A FRAMEWORK FOR IPv6 BASED ENERGY EFFICIENT ROUTING IN IoT WITH LOW POWER LOSSY NETWORK AND MULTIMODAL SENSORS

Thesis

Submitted in partial fulfillment of the requirements
for the award of the degree of

DOCTOR OF PHILOSOPHY

by

ARCHANA BHAT

DEPARTMENT OF INFORMATION TECHNOLOGY
NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA
SURATHKAL, MANGALORE - 575 025

MAY, 2023

DECLARATION

I hereby declare that the Research Thesis entitled "**A FRAMEWORK FOR IPv6 BASED ENERGY EFFICIENT ROUTING IN IoT WITH LOW POWER LOSSY NETWORK AND MULTIMODAL SENSORS**", which is being submitted to **National Institute of Technology Karnataka, Surathkal** in partial fulfilment of the requirements for the award of the degree of **Doctor of Philosophy** in **Information Technology** is a bonafide report of the research work carried out by me. The material contained in this Research Thesis has not been submitted to any University or Institution for the award of any degree.

Archana Bhat 19/5/2023

Place : NITK - Surathkal
Date : 19/5/2023

ARCHANA BHAT
Reg.No.: 165016IT16FV02
Department of IT,
NITK Surathkal.

CERTIFICATE

This is to certify that the Research Thesis entitled, "**A FRAMEWORK FOR IPv6 BASED ENERGY EFFICIENT ROUTING IN IoT WITH LOW POWER LOSSY NETWORK AND MULTIMODAL SENSORS**", submitted by **ARCHANA BHAT (Reg.no. 165016IT16FV02)**, as the record of research work carried out by her, *is accepted as the Research Thesis* submission in partial fulfilment of the requirements for the award of the degree of **Doctor of Philosophy** in **Information Technology**.

Geetha 19/5/2023

Place : NITK - Surathkal
Date : 19-05-2023

DR. GEETHA V
Research Guide,
Assistant Professor,
Department of IT,
NITK Surathkal.

19/5/2023

Chairman DRPC,
Dept. of IT,
NITK Surathkal.

CHAIRMAN - DRPC
Department of Information Technology
NITK Surathkal, Srinivasnagar P.O.
Mangaluru 575 025, INDIA

I dedicate my thesis to my Grandfather,

Parents, Husband and Sisters.

Acknowledgements

I would like to express my deepest gratitude to my Guide - Dr. Geetha V, for her invaluable feedback on my analysis and framing, her noble guidance, support with full encouragement and enthusiasm. I have benefited greatly from her wealth of knowledge and meticulous editing.

I would like to express my gratitude to my RPAC panel - Dr. Rathnamala Rao, Dept. of ECE and Prof. Ram Mohana Reddy Guddeti, Dept. of IT, for their great feedback.

Many thanks to all of the faculties and staff of Department of Information Technology, NITK for numerous opportunities of learning and all support at times of need. I am thankful for the NITK providing extraordinary experience and for furnishing opportunities for me to grow professionally.

I am grateful to my parents - Shambhavi B and Chidambara K, whose constant love and support kept me motivated and confident. My accomplishments and success are because they believed in me. I also express my deepest gratitude to my Grandfather Late. B. N. Rao, for his unfailing support and continuous encouragement. I owe my deepest gratitude to my husband, Abhay Bhaskar for unconditional support throughout the entire journey. Deepest thanks to my sisters - Ashwini Bhat & Akshatha Bhat, who kept me grounded, and are always supportive of my endeavors.

My Special friends - Gokul, Shridhar, Ashwin, Manjunath, Deepthi, Shashank, Karthik, Thanmayee, and Rashmi deserve my thanks who directly and indirectly provide me inspirations and valuable suggestion during the course of this study.

I acknowledge the generous financial support from the R&D work undertaken in the project under the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India.

ARCHANA BHAT

Abstract

With the advancement in semiconductor technology, a variety of low-end devices armed with different types of sensors are making their way into the market. These devices sense the environment, are capable of connecting to a network and exchange data to support decision making systems. Most of these devices have energy, bandwidth and compute limitations. Given the scale of such devices being deployed, there is a need for a technology that can connect them to the network.

The IEEE 802.15.3 standard defines operations for high-rate (11 to 55 Mbit/s) WPANs. Devices running this standard generally operate on an external power source or have large batteries. It does not work well for devices that do not have high data rates and work on small batteries with limited power source. The IEEE 802.15.4 is the standard that defines the operation of a low-rate wireless personal area network (LR-WPAN) at the physical layer. LR-WPAN is targeted for low power, low bandwidth devices (20 to 250 Kbit/s) vs. WiFi which offers more bandwidth but has higher power requirements.

Given the need is to connect the devices to the Internet, the standard used at the network layer plays a major role. The Internet Protocol (IP) which is the backbone of the Internet is the obvious choice for the network layer. The predominant version of IP used in the networks today is IPv4. But IPv4 has a limited address space that does not fit well to connect millions and billions of IoT devices to the Internet. IPv6 on the other hand with a much larger address space is better suited for the needs of IoT. But the IP cannot be used directly for IEEE 802.15.4 based networks.

To bridge the WPAN and IP based networks, the IETF group defined a new standard for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) in RFC 6282. 6LoWPAN includes encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks. 6LoWPAN operates in a layer between the data-link and network layer called the adaptation layer. In addition to the new adaptation layer, the IETF defines a new routing protocol called IPv6 routing protocol for low-power and

lossy networks (RPL) specifically for low power lossy networks (LLN). RPL is a distance-vector routing protocol that fulfills the requirements of a wide range of LLN applications.

With the growth in semiconductor technology, more and more low cost devices are arriving in the market supporting sensors such as audio, image and video but with limited energy capacity. The focus of most research in the area of LLN has been using sensor networks that operate on scalar data such as temperature, pressure, humidity etc. Scalar sensor networks have lower bandwidth and energy requirements. While the current design paradigms of 6LoWPAN and RPL work well for scalar data, it does not perform well for sensor network with multimodal data such as audio, image, video etc. The primary focus of this research is on improving the performance of 6LoWPAN and RPL for multimodal sensor networks. Only one multimodal data type image is chosen for performance analysis and comparison with existing implementations.

The focus of this research is split into multiple areas. The first area of focus is on improving the parent selection algorithm for RPL that functions better for multimodal sensors. The current parent selection algorithms in RPL do not operate well for multimodal sensors that have different properties in the areas of packet delivery ratio, energy consumption, and latency.

The next area of the research defines a new IPv6 address compression schemes to reduce the overhead of the network layer in a LLN and enable more application data to be encoded in a single 802.15.4 frame. Given the size of a 802.15.4 frame is very limited, it is very important to ensure the network overhead is minimal to increase the percentage of application data that can be transmitted in a single frame.

The research then defines a new weight based ranking scheme in RPL to lower the packet drops and re-transmissions in heterogeneous sensor networks (ones with both scalar and multimodal sensor nodes) by accounting the energy and data-rate requirements for individual nodes and also the link quality between nodes and assigning suitable weights to each. This helps reduce the number of re-transmissions in the network while also increasing the total network lifetime.

Another area of focus of this research is to define a new multicast group management scheme in RPL to optimize the multicast traffic in a LLN. Multicast traffic is important in IoT deployments and improving network efficiency to distribute such traffic is very important. All the proposals in this research is implemented in the Contiki-OS and a comparison of the performance of the same against the current RPL implementation is documented by running tests on Cooja and in the

FiT-IoT lab.

KEYWORDS: 6LoWPAN, Objective Function, IPv6, Multimedia, RPL, IEEE 802.15.4, Address Compression, SCHC Compression, Fragmentation, Header Compression, Multipoint-to-Point Communication, Multimodal Routing, IoT, Contiki Cooja, Multicast, Query, Routing.

