11280-020-00855-2

[13] Almusaylim, Z. A., Alhumam, A., Mansoor, W., Chatterjee, P., & Jhanjhi, N. Z. (2020). Detection and mitigation of RPL rank and version number attacks in smart Internet of things. Academic Press.

[14] Al-Shargabi, B., & Aleswid, M. (2020). Performance of RPL in healthcare wireless sensor network. arXiv preprint arXiv:2005.02454.

[15] Ambili, K. N., & Jose, J. (2020). TN-IDS for network layer attacks in RPL-based IoT systems. Cryptology ePrint Archive.

[16] Anamalamudi, M. Zhang, C. Perkins, S.V.R.Anand " Supporting Asymmetric Links in Low Power Networks ", draft-ietf-roll-aodvrpl- 13, pp.1-2, 7 March 2022.

[17] Anamalamudi, S., Zhang, M., Sangi, A. R., Perkins, C. E., & Anand, S. (Manuscript submitted for publication). BL Asymmetric AODV-P2P-RPL in Low-Power and Lossy Networks (LLNs). Internet-Draft draft-ietf-roll-aodvrpl- 03. Work (Reading, Mass.).

[18] B. Djamaa, M.R. Senouci, H. Bessas, B. Dahmane, A. Mellouk, Efficient and stateless P2P routing mechanisms for the Internet of Things, IEEE Internet Things J. 8 (14) (2021) 11400–11414.

[19] B. Priyeash, J. Thyagarajan, "Performance Evaluation and Comparison Analysis of AODV and RPL Using NetSim in Low Power, Lossy Networks," Futuristic Communication and Network Technologies, pp.6, 12 October 2021.

[20] B. Priyeash, J. Thyagarajan, Performance evaluation and comparison analysis of AODV and RPL using NetSim in low power, lossy networks, in: Futuristic Communication and Network Technologies: Select Proceedings of VICFCNT 2020, Springer, 2022, pp. 11–22.

[21] B.P. Santos, O. Goussevskaia, L.F. Vieira, M.A. Vieira, A.A. Loureiro, Mobile matrix: Routing under mobility in IoT, IoMT, and social IoT, Ad Hoc Netw. 78 (2018) 84–98.

[22] B.S. Babu, TLBO based power system optimization for AC/DC hybrid systems, J. Phys.: Conf. Ser. 1916 (1) (2021) 012023.

[23] Babu, E. S., Dadi, A. K., Singh, K. K., Nayak, S. R., Bhoi, A. K., & Singh, A. (2022). A distributed identity-based authentication scheme for Internet of Things devices using a permissioned blockchain system. Expert Systems: International Journal of Knowledge Engineering and Neural Networks, 39(10), e12941. doi:10.1111/exsy.12941

[24] Babu, E. S., Kavati, I., Nayak, S. R., Ghosh, U., & Al Numay, W. (2022). Secure and transparent pharmaceutical supply chain using a permissioned blockchain network. International Journal of Logistics Research and Applications, 1-28.

[25] Babu, E. S., Nagaraju, C., & Prasad, M. K. (2015, September). A secure routing protocol against heterogeneous attacks in wireless ad-hoc networks. In Proceedings of the Sixth International Conference on Computer and Communication Technology 2015 (pp. 339-344). doi:10.1145/2818567.2818670

[26] Babu, E. S., Nagaraju, C., & Prasad, M. K. (2016). IPHDBCM: Inspired Pseudo Hybrid DNA Based Cryptographic Mechanism to Prevent Against Collaborative Black Hole Attack in Wireless Ad hoc Networks. International Journal of Information Security and Privacy, 10(3), 42–66. doi:10.4018/IJISP.2016070104

[27] Babu, Erukala Suresh "Trust-Based Permissioned Blockchain Network for Identification and Authentication of Internet of Smart Devices: An E-Commerce Prospective," J=Journal of Interconnection Networks, P =2243001, Y=2022, P=World Scientific

[28] C. Samuel, B.M. Alvarez, E.G. Ribera, P.P. Ioulianou, V.G. Vassilakis, Performance evaluation of a wormhole detection method using round-trip times and hop counts in RPL-based 6LoWPAN networks, in: 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP, IEEE, 2020, pp. 1–6.

[29] C.M. Dasari, R. Bhukya, Explainable deep neural networks for novel viral genome prediction, Appl. Intell. 52 (3) (2022) 3002–3017.

[30] Cakir, S., Toklu, S., & Yalcin, N. (2020). RPL attack detection and prevention in the Internet of Things networks using GRU-based deep learning. IEEE Access: Practical Innovations, Open Solutions, 8, 183678–183689. doi:10.1109/ACCESS.2020.3029191

[31] Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2014). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Systems Journal, 9(1), 65–75. doi:10.1109/JSYST.2013.2296197

[32] Chen, D., Brown, J., & Khan, J. Y. (2013, July). 6LoWPAN-based neighborhood area network for a smart grid communication infrastructure. In 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 576-581). IEEE. doi:10.1109/ICUFN.2013.6614885

[33] Dall'Ora, R., Raza, U., Brunelli, D., & Picco, G. P. (2014, September). SensEH: From simulation to deployment of energy harvesting wireless sensor networks. In 39th Annual IEEE Conference on Local Computer Networks Workshops (pp. 566-573). IEEE. doi:10.1109/LCNW.2014.6927704

[34] Dharmini Shreenivas, Shahid Raza, Thiemo Voigt, "Intrusion Detection in the RPL-connected 6LoWPAN Networks", IoTPTS '17: Proceedings of the 3rd ACMInternationalWorkshop on IoT Privacy, Trust, and Security, pp. 6,2 April 2017.

[35] Djamaa, Badis and Senouci, Mustapha Reda and Bessas, Hichem and Dahmane, Boutheina and Mellouk, Abdelhamid “Efficient and stateless P2P routing mechanisms for the Internet of Things”, IEEE Internet of Things Journal, volume=8, number=14, pp. 11400—11414, year=2021.

[36] Don Sturek, Joseph Reddy “ZigBee IP Specification” ZigBee IP Specification 12-0572-10, pp.5-156, February 2013.

[37] Duan, J., Yang, D., Zhu, H., Zhang, S., & Zhao, J. (2014). TSRF: A trust-aware secure routing framework in wireless sensor networks. International Journal of Distributed Sensor Networks, 10(1), 209436. doi:10.1155/2014/209436

[38] E.S. Babu, A.K. Dadi, K.K. Singh, S.R. Nayak, A.K. Bhoi, A. Singh, A distributed identity-based authentication scheme for Internet of Things devices using permissioned blockchain system, Expert Syst. 39 (10) (2022) e12941.

[39] E.S. Babu, A.K. Dadi, K.K. Singh, S.R. Nayak, A.K. Bhoi, A. Singh, A distributed identity-based authentication scheme for Internet of Things devices using permissioned blockchain system, Expert Syst. 39 (10) (2022) e12941.

[40] Emanuele Toscano, Lucia Lo Bello, "Comparative assessments of IEEE 802.15.4/ZigBee and 6LoWPAN for low-power industrial WSNs in realistic scenarios",2012 9th IEEE InternationalWorkshop on Factory Communication Systems, pp. 5-6,19 July 2012.

[41] Ender Yuksel, Nielson “Zigbee-2007 security essentials”, B=Proc. 13th Nordic Workshop on Secure IT-systems, pages=65–82, year=2008.

[42] Erukala Suresh Babu, “Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks,” J=Computers and Electrical Engineering, V=103, P=108287, Y= 2022,= Elsevier

[43] Foley, J., Moradpoor, N., & Ochen, H. (2020). Employing a machine learning approach to detect combined Internet of Things attacks against two objective functions using a novel dataset. Security and Communication Networks, 2020, 1–17. doi:10.1155/2020/2804291

[44] Ghada Glissa “6LowPSec: An end-to-end security protocol for 6LoWPAN” J=Ad Hoc Networks, V=82, P=100–112, Y=2019, P=Elsevier.