Contents

List of Figures

List of Tables

Abbreviations

6LoWPAN IPv6 over Low-Power Wireless Personal Area Networks

AODV Ad Hoc on Demand Vector

DAO-ACK Destination Advertisement Object Acknowledgement

DAO Destination Advertisement Object

DIO DODAG Information Object

DIS DODAG Information Solicitation

DODAG Destination-Oriented Directed Acyclic Graph

ETSI European Telecommunications Standards Institute

ETX Estimated Transmission Count

HEE-OF HopCount, ETX and ENERGY selection based Objective Function

ICMP Internet Control Message Protocol

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IID Network Identifier

IoT Internet of Things

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IS-IS Intermediate System to Intermediate System

LLN Low power lossy network

LLNs Low power lossy networks

M-IoT Multimedia Internet of Things

MP2P Multipoint-To-Point

MRHOF Minimum Rank with Hysteresis Objective Function

MTU Maximum Transmission Unit

OF Objective Functions

OF0 Objective Function Zero

OLSR Optimized Link State Routing

OSPF Open Shortest Path First

P2MP Point-To-Multipoint

QoS Quality of service

RFID Radio-Frequency Identification

RPL IPv6 routing Protocol for Low power lossy networks

SCHC Static Context Header Compression

SOA Service-oriented architecture

UDP User Datagram Protocol

W3C World Wide Web Consortium

WIoT Wearable Internet of Things

WMSN Wireless Multimedia Sensor networks

WPAN Wireless Personal Area Networks

WSN Wireless Sensor networks

Chapter 1

Introduction

Internet of Things (IoT) is an emerging paradigm, where smart objects are seamlessly connected to the overall Internet and can potentially cooperate to achieve common objectives such as supporting smart cities, innovative home automation services, environmental monitoring, urban sensor networks and energy management. The IoT contains the network with resource constraint devices as well as the network with resource available devices. Existing internet technology is the resource available network. The resource constraint networks such as Wireless Sensor networks (WSN) and Wireless Multimedia Sensor networks (WMSN) are mainly designed to sense the environment phenomena. The Wireless Sensor Network and Wireless Multimedia Sensor Network can be deployed either statically or randomly based on application requirement. The current WSN and WMSN are resource constraint non-IP networks.

The idea and development of IoT is focusing on connecting things such as smart cities, smart home and provides facility to handle big data and perform automation for various applications. For certain applications such as habitat monitoring, animal rearing, medical monitoring, it is sufficient to have a small set of nodes with limited resources, as the data collection is based on occurrence of event. The WSN and WMSN are designed for the same, where nodes are tiny in size, resource constraint, and self-configurable for event detection. But WSN/WMSN requires proxies or gateways between internet and WSN/WMSN as they are non-IP based networks.

There is a need for IP based address to connect each device on Internet. Internet Protocol version 4 (IPv4) has depleted since late 2010 to 2011, as a result, it needs a larger addressing space to accommodate the ever increasing growth of network devices. The Internet Protocol version 6 (IPv6) is current solution for the same. This IPv6 provides larger address space to accommodate the increased demand along with better traffic routing and safety. Sometimes even routers and their interconnects are highly resource constrained. It is required that the reachability of a router be verified before the router can be used as a parent. IP based routing protocol for low power and lossy networks is one of the challenging issue for multimodal sensor network.

IoT has several large scale applications http://european-iot-pilots.eu/ in deployments today. Activage is a project where IoT is being used for smart living environments to help senior citizens age better. Autopilot is a project where IoT is being leveraged for self-driven cars. IoF2020 is a project where IoT is being leveraged to improve farming.

Certain applications such as, Vehicular network, Industrial IoT, Agricultural IoT etc needs a collection of data through multimodal sensors as well as enabling/disabling actuators. In such cases to connect each device to internet directly, it needs IP based communication protocol on each device.Low power lossy networks (LLNs) are the network which are IP enabled nodes with limited resources in terms of processing power, battery and memory, and their interconnects are characterized by unstable links with high loss rates, low data rates and low packet delivery rates. Since IPv4 is having limitation on addressing a very large number of nodes in network, the IPv6 based LLNs are proposed in literature. In such applications, each Low power lossy network (LLN) can contain a small set of sensors to sense the environment, which can be identified as multimodal sensor nodes, as the type of sensor data sensed by sensors may be scalar, image, audio or video. Routing the multimodal data to destination is an important task in such kind of networks. Wi-Fi network supports multimodal sensor data transmission over Wi-Fi. But Wi-Fi consumes scalability and resource constraint that makes Wi-Fi not much suitable. As a result there is a need for efficient routing protocol for IPv6 based multimodal sensor nodes based on available resources, types of sensors, data and network availability. In a network, the specifications of multimodal sensors for sensing the same type data can either be the same across all the nodes or different. For example, the sensors used on two different nodes responsible for motion capture can be two different models. This work mainly focuses on developing an efficient IPv6 based routing protocol for both types of networks in the context of IoT.

To support IoT in smart cities and monitoring and management of systems, there is a need for developing IPv6 based LLN with multimodal sensors. As of our knowledge, developing an efficient routing algorithm for such kind of systems is a novel approach.

1.1 Internet of Things

The Internet of things (IoT) is a system that enables a new connected experience by changing the way people interact with everything around them. The devices around people sense the environment around and push it to a central server that derives meaningful inference out of them to drive the connected experience. The actors in IoT include the people, the end devices that people use or are around and servers.

Internet is a worldwide network linking millions of engrained hardware devices, providing diversity of information and communication amenities, consisting of interconnected networks using standardized communication protocol. A thing, in the context of the Internet of things (IoT), is an entity or physical object that has an exclusive identifier, an engrained system and the capability to transmit information over a network. Today a mediocre family has more devices at home connected to the internet than those who dwell there. Every device on internet is identifiable with the unique ID, the IP address. Huge increase in address space of IPv6 is a vital aspect for the advancement of the Internet of Things. Currently, the quantum of intelligent devices continue to grow exponentially, giving these nifty things the ability to sense, interpret, control, actuate, communicate and negotiate over the hyper-connected Internet of Things space. Things can be cars, buses and trains or wearable devices such as smart watches, wrist bands, smartphone robots, unmanned aerial vehicles and many more.

IoT exploits latest improvements in software technologies, plummeting hardware costs, and present-day attitudes concerning technology. It's new and cutting-edge elements bring main alterations in the delivery of products, goods, and services; and the social, economic, and political impact of those alterations. The added value to the IoT is created by the information that is collected by IoT devices which go through five phases of IoT lifecycle as shown in the Figure 1.1:

1. Phase 1 is where the information is collected from the physical environment by the devices or sensors. This is termed the 'Create Phase'.

2. Phase 2 is where the information collected in the first phase is transmitted to the desired destination via the network. This is called the 'Communicate Phase'.

3. Phase 3 involves aggregation of all the data collected by various devices in the network. This phase is called the 'Aggregate Phase'.

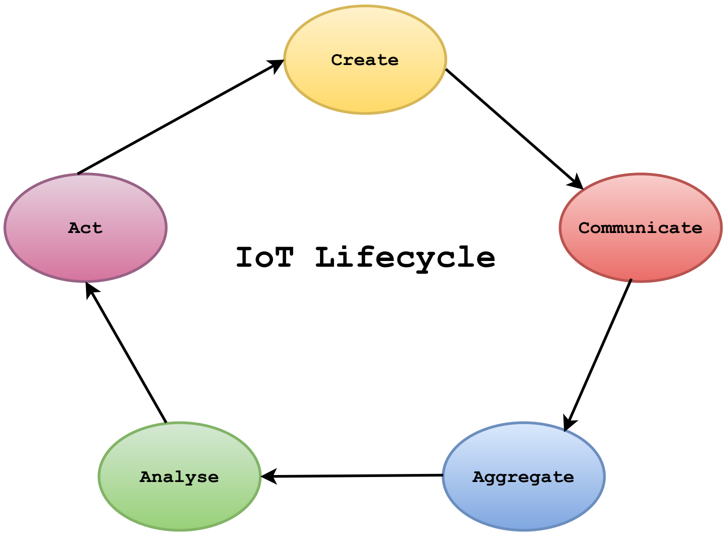


Figure 1.1: IoT Lifecycle

4. Phase 4 is when the aggregated data is analysed. The analysis can lead to generation of patterns that in turn can help optimize processes and workflows. This is termed the 'Analyse Phase'.