[45] Ghaleb, B., Al-Dubai, A. Y., Ekonomou, E., Alsarhan, A., Nasser, Y., Mackenzie, L. M., & Boukerche, A. (2018). A survey of limitations and enhancements of the ipv6 routing protocol for low-power and lossy networks: A focus on core operations. IEEE Communications Surveys and Tutorials, 21(2), 1607–1635. doi:10.1109/COMST.2018.2874356

[46] Glissa, Ghada and Rachedi “A secure routing protocol based on RPL for Internet of Things,” B=2016 IEEE Global Communications Conference (GLOBECOM) P=1–7, Y=2016, organization=IEEE

[47] Gupta, Malvika and Singh, Shweta "Asurvey on the Zigbee protocol, its security in the internet of things (IoT) and comparison of Zigbee with Bluetooth and wi-fi," pages= 473–482, Y=2021.

[48] Gupta, Tania, and Bhatia, Richa "Communication technologies in the smart grid at different network layers: an overview," 2020 International Conference on Intelligent Engineering and Management (ICIEM), pp. 177-182, year-2020.

[49] H.B. Mahajan, A. Badarla, A.A. Junnarkar, CL-IoT: Cross-layer Internet of Things protocol for intelligent manufacturing of smart farming, J. Ambient Intell. Humaniz. Comput. 12 (7) (2021) 7777–7791.

[50] Halder, M., Sheikh, M., Rahman, M., & Rahman, M. (2018). Performance analysis of CoAP, 6LoWPAN, and RPL routing protocols of IoT using COOJA simulator. International Journal of Scientific and Engineering Research, 9(6), 1670–1677.

[51] Haque, Halima, and Labeeb, Kashshaf and Riha, Rabea Basri and Khan, Md Nasfikur R "IoT based water quality monitoring system by using Zigbee protocol," pages=619–622, year=2021.

[52] Hasan, Shah Muhammad Jannatul and Ali, Mohammad and Khan, Taufiqul Islam and Afrin, Farzana and Islam, Md Motaharul "6LoWPAN Based Futuristic Smart Architecture for Home Automation", 2nd International Conference on Advanced Information and Communication Technology (ICAICT), pp. 449—454, year-2020.

[53] Hidayat, Taufik, Mahardiko, Rahutomo and Tigor, FrankyDSianturi "Method of systematic literature review for the internet of things in ZigBee smart agriculture" 2020 8th International Conference on Information and Communication Technology (ICoICT), P=1–4, Y=2020.

[54] Hidayat, Taufik, Mahardiko, Rahutomo and Tigor, FrankyDSianturi "Method of systematic literature review for the internet of things in ZigBee smart agriculture," 2020 8th International Conference on Information and Communication Technology (ICoICT), P=1–4, Y=2020.

[55] Hosen, A. S., Singh, S., Sharma, P. K., Ghosh, U., Wang, J., Ra, I. H., & Cho, G. H. (2020). Blockchain-based transaction validation protocol for a secure distributed IoT network. IEEE Access: Practical Innovations, Open Solutions, 8, 117266–117277. doi:10.1109/ACCESS.2020.3004486

[56] I. Alaoui Ismaili1, A. Azyat2, N.Raissouni3, N. Ben Achhab4, A. Chahboun5, M.Lahraoua "Comparative Study of ZigBee and 6LoWPAN Protocols: Review", Proceedings of the Third International Conference on Computing and Wireless Communication Systems, ICCWCS 2019, pp.5-6, 23 May 2019

[57] I. Rabet, S.P. Selvaraju, M.H. Adeli, H. Fotouhi, A. Balador, M. Vahabi, M. Alves, M. Björkman, Pushing IoT mobility management to the edge: Granting RPL accurate localization and routing, in: 2021 IEEE 7th World Forum on Internet of Things, WF-IoT, IEEE, 2021, pp. 338–343.

[58] I.D.I. Saeedi, A.K.M. Al-Qurabat, An energy-saving data aggregation method for wireless sensor networks based on the extraction of extrema points, in: AIP Conference Proceedings, Vol. 2398, no. 1, AIP Publishing LLC, 2022, 050004.

[59] I.D.I. Saeedi, A.K.M. Al-Qurabat, Perceptually important points-based data aggregation method for wireless sensor networks, Baghdad Sci. J. 35 (2022) 0875.

[60] Idris Khan, F., Shon, T., Lee, T., & Kim, K. H. (2014). Merkle tree-based wormhole attack avoidance mechanism in low power and lossy network-based networks. Security and Communication Networks, 7(8), 1292–1309. doi:10.1002/sec.1023

[61] Ioulianou, P. P., & Vassilakis, V. G. (2020). Denial-of-service attacks and countermeasures in the RPL-based Internet of Things. In Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers 5 (pp. 374-390). Springer International Publishing. doi:10.1007/978-3-030-42048-2_24

[62] Ioulianou, P. P., Vassilakis, V. G., & Shahandashti, S. F. (2022). A trust-based intrusion detection system for RPL networks: Detecting a combination of rank and blackhole attacks. Journal of Cybersecurity and Privacy, 2(1), 124–153. doi:10.3390/jcp2010009

[63] J. Van Kerkhoven, N. Charlebois, A. Robertson, B. Gibson, A. Ahmed, Z. Bouida, M. Ibnkahla, IPv6-based smart grid communication over 6LoWPAN, in: 2019 IEEE Wireless Communications and Networking Conference, WCNC, IEEE, 2019, pp. 1–6.

[64] J.V. Sobral, J.J. Rodrigues, R.A. Rabêlo, J. Al-Muhtadi, V. Korotaev, Routing protocols for low power and lossy networks in Internet of Things applications, Sensors 19 (9) (2019) 2144.

[65] Jamal Zbitou, Adil Echchelh, Mostafa Hefnawi, Ahmed Errkik, "Third International Conference on Computing and Wireless Communication Systems," ICCWCS 2019, pp.,23 May 2019.

[66] Khader, R., & Eleyan, D. (2021). Survey of dos/ddos attacks in IoT. Sustainable Engineering and Innovation, 3(1), 23–28. doi:10.37868/sei.v3i1.124

[67] Khanuja, H. K., & Adane, D. (2020). Monitor and detect suspicious transactions with database forensic analysis. In Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice (pp. 402-426). IGI Global.

[68] Kiayias, Aggelos "Ouroboros: A provably secure proof-of-stake blockchain protocol," B=Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part I, P=357–388, Y=2017, organization=Springer.

[69] Kumar, S. A., Babu, E. S., Nagaraju, C., & Gopi, A. P. (2015). An empirical critique of on-demand routing protocols against rushing attack in MANET. Iranian Journal

of Electrical and Computer Engineering, 5(5), 1102. doi:10.11591/ijece.v5i5.pp1102-1110

[70] Lau, Chi Ho and Alan "Blockchain-based authentication in IoT networks" B=2018 IEEE conference on dependable and secure computing (DSC), P=1–8, Y=2018, organization=IEEE

[71] Le, A., Loo, J., Luo, Y., & Lasebae, A. (2011, October). Specification-based IDS for securing RPL from topology attacks. In 2011 IFIP Wireless Days (WD). IEEE.

[72] Lu, C. W., Li, S. C., & Wu, Q. (2011, November). Interconnecting ZigBee and 6LoWPAN wireless sensor networks for smart grid applications. In 2011 Fifth International Conference on Sensing Technology (pp. 267-272). IEEE.

[73] M. Al-Qurabat, A. Kadhum, A lightweight Huffman-based differential encoding lossless compression technique in IoT for smart agriculture, Int. J. Comput. Digit. Syst. (2021).

[74] M.A. Rahman, A.T. Asyhari, I.F. Kurniawan, M.J. Ali, M. Rahman, M. Karim, A scalable hybrid MAC strategy for traffic-differentiated IoT-enabled intra-vehicular networks, Comput. Commun. 157 (2020) 320–328, http://dx.doi.org/10.1016/j.comcom.2020.04.035, URL: https://www.sciencedirect.com/ science/article/pii/S014036642030164X.

[75] Marcano, Néstor J HetnM´ endez and N, Jonas Gabs Fugl, and Jacobsen, Rune Hylsberg, "On ad hoc on-demand distance vector routing in low earth orbit nanosatellite constellations" 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring, pages=1–6, year=2020.