5. Phase 5, the 'Act Phase' is the last phase where actions are taken based on the analytical data generated in the previous phase.

The IoT is a complex system with a number of characteristics. It's characteristics vary from one domain to another. The pivotal features of the IoT are as follows.

1. Inter-connectivity in IoT: Anything can be intersected with the worldwide information and communication structure. The most basic piece of the IoT puzzle is connecting things to the Internet. There are several options available to interconnect things. The options include but not limited to Cellular, RFID, Bluetooth, WiFi, NFC, LPAN, Satellite and Ethernet. There are different service providers for each of these services.

2. Things-related services: The IoT shall provide services that are specific to the thing. The services can include privacy protection, a consistent semantics between physical and the virtual things extending for the physical thing. The technologies in the physical and information world needs to change to provide such services.

3. Heterogeneity: The devices in the IoT run on different types of hardware platforms and connect using different types of networks. Thus, an IoT net-

work is heterogeneous in nature both in terms of the types of platforms and how they connect to the network.

4. Enormous scale: The devices which converse with each other and those which require management will be larger than the devices connected to the internet in terms of magnitude.

5. Safety: As the nodes are deployed in open environment, the safety is one of the important aspect in Internet of Things. Safety relates to security of personal data, physical devices and security of communications. Creating a secure paradigm that shall sustain result from securing the endpoints, network and the data moving across it.

6. Connectivity: The compatibility and accessibility of data is ensured by connectivity. If accessibility is getting on a network then compatibility aids the consumption and production of data.

1.1.1 Architecture of Internet of Things

Radio-Frequency Identification (RFID) is a technology that is based on utilizing radio waves to identify objects from few inches to hundreds of feet away. It uses a RFID tag and a RFID reader for the purpose of identification. While the technology is effective for longer read range and faster scanning use cases, it suffers in the areas of cost and lack of privacy.

WSN is a technology that connect several devices running low-cost sensors. The devices run multiple sensors that sense things around them and exchange data over the network. WSN is designed to extend the lifetime of these low energy and low-cost devices. WSN is a part of the larger IoT scheme where millions of such devices communicate with each other to accomplish several tasks (Kocakulak and Butun, 2017).

Service-oriented architecture (SOA) is a model that is designed to allow services housed on different platforms programmed using different languages to come together to form large applications. A typical service in the context of SOA is meant to accomplish a specific task and is self-contained.

The architecture of Internet of Things has four layers as shown in Figure 1.2, networked things, typically wireless sensors and actuators form the first layer of IoT architecture. Layer 2 Gateway and network includes sensor data aggregation systems and analog-to-digital data conversion. In Layer 3 Management service is in charge of information analytic, security control, process modeling and device

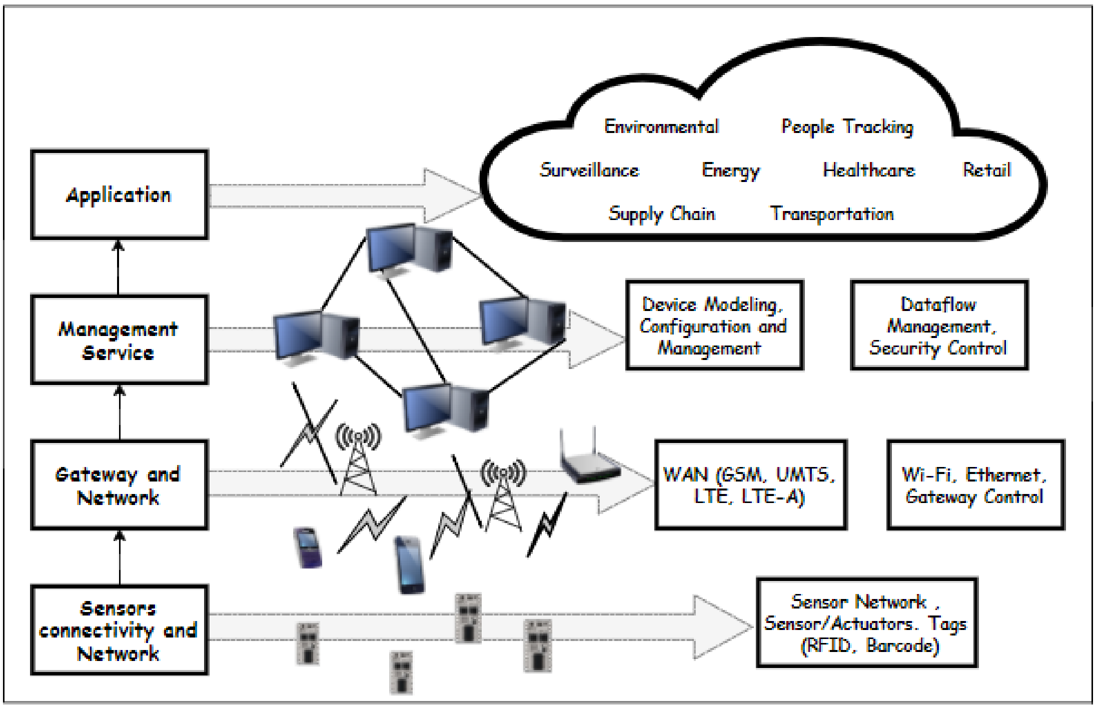


Figure 1.2: Internet of Things Architecture

management. The preprocessing of the data takes place before it proceeds on to the data center or cloud. Lastly, in Layer 4, Application can be classified based on the type of network availability, the coverage size, the heterogeneity.

1.1.2 Architecture of IoT Network

The architecture of the IoT Network is shown in Figure 1.3. IoT nodes at the leafs communicate with each other over a IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) network and a gateway at the edge of every such network will terminate the 6LoWPAN connection and use traditional IPv4/IPv6 packets to communicate to/from the cloud.

1.1.3 Applications of the Internet of Things

IoT has several applications due to its flexibility of adapting to any vertical that uses technology capable of generating information related to operations and work environment. These can be monitored and controlled remotely through the use of IoT. Various industries today have adopted IoT to simplify and automate many of their business operations. Following are some of the applications of Internet of Things.