[76] McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018, July). Botnet detection in the Internet of Things using deep learning approaches. In 2018 international joint conference on neural networks (IJCNN) (pp. 1-8). IEEE. doi:10.1109/IJCNN.2018.8489489

[77] Mutchler, L. A., & Warkentin, M. (2020). Experience matters: The role of vicarious experience in secure actions. Journal of Database Management, 31(2), 1–20. doi:10.4018/JDM.2020040101

[78] N.J.H. Marcano, J.G.F. Nø rby, R.H. Jacobsen, On ad hoc on-demand distance vector routing in low earth orbit nanosatellite constellations, in: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, 2020, pp. 1–6.

[79] Nagarajan, S. M., Deverajan, G. G., Chatterjee, P., Alnumay, W., & Ghosh, U. (2021). Effective task scheduling algorithm with deep learning for Internet of Health Things (IoHT) in sustainable smart cities. Sustainable Cities and Society, 71, 102945. doi:10.1016/j.scs.2021.102945

[80] Napiah, M. N., Idris, M. Y. I. B., Ramli, R., & Ahmedy, I. (2018). Compression header analyzer intrusion detection system (CHA-IDS) for 6LoWPAN communication protocol. IEEE Access: Practical Innovations Open Solutions, 6, 16623–16638. doi:10.1109/ACCESS.2018.2798626

[81] P. Aithal, et al., Smart city waste management through ICT and IoT driven solution, Int. J. Appl. Eng. Manag. Lett. (IJAEML) 5 (1) (2021) 51–65.

[82] Patel, D. N., Patel, S. B., Kothadiya, H. R., Jethwa, P. D., & Jhaveri, R. H. (2014, February). A survey of reactive routing protocols in MANET. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-6). IEEE. doi:10.1109/ICICES.2014.7033833

[83] Perrey, H., Landsmann, M., Ugus, O., Schmidt, T. C., & Wahlisch, M. (2013). TRAIL: Topology Authentication in RPL. arXiv preprint arXiv:1312.0984.

[84] Pongle, P., & Chavan, G. (2015, January). A survey: Attacks on RPL and 6LoWPAN in IoT. In 2015 International Conference on pervasive computing (ICPC) (pp. 1-6). IEEE. doi:10.1109/PERVASIVE.2015.7087034

[85] R.J. Tom, S. Sankaranarayanan, V.H.C. de Albuquerque, J.J. Rodrigues, Aggregator based RPL for an IoT-fog based power distribution system with 6LoWPAN, China Commun. 17 (1) (2020) 104–117.

[86] Rabet, Iliar and Selvaraju, Shunmuga Priyan and Adeli, Mohammad Hassan and Fotouhi, Hossein and Balador, Ali and Vahabi, Maryam and Alves "Pushing IoT mobility management to the edge: Granting RPL accurate localization and routing," 2021 IEEE 7thWorld Forum on Internet of Things (WF-IoT), pages=338–343, year=2021.

[87] Rajesh K "An introduction to Zigbee / IEEE 802.15.4 Wireless Network." 27 September 2011.

[88] Reen-Cheng Wang, Ruay-Shiung Chang, Han-Chieh Chao, "Internetworking Between ZigBee/802.15.4 and IPv6/802.3 Network", pp.4-6.

[89] Rghioui, A., Khannous, A., & Bouhorma, M. (2014). Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition. Journal of Advanced Computer Science & Technology, 3(2), 143. doi:10.14419/jacst.v3i2.3321

[90] S.A. Abdulzahra, A.K.M. Al-Qurabat, A.K. Idrees, Compression-based data reduction technique for IoT sensor networks, Baghdad Sci. J 18 (1) (2021)184–198.

[91] S.M.J. Hasan, M. Ali, T.I. Khan, F. Afrin, M.M. Islam, 6LoWPAN based futuristic smart architecture for home automation, in: 2020 2nd International Conference on Advanced Information and Communication Technology, ICAICT, IEEE, 2020, pp. 449–454.

[92] Sadikin, Fal and Van Deursen, Ton and Kumar, Sandeep "A ZigBee intrusion detection system for IoT using secure and efficient data collection," journal=Internet of Things, V=12, P=100306

[93] Seyfollahi, A., & Ghaffari, A. (2021). A review of intrusion detection systems in RPL routing protocol based on Machine learning for Internet of Things applications. Wireless Communications and Mobile Computing, 2021, 1–32. doi:10.1155/2021/8414503

[94] Shen, M., Wang, J., Liu, O., & Wang, H. (2020). Expert detection and recommendation model with user-generated tags in collaborative tagging systems. Journal of Database Management, 31(4), 24–45. doi:10.4018/JDM.2020100102

[95] Sikder, A. K., Acar, A., Aksu, H., Uluagac, A. S., Akkaya, K., & Conti, M. (2018, January). IoT-enabled smart lighting systems for smart cities. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 639-645). IEEE. doi:10.1109/CCWC.2018.8301744

[96] Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2020). Machine learning-based IoT-botnet attack detection with sequential architecture. Sensors (Basel), 20(16), 4372. doi:10.3390/s20164372 PMID:32764394

[97] Sturek, Don "Zigbee ip stack overview," J= ZigBee Alliance, V= 2009, Y= 2009.Sturek, Don "Zigbee ip stack overview," J= ZigBee Alliance, V= 2009, Y= 2009.

[98] Suresh Babu, E., Naganjaneyulu, S., Srivasa Rao, P. V., & Narasimha Reddy, G. K. V. (2019). An Efficient Cryptographic Mechanism to Defend Collaborative Attack Against DSR Protocol in Mobile Ad hoc Networks. In Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2018, Volume 1 (pp. 21-30). Springer Singapore. doi:10.1007/978-981-13-1742-2_3

[99] Suresh Babu, E., Nagaraju, C., & Krishna Prasad, M. H. M. (2016). Efficient DNA-based cryptographic mechanism to defend and detect blackhole attack in MANETs. In Proceedings of International Conference on ICT for Sustainable Development: ICT4SD 2015 Volume 1 (pp. 695-706). Springer Singapore. doi:10.1007/978-981-10-0129-1_72

[100] T. Gupta, R. Bhatia, Communication technologies in smart grid at different network layers: An overview, in: 2020 International Conference on Intelligent Engineering and Management, ICIEM, IEEE, 2020, pp. 177–182.

[101] T. Hidayat, R. Mahardiko, F.D.S. Tigor, Method of systematic literature review for Internet of Things in zigbee smart agriculture, in: 2020 8th International Conference on Information and Communication Technology, ICoICT, IEEE, 2020, pp. 1–4.

[102] Tanveer, Muhammad "REAP-IIoT: Resource-Efficient Authentication Protocol for the Industrial Internet of Things," J= IEEE Internet of Things Journal, V=9, N=23 P=24453–24465,

[103] Tom, Rijo Jackson and Sankaranarayanan, Suresh and de Albuquerque, Victor Hugo C, and Rodrigues, Joel JPC "Aggregator based RPL for an IoT-fog based power distribution system with 6LoWPAN," China

[104] Toscano, E., & Bello, L. L. (2012, May). Comparative assessments of IEEE 802.15. 4/ZigBee and 6LoWPAN for low-power industrial WSNs in realistic scenarios. In 2012 9th IEEE International Workshop on Factory Communication Systems (pp. 115-124). IEEE.

[105] Tseng, C. Y., Balasubramanyam, P., Ko, C., Limprasittiporn, R., Rowe, J., & Levitt, K. (2003, October). A specification-based intrusion detection system for AODV. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (pp. 125-134). doi:10.1145/986858.986876

[106] Vaigandla, Karthik Kumar and Karne, Radha Krishna and Rao, Allanki Sanyasi "A Study on IoT Technologies, Standards and Protocols," journal=IBMRD's Journal of Management & Research, V=10, N=2, P=7–14, Y=2021.

[107] Vaigandla, Karthik Kumar and Karne, Radha Krishna and Rao, Allanki Sanyasi "A Study on IoT Technologies, Standards and Protocols," IBMRD's Journal of Management & Research, V=10, N=2, P=7–14, Y=2021.

[108] Van Kerkhoven, J., Charlebois, N., Robertson, A., Gibson, B., Ahmed, A., Bouida, Z., & Ibnkahla, M. (2019, April). IPv6-Based Smart Grid Communication over 6LoWPAN. In 2019 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[109] Verma, A., & Ranga, V. (2020). CoSec-RPL: Detection of copycat attacks in RPL based 6LoWPANs using outlier analysis. Telecommunication Systems, 75(1), 43–61. doi:10.1007/s11235-020-00674-w

[110] Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication Systems, 73(1), 3–25. doi:10.1007/s11235-019-00599-z

[111] W. Kassab, K.A. Darabkh, A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations, J. Netw. Comput. Appl. 163 (2020) 102663.