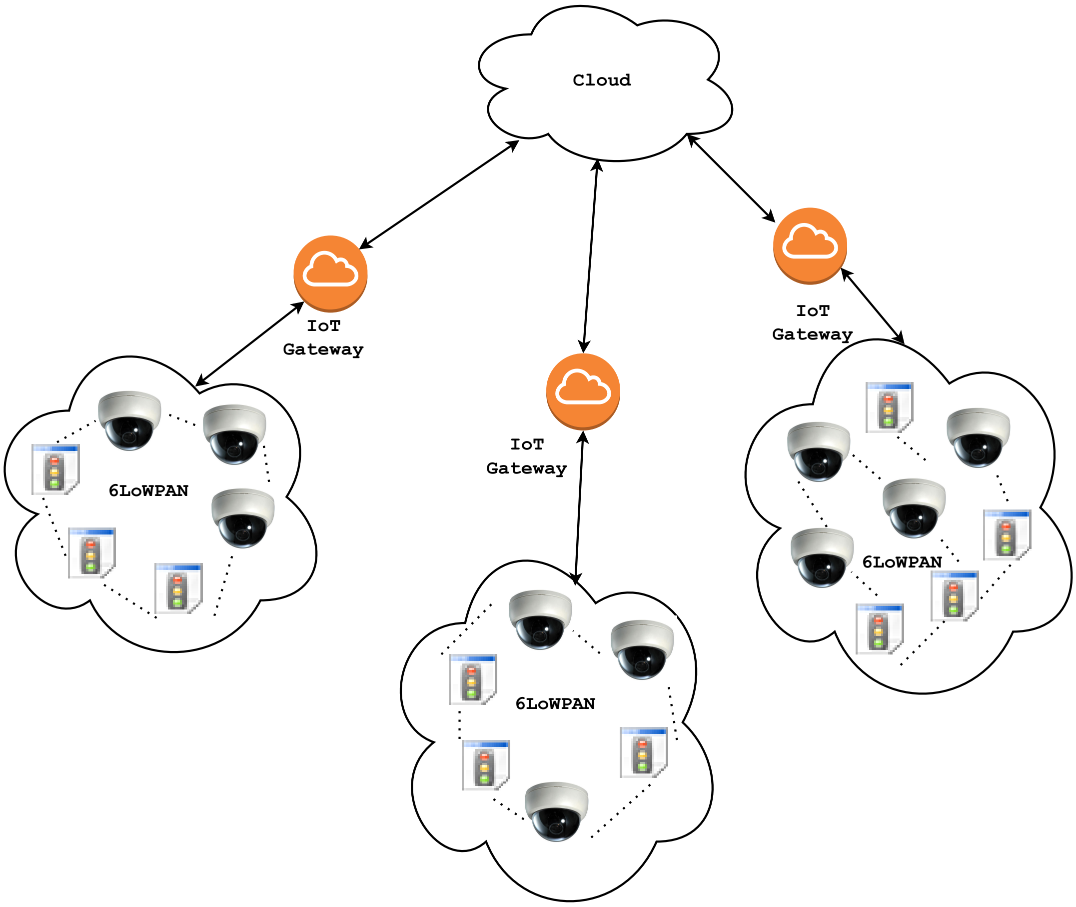


Figure 1.3: IoT Network Architecture

1. Smart Home: In contemporary times, smart home is likely the most widespread IoT application, known for its affordability and easy availability to consumers. The home automation system and smart home application provides a way for user to interact with various items in the home through internet. It also provides remote handling and remote monitoring along with intelligent safety system for the house.

2. Wearable: Nowadays, wrist watches are used for many purposes such as chatting with text message, making phone calls, recording, etc. Devices such as Fitbit and Jawbone have revolutionised the fitness world by providing details about workouts.

3. Smart Cities: By the way of providing solutions to real world problems faced by citizens regarding traffic, availability of service, instant help etc, IoT has the ability to renovate entire cities. With the proper techniques, connections for communication and data collection and information processing, the In-

ternet of Things can resolve various issues like traffic congestion and noise, crime, and pollution.

4. Health Monitoring: With the use of IoT in medical devices that are either planted inside the patient or the patient is externally connected to, doctors can monitor patients remotely reducing the need to physically visit hospitals. Additionally, these devices can also alert doctors during a medical emergency potentially saving lives.

5. Connected Cars: Vehicles equipped with Internet access can share access with others similarly like associating with a wireless network at home or office. The vehicular network can provide more services with these connected vehicles for traffic monitoring, lowering accidents, and informing concerned departments and other vehicles when any accident happens on road.

1.1.4 Issues and Challenges in Internet of Things

The Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits.

1. Robustness: Localization, resource utilization, coverage problem, power usage optimization and communication protocols requires improvement for static and dynamic deployment.

2. Coordination: Coordination of static and mobile nodes for data transmission is an issue as the neighbours of the node changes frequently due to mobile nodes.

3. Information retrieval: The network collects a large amount of data from various devices connected to Internet of things. The storage and information retrieval from collected big data, in IoT is a challenging task, as the information leads for appropriate decision making.

4. Organization: Organization of resource constraint and resourceful devices to existing network, along with new strategic networks is an important issue, as it requires standardization of the system which can cooperatively run with existing networks.

5. Platform for heterogeneous network: Most of the proposed work on IoT concentrates on homogeneous networks such as adhoc network, vehicular

network. But, the system needs enough structure/ platform for communication between heterogeneous networks, where the availability of resource depends on application.

6. Multimodal sensors data routing: In Multimedia Communication Sensor network ensures collection and communication of multimedia information. In addition to data delivery, nodes typical of scalar sensor networks, multimedia data include snapshot and streaming multimedia content. Processing and delivery of multimedia content demand high bandwidth for transmission as they are dependent and their interaction has a major influence on the achievable Quality of service (QoS).

7. Link layer challenges: The link layer protocols must be energy efficient as nodes are resource constraint. The Link layer protocols may also require fragmentation to transfer large network layer packets. The re-transmission techniques must be able to support multimodal data over the network.

Privacy is a concern with respect to IoT application as the same is managed and run by multiple technologies and multiple vendors are involved in it. The architectures of these multiple technologies vary from one another which adds to the complexity of the IoT network. Hence any glitch or failure in the IoT network requires additional time for restoration of services to consumers.

1.2 Challenges in WSN and WMSN

Routing protocols in WSN are responsible for discovering and maintaining energy efficient routes, in order to make communication reliable and efficient (Kocakulak and Butun, 2017). Monitoring the status of nodes is a challenge in WSN in the context of IoT as the nodes are identified by arbitrary IDs and not IP addresses. Additionally, a gateway is essential to connect a WSN based network to the Internet. It is desirable to have nodes be IP based making it easy to monitor and manage in the context of IoT.

Integration with Internet (IP) architecture: As the advancement of the sensor based networks commercially is dependent on the assimilation of such networks with Internet Protocol (IP). A remotely accessible WMSN requires it to be integrated with the IP architecture (Akyildiz *et al.*, 2007).

1.3 Low Power and Lossy Networks (LLN's)

The Internet of Things (IoT) contains a large network of low powered devices with limited memory and compute capabilities. These devices have short wireless range and very high loss rates. A network of such devices is termed LLN. The Internet Engineering Task Force (IETF) in an attempt to address the constraints and unique requirements of such a network created the 6LoWPAN Working Group (IPv6 in Low-Power Wireless Personal Area Networks). The objective of this group is to define a standard necessary for the adaptation of IPv6 networks using IEEE 802.15.4 physical and MAC layers.

LLNs are those networks which are highly resource constrained with respect to routers and their interconnects. Routers are usually limited in terms of processing power, battery and memory, and their interconnects are characterized by links which are unstable with low data rates, high loss rates, and low packet delivery rates. IEEE 802.15.4, Bluetooth, Low Power WiFi, wired or other low power PLC links interconnect these networks. The traffic patterns are also varied, and may comprise of point to point (P2P), point to multipoint (P2MP) or multipoint to point (MP2P). They can potentially comprise thousands of nodes. In order to avoid the problem of non interoperable networks that are interconnected by protocol translation gateways and proxies, LLNs are transitioning to an end-to-end IP-based solution.

An additional consideration is that high data-traffic very easily leads to network congestion. Such scenarios cause large amount of packet loss and delay. Since sensor networks are commonly deployed in environments with potentially high data-traffic and requires a time-sensitive response, it is essential to consider while designing a routing protocol for LLNs.

Multimodal sensor includes various sensor like video, audio, image, temperature, humidity and so on. Multimodal sensors can be homogeneous or heterogeneous based on the application. The routing of data must be based on type of data for transmission and resource availability in the path. So main focus is to develop a IPv6 based routing algorithm for multimodal sensor networks for IoT.

1.4 RPL

IPv6 routing Protocol for Low power lossy networks (RPL) by Winter (2012) is specified in RFC 6550. Contiki-NG implements this RFC in it's IPv6 network stack. RPL builds a Destination-Oriented Directed Acyclic Graph (DODAG) topology that starts a designated root node. This root node most often serves as the border router to connect to the Internet. Trickle timers are used to periodically transmit broadcast frames containing routing information. An objective function governs how a topology is built. The goal of an objective function can be to keep the Estimated Transmission Count (ETX) to a minimum on the path to the root of the network. The topology is built according to a certain goal by an objective function. Contiki-NG implements two objective functions Minimum Rank with Hysteresis Objective Function (MRHOF) and Objective Function Zero (OF0), both of which try to minimize the ETX on the path to the root node.

The different traffic directions in RPL include:

1. Upward routing: Traffic destined to root from any node.

2. Downward routing: Traffic destined to any node from the root.

3. Any-to-any routing: Traffic between any two nodes in the network. Packets are routed upwards to the nearest common ancestor in case of storing mode and to the root node in case of non-storing mode. They are then sent downwards towards the destination.

The upward routing for a packet is handled at every node on it's path to the root node. The nodes forward the packet through their preferred parent. The downward routing is handled differently based on the mode used: *non-storing* and *storing mode*.

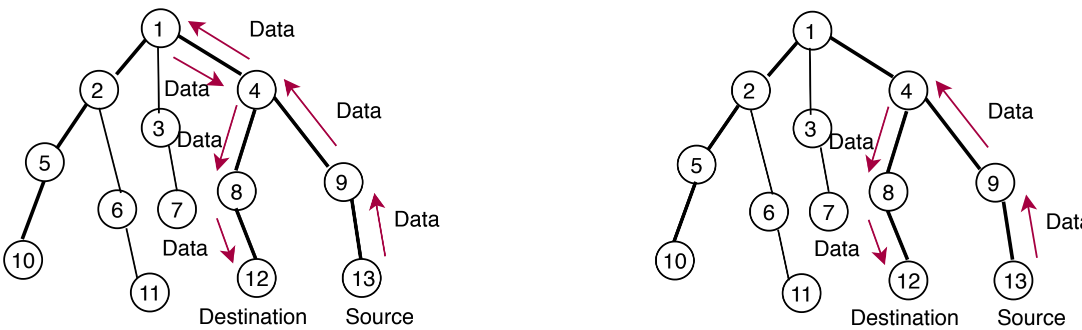


Figure 1.4: Non-Storing and Storing mode

The non-storing mode operation is depicted in Figure 1.4. It uses IPv6 source routing to forward the packet. This can result in the packets getting very large if the number of hops between the source and destination are significant. But the advantage of using this mode is that nodes do not have the necessity to maintain the routing table for nodes below them in the DODAG.

In the storing mode operation also depicted in Figure 1.4, the routing table is maintained by each node in the network. This avoids large routing headers in IPv6 packets when sending packets across multiple hops towards the destination but increases the memory footprint on nodes due to the need for storing the routing table.

1.4.1 Control Messages of RPL

RPL has four different types of messages to create and manage a topology:

1. DODAG Information Object (DIO) : The DIO are control messages used to share information to create and maintain a DODAG. The designated root of the network broadcasts this message first and each node starts transmitting one of its own after receiving one.

2. DODAG Information Solicitation (DIS) : The DIS is a control message used by a node to advertise that it is available to join a DODAG. These are used by nodes when they do not get any DIO frames within a specified amount of time.

3. Destination Advertisement Object (DAO) : The DAO messages are transmitted by nodes to their parents. This is used by nodes to indicate to their parents that they have been chosen as one.

4. Destination Advertisement Object Acknowledgement (DAO-ACK) : The DAO-ACK is a control message that is used to acknowledge a DAO message received.

1.5 Motivation

Routing protocols in WSNs are responsible for discovering and maintaining energy efficient routes, in order to make communication reliable and efficient. Monitoring the status of nodes is a challenge in WSN in the context of IoT as the nodes are identified by arbitrary IDs and not IP addresses. Additionally, a gateway is essential to connect a WSN based network to the Internet. It is desirable to have nodes be IP based making it easy to monitor and manage in the context of IoT.

The main focus is on finding a routing protocol for low power lossy nodes with multimodal sensor networks. All devices are required to have IP addresses. Addressing assist to ensure whether the device performs its task or not. If the nodes are IP based, it is easier to access individual sensor nodes through Internet, as it helps to query and collect information from either a single node or from group of nodes. It is essential to assign IPv6 address for each node to communicate and collaborate in the network. Hence, the proposed framework helps in developing an efficient IPv6 based routing protocol in Low Power Lossy Networks for homogeneous or heterogeneous based multimodal sensor network.

1.6 Problem Statement and Objectives

1.6.1 Problem Statement

"To Design and Develop an energy efficient IPv6 based routing protocol for IoT with low power and Lossy networks which contains homogeneous or heterogeneous multimodal sensors, for Smart City with respect to resource utilization, communication overhead and delay".

1.6.2 Objectives

1. To design and develop Hybrid Objective Function to improve the performance of 6LoWPAN Adaptation Layer based IPv6 IoT network with multimodal sensors.

2. To design and develop Address Compression Techniques for 6LoWPAN.

3. To design and develop energy efficient multipoint to point routing protocol for IoT network with multimodal sensors.

4. To design and develop energy efficient point to multipoint routing protocol for IoT network with multimodal sensors.

5. Performance analysis of proposed multimodal sensor communication in IPv6 based Low Power Lossy Networks testbed.

1.6.3 Publications based on Research Work

1. Archana Bhat, Geetha V "*Hybrid HopCount, ETX and ENERGY Based Objective Function (HEE_OF) for Image Data Transmission over 6LoWPAN in IoT*". International Journal of Wireless and Mobile Computing(IJWMC), InderScience [Scopus] (Accepted).

2. G. V., A. Bhat and S. Thanmayee, "New Bit Pattern Based IPv6 Address Compression Techniques for 6LoWPAN Header Compression," in IEEE Access, vol. 10, pp. 80055-80070, 2022, doi: 10.1109/ACCESS.2022.3193235.

3. Archana Bhat, Geetha V "*Ranking based RPL for Multipoint-to-Point Multimodal Data Communication in IoT Network*". Journal of Wireless personal Communications, Springer. https://www.researchsquare.com/article/rs-742884/v1 (Under Review).

4. Archana Bhat, Geetha V "*Multicast Group Management based RPL for Point to Multipoint Multimodal Data Communication*". Ad Hoc Networks, Elsevier (Working on review comments).

5. A. Bhat and V. Geetha, "Survey on routing protocols for Internet of Things," 2017 7th International Symposium on Embedded Computing and System Design (ISED), Durgapur, India, 2017, pp. 1-5, doi: 10.1109/ISED.2017.8303949.

1.7 Organization of the Thesis

A high level overview of research carried out with respect to proposed system and our contributions towards defined objectives is shown in Figure 1.5

In the application layer, the type of the sensor data is determined. It can be one of scalar or multimodal data. After processing the information, if the data received is scalar then routing will be delay tolerant. In case the type of sensor data is image then routing can have minimum delay tolerant otherwise routing will meet the QoS based routing.

At the 6LoWPAN layer, supports with Objective Functions (OF) for supporting routing, header compression and fragmentation to reduce the number of bits in IPv6 header, so that the packet can be transmitted over IEEE 802.15.4 MAC which has limitation of 127 bytes. Hence, performance analysis of existing Objective Functions are performed and a hybrid Objective Function based on Hop count, ETX and Energy HopCount, ETX and ENERGY selection based Objective Function (HEE-OF) parameters is proposed.

At the network layer, the neighbors of the node are ranked based on various metrics and the weights assigned to each. This ranking scheme is used to determine the parent for a given node. Additionally, in case of Multipoint-To-Point (MP2P)

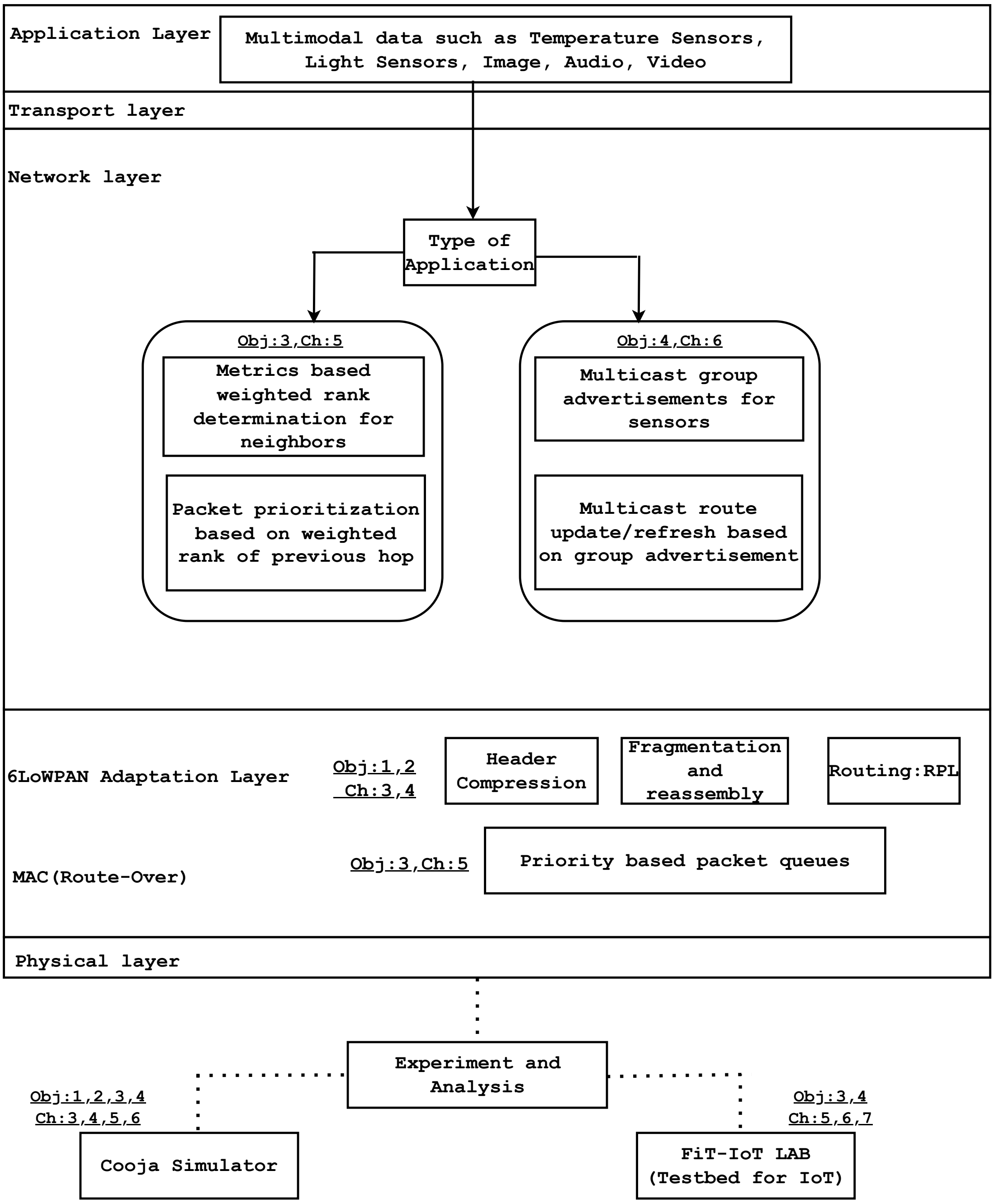


Figure 1.5: Proposed System

transmission, when a packet from the application layer enters the network layer destined towards the root of the network, a priority is assigned to the packet based on the previous hop. This priority is carried in the packet metadata to the MAC layer. At the MAC layer, the packet is queued based on the priority assigned. Lower priority packets are dropped in favor of higher priority frames ensuring the network can support the necessary QoS requirements of multimodal applications.

In case of Point-To-Multipoint (P2MP) transmission, traffic originating from different sensors are grouped under different multicast addresses. These groups are advertised from the root of the network enabling the rest of the network to join or leave groups based on the sensors housed on the node and its downstream network. This optimizes the flow of multicast packets destined to a certain group address in the network and restricts it to only those areas of the network that are subscribed to it instead of flooding them in the entire network. In addition to the flow and route optimization, the packets are compressed at the network layer to increase the amount of application data that can be carried in a frame which in turn reduces the total number of packets required to transmit the same amount of application data in the network. Implemented the proposals in the Contiki-OS and compare the performance against the current RPL implementation by running tests on Cooja and FIT-IoT lab.

The organization of thesis as follows. In chapter 2, brief literature review on the Internet of Things, RPL are presented. In chapter 3 and 4, the proposed Objective Function for multimodal network and the need for header compression techniques has been considered. In chapter 5, the proposed approach for Multipoint-to-Point regarding best parent selection has been presented. In chapter 6, Point-to-Multipoint transmission has been discussed. In chapter 7, implementation of proposed work has been compared with FiT-IoT lab.

1.8 Summary

With the exponential growth in the number of low cost sensor based devices and the need to interconnect them for meaningful applications, there is a shift to use IP over the traditional WSN (Kocakulak and Butun, 2017) and WMSN standards for building a network of such devices. While the 6LoWPAN and RPL provide the foundation to connect such low cost devices to the Internet, the initial work was on devices generating scalar data. The current design of the 6LoWPAN and RPL based networks does not scale when connecting devices that generate multimodal data such as image, audio and video. Thus, there is an opportunity to improve the technology in the context of multimodal devices.

Chapter 2

Literature Review

The IoT provides an outstanding market opportunity for Internet service providers, application developers, and equipment manufacturers. Various groups such as World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF), EPCglobal, Institute of Electrical and Electronics Engineers (IEEE), and the European Telecommunications Standards Institute (ETSI) are leading the activity to define protocols to enable IoT networks. In the subsequent sections, discussed six main elements needed to deliver the functionality of the IoT followed by the Protocol RPL with various fields of Routing protocols and concluded by the outcome of the literature survey.

2.1 IoT Essentials

In order to gain better insights into the real meaning and functionality of the IoT, it is important that we understand the IoT essentials (Al-Fuqaha *et al.*, 2015) as shown in Figure 2.1. IoT is the combination of various field like Identification, sensing, communication, computation, services, semantics and application. This section, explains various research issues in each of these areas related to Internet of Things.

IoT = Identification + Sensing + Communication + Computation + Services + Semantics.

For the purpose of naming and matching services with their demand, identification is vital for the IoT and also considered as the first important element. Multiple identification techniques are available for the IoT such as Radio Frequency Identification (RFID), barcode/2D code, electronic product codes (EPC), and ubiquitous codes (uCode) (Yashiro *et al.*, 2013). It is assumed to be a funda-

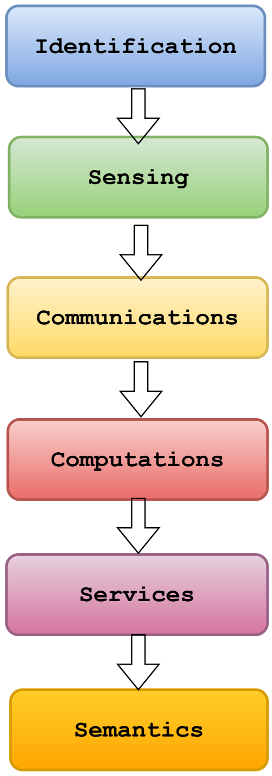


Figure 2.1: IoT Essentials

mental factor in developing a connection or relationship between individuals and is essential for IoT system success. It allows us to identify billions of heterogeneous objects and manage remote objects through the Internet. Addressing the IoT objects includes IPv4, IPv6, and 6LoWPAN. Using 6LoWPAN causes IPv6 addresses suitable for low-power wireless networks. But these addresses are not globally unique. They are unique within the network. This way identification provides a precise and distinctive identity.

The gathering of data from corresponding objects within the network and sending it back to a data warehouse, database, or cloud is termed as sensing operation in IoT. The collected data is then analysed in order to take specific actions based on required services. The IoT sensors can be actuators, smart sensors or wearable sensing devices. The technology of wearable devices is booming and has created a new segment - Wearable Internet of Things (WIoT) (Hiremath *et al.*, 2014). The capabilities of wearable devices that can sense, compute and communicate is transforming the health sector. WIoT requires a strong framework in the areas of networking, compute, storage and visualization to design solutions that are acceptable clinically. In general, the sensor devices must be energy efficient, easy to connect with devices and accurate enough to sense the environment.

The IoT communication Technologies supports delivering smart services by connecting heterogeneous objects. In Saloni and Hegde (2016), it indicates about Neighbour Awareness Network(NAN) known as Wi-Fi aware, is a standard, which enables low power discovery over Wi-Fi. In Kumar and Lee (2014) Bluetooth or internet connection is used for connecting smart living system. In order to control home devices remotely Fuller and Ramsey (2015) and Yassein *et al.* (2016), Z-Wave protocol has been implemented in smart homes which provide better reliability, low radio rebirth, easy usage, and easy interoperability than ZigBee protocol. Radio Frequency Identification (RFID) and Ultimate Web Designers(UWD) (Nekoogar and Dowla, 2016) are the specific communication technologies. Passive RFID tags integrated with sensors, play an important role in IoT ecosystem for longer range sensor applications. They represent the advantage of separating the forward link and reverse link channels in passive RFIDs and use UWB-UHF hybrid signalling to better fit in an IoT space. The author proposed system helps in improving the powering range of UWB passive tags. Near Field Communication(NFC - Contactless communication between devices like smartphones or tablets) (Garrido *et al.*, 2010) works at high Frequency band in association with services and resources to augmented objects through tags. For testing the utility and functionality of the interaction model, NFC Scenarios Creator(NFCSC) is used. Communication technologies for IoT further needs research for connecting a very large number of sensor nodes with multimodal sensors.

The "brain" and the computational ability of the IoT is represented by the processing units (e.g.microcontrollers, microprocessors, SOCs, FPGAs) and software applications. Hardware Platforms use Raspberry Pi client-server communication using various wireless communication as Wi-Fi and ZigBee (Maksimović *et al.*, 2014) (Zhao *et al.*, 2015). The methodology indicates that Raspberry Pi is used as server by connecting it to several laptops as client in the same network. Software platform includes Operating systems (Baccelli *et al.*, 2013) (Gaur and Tahiliani, 2015) with different kernel architecture, various programming model, scheduling based on system performance, network connectivity, extension of memory management and portability with respect to different hardware platforms. It also has many real-time Operating systems (RTOS) that are very useful for designing IoT applications. For IoT scenarios, Contiki RTOS has come into existence. The Cooja simulator of ContikiOS will stimulate and emulate the WSN and IoT applications. Apart from software and hardware platforms for computational, cloud platforms are much of a need for IoT-based applications. This helps the smart objects to transfer the data to the cloud and help the end-users to aid the knowledge from the gathered data. It also helps the big data to be processed. Even free and commercial cloud services are available to provide IoT services.

IoT services can be classified into four classes; Identity-related services (Existing applications) - basic services, information aggregation(Smart Grid) - To gather and condense basic sensory measurements that is essential to be function and conveyed to the IoT application. (Rahman *et al.*, 2016), Collaborative Aware(Smart Home) (Fuller and Ramsey, 2015), (Yassein *et al.*, 2016) - data to make decision and respond accordingly, and/or ubiquitous(Smart City) (Madakam and Ramaswamy, 2015) - anytime and anywhere.

The ability to extract knowledge smartly by various machines to supply the required services is referred to as Semantic. Knowledge extraction includes identifying and examining data right decision for the exact service. Semantic in the IoT represents the brain of the IoT by sending demands to the right resources. Semantic Web technologies are the Web Ontology Language (OWL)(Yang *et al.*, 2011) and Resource Description Framework (RDF). In 2011, the World Wide Web Consortium (W3C) adopted the Efficient XML Interchange (EXI) format as a recommendation. EXI helps to improve XML applications for constrained environments. It helps to decrease the bandwidth without impacting the resources that has already existed.

Small devices are unable to communicate with constrained resources. In addition to that IoT has to take care of heterogeneity as billions of different sensors, computers and other communication elements need to be connected together which may work on different protocols.

1. COAP: Constrained Application Protocol aims at enabling tiny devices with low power, computation and communication capabilities to utilize RESTful interactions. Base CoAP is insensible to network conditions. So, (Betzler *et al.*, 2016), CoCoA provides congestion control solution and offers performance that is better than or at least similar to that of default CoAP.

2. MQTT: Message Queue telemetry transport aims at connecting embedded devices and networks with middleware and applications. It describes new methods of connecting devices in home networks and the internet that reduce data traffic by the use of MQTT brokers. In (Gomes *et al.*, 2015), the proposed architecture connection between ISO/IEEE 11073 agents and managers have been established. It creates an automatic discovery mechanism of new devices in home networks.

2.2 Routing in Internet of Things

In sensor networks IP connectivity mainly relies on two IETF standards: 6LoWPAN (Kushalnagar *et al.*, 2007*c*) and RPL (Winter, 2012). 6LoWPAN is an acronym for IPV6 over Low Power Personal Area Networks. The new standard, IEEE 802.15.4 defined by the IETF 6LoWPAN enables a wireless based IPv6 communication between nodes (ex: sensor nodes) that have low-power radio, limited energy, storage, and memory.

6LoWPAN adds IP capabilities to a WSN node. A new adaptation layer over the IEEE 802.15.4 link layer allows TCP/IP based communication over a IEEE 802.15.4 network. This is essential because a conventional IP stack does not fit within a single IEEE 802.15.4 frame.

6LoWPAN with support for low-power IP based devices and a mesh network is enabling more devices to connect to the cloud each day which is essential for IoT and IoT based applications. IPv6 over Low-Power Wireless Personal Area Networks" or simply 6LoWPAN (RFC 6282) is an adaptation layer enabling the capability to carry IPv6 based frames efficiently over link layers technologies with small MTU such as IEEE 802.15.4. Using an IP based architecture allows IoT applications to take full advantage of the IP technologies which is visible with the Internet and its multiple billion users.

IPv6 is suited for a dense 6LoWPAN because of its large addressing space of IPv6. Without using any proxies, 6LoWPAN makes IoT and other devices connect to IP based network. It helps to utilize relevant tools and various protocols run on top of IP technologies. A representation of the technologies and the corresponding layer is shown in Figure 2.2.

Application Layer	MQTT, CoAP
Transport Layer	TCP,UDP
Network Layer	6LoWPAN with RPL
Physical & MAC Layer	IEEE 802.15.4

Figure 2.2: 6LoWPAN Protocol Stack Olsson (2014)

The Internet Engineering Task Force (IETF) is an open international community of network designers and researchers. IETF has taken the initiatives in standardizing communication protocols and developing internet protocols for WSNs including the Routing Protocol for Low-Power and Lossy-Networks (RPL). Routing Over Low-power and Lossy networks (ROLL) working group have made their efforts in standardising a link independent routing protocol that is based on IPv6 for LLNs named RPL.

Based on the detailed analysis and evaluations conducted by ROLL working group on the existing routing protocols such as Intermediate System to Intermediate System (IS-IS) (Przygienda, 2002), Open Shortest Path First (OSPF) (Chapin *et al.*, 1992), Ad Hoc on Demand Vector (AODV) (Perkins *et al.*, 2003) and Optimized Link State Routing (OLSR) (Clausen and Jacquet, 2003), led ROLL to deduce that these protocols failed in satisfying the requirements of LLNs. The requirements of multipoint-to-point application in WSNs were not satisfied by traditional IP routing protocols, therefore ROLL WG aimed to provide IPv6 routing architectural framework for IoT's application scenarios.

If power was not a problem and wireless/radio path unimpeded, this could force all the sensors to talk to a single controller. But this is not the case. So RPL assumes that:

1. The sensors need to construct paths back to a controller of some kind.
2. Some or all of the sensors are constrained by power.
3. Some sensors lack a direct path to the controller and will need other sensors to pass on their data to the controller.

Significant research in RPL can be classified into different categories, on the basis of methodologies employed in these systems as shown in Figure 2.3

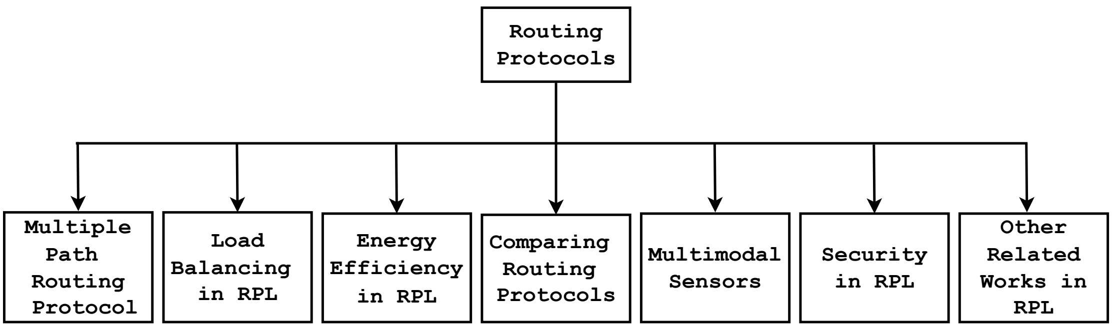


Figure 2.3: Classification of Routing protocols

1. Multiple Path Routing Protocol

2. Load Balancing in RPL
3. Energy Efficiency in RPL
4. Comparing Routing Protocols
5. Multimodal Senosrs
6. Security in RPL
7. Other related works in RPL

2.2.1 Multiple Paths Routing Protocol

When single-path routing is considered, it achieves minimum resource utilization and computational complexity, thus reducing the feasible output of the network. Throughput increases when active path becomes congested and fails to transfer the data than searching multiple paths in high traffic load. The Table 2.1 and Table 2.2 depicts the work in the area of RPL with multiple path routing protocol.

Multipath routing Lodhi *et al.* (2015) strives to find several paths to the destination from a source node. Multipath routing achieves higher reliability, increased throughput, fault tolerance and congestion mitigation. It also provides temporary Multipath routing only during when congestion occurs. Still further study on load imbalance network is required.

In paper Le *et al.* (2014) highlighted drawbacks of single path routing protocol. They focused on multipath solutions for RPL routing protocol for energy load balancing, fast local repair and combination of both and along with integrating the same in an modified IPv6 communication stack for IoT. The author proposed energy-awareness load balancing (ELB) protocol that has solved the unbalanced load in RPL i.e one node chooses preferred parent by taking into consideration not only residual energy, but also considers frequency of Parents. The second method is to use a Fast local repair (FLR) technique so as to minimize local repairs in situations which demand urgency. The hybrid approach called ELB-FLR combines the OF and load balancing of ELB, fast local repair and loop detection/avoidance of FLR into RPL. Performance evaluation includes implementation of IPv6 communication stacks for WSN on OMNET++ simulator. The experiment outcome includes (i) network layer overhead- ELB-FLR has a least percentage of overhead compared to RPL, ELB and FLR. (ii) end-to-end delay- ELB has lower delay than other protocols. (iii) Packet delivery ratio (PDR) – ELB-FLR shows better performance. (iv)Residual energy level distribution- all three protocols give better performance. The analysis considers the homogeneous network and scalar data type for data transmission.

In paper Pavković *et al.* (2011) proposed a multipath opportunistic RPL routing protocol. The reason behind this proposed work is to deliver QoS for multiple paths. Rather than using a preferred parent to forward the packet to the sink, a node will opportunistically transfer the packets through another parent as long as the route to the sink is better. The performance of PDR increases thereby reducing the overhead and energy consumption. Due to the cross-layer approach, Multipath opportunistic RPL interacts with the underlying link layer. This also utilizes link quality assessments and IEEE 802.15.4 supplies such information so that useful links are used for the creation of DAG formation. For the sake of packet delivery ratio, only nodes with high priority delay-sensitive data are forwarded through multiple paths. The 6LOWPAN adaptation layer needs to be considered to perform further analysis of the various type of data on multipath-based routing.

In the paper Iova *et al.* (2015) proposed an energy-balancing routing scheme to increase the lifetime. The purpose of using this scheme is that all paths must consume the same quantity of energy. Through the DIO message, a node has a list of all known bottlenecks, greatly increasing the existing DIO size and thus leading to overhead. The author used an Expected Lifetime metric, representing the residual time of the nodes. Existing RPL constructs a Destination Oriented Directed Acyclic Graph (DODAG) that implements a single path. The proposed method help to utilize its natural multipath design. This approach permits reducing the number of DODAG reconstructions that leads to fluctuations and convergence problems. Simulations shows the improvement in both the routing reliability and the network lifetime. In future, integration inaccuracies with respect to RPL in the metric estimation needs to be analysed.

In the work Somaa *et al.* (2017) proposed Braided Multipath RPL(MBM-RPL) to functionally help the mobility of one's node. MBM-RPL establishes an initial path established on a new routing metric that controls the expected sensor nodes' speed values. To prevent the link's expiration along the primary path, an alternate path is specified. To calculate the performance of MBM-RPL, initially accuracy of the Bayesian model using the Cooja simulator needs to be validated. MBM-RPL outperforms in terms of average transmission delay and packet loss rate compared to BMP-RPL. Further analysis with respect to realtime applications is required

In paper Khaleghnasab *et al.* (2020) most of the network's characteristics include topology dynamicity, energy constraint, and faces challenges in routing problems. To satisfy the requirements of these networks, author proposed a one of the routing methods used for utilization of multipath protocols that send data to its destination using routes with separate links. One such is RPL. So using composite metric author proposed Energy and Load aware RPL (ELaM-IoT) protocol. The proposed method has been compared with ERGID and ADRM-IoT approaches with respect to remaining energy and network lifetime.

Table 2.1: Literature Survey - RPL based on Multiple path Routing protocol

Author	**Methodology**	**Merits and Demerits**	**Observed work**
Lodhi *et al.* (2015)	Multiple path RPL used for congestion detection and Congestion mitigation	1.New protocol M-RPL supports high data rates as compared to single path RPL. 2.Should overcome unbalanced network and Path redundancy.	Future work must consider about load imbalance network.
Le *et al.* (2014)	Energy-awareness load balancing and fast local repair mechanism	1.Introduced three Multipath protocols based on RPL. 2.ELB protocol does not include link quality and FLR increases end-to-end delay wrt RPL.	Consider homogeneous network and scalar data type for data transmission.
Pavković *et al.* (2011)	Adapted cluster tree for IEEE