[112] Wang, T., Wang, Y. Y., & Yen, J. C. (2021). It's not my fault: The transfer of information security breach information. In Research Anthology on Artificial Intelligence Applications in Security (pp. 1916–1937). IGI Global.

[113] Wang, Weicheng, and Cicala "Analyzing the attack landscape of Zigbee-enabled IoT systems and reinstating users' privacy," B=Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks,p=133–143, year=2020

[114] X. Wang, Y. Feng, J. Sun, D. Li, H. Yang, Research on Fishery water quality monitoring system based on 6LoWPAN, J. Phys.: Conf. Ser. 1624 (4) (2020) 042057.

[115] Xu, W., Zhang, J., Kim, J. Y., Huang, W., Kanhere, S. S., Jha, S. K., & Hu, W. (2019). The design, implementation, and deployment of a smart lighting system for smart buildings. IEEE Internet of Things Journal, 6(4), 7266–7281. doi:10.1109/JIOT.2019.2915952

[116] Yan Li, Zicheng Chi, Xin Liu, Ting Zhu, Passive-ZigBee: Enabling ZigBee Communication in IoT Networks with 1000X+ Less Power Consumption, 16th ACM Conference on Embedded Networked Sensor Systems (SenSys 2018), pp.4-6, 4 November 2018.

[117] Yavari, Mostafa and Safkhani "An improved blockchain-based authentication protocol for IoT network management" J=Security and Communication Networks, V=2020, P=1–16, Y=2020, publisher= Hindawi Limited

[118] Yavuz, F. Y., Devrim, U. N. A. L., & Ensar, G. U. L. (2018). Deep learning for detection of routing attacks in the Internet of things. International Journal of Computational Intelligence Systems, 12(1), 39. doi:10.2991/ ijcis.2018.25905181

[119] Zaminkar, M., Sarkohaki, F., & Fotohi, R. (2021). A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem. International Journal of Communication Systems, 34(3), e4693. doi:10.1002/dac.4693

[120] Zhou, Q., & Jing, M. (2020). Detecting expressional anomie in social media via fine-grained content mining. Journal of Database Management, 31(1), 1–19. doi:10.4018/JDM.2020010101

[121] Zucheng Huang, Feng Yuan, "Implementation of 6LoWPAN and Its Application in Smart Lighting", Institute of Software Application Technology, Guangzhou & Chinese Academy of Sciences (GZIS), Journal of Computer and Communications, Vol.3 No.3, pp.5-6 March 2015.

List of Publications

Journal Papers

1. **B. Padma** and S. B. Erukala, “End-to-end communication protocol in iot-enabled zigbee network: Investigation and performance analysis,” Internet of Things, vol. 22, p. 100796, 2023.Elsevier **(SCIE)**

2. **B. Padma** and E. S. Babu, “Efficient secure communication in zigbee network using the dna sequence encryption technique,” Life, vol. 13, no. 5, p. 1147, 2023.(MPDI) **(SCIE)**.

3. **B. Padma**, E. Suresh Babu, “Cooperative IDS for detecting collaborative attacks in RPL-AODV protocol in Internet of Everything,” IGI Global (Journal of Database Management (JDM), **(SCIE)**

4. **B. Padma**, E. Suresh Babu "Keys Distribution among End Devices Using Trust-Based Blockchain System for Securing ZigBee-enabled IoT Networks". Elsevier. (Digital Communications and Networks) (Under Review)

Conference Paper

5. Babu, E.S., Devi, A.A., **Padma, B.** (2023). A Trust-Based Blockchain System for Secured Migration of BLE Devices in IoT Networks. In: You, I., Kim, H., Angin, P. (eds) Mobile Internet Security. MobiSec 2022. Communications in Computer and Information Science, vol 1644. Springer, Singapore. https://doi.org/10.1007/978-981-99-4430-9_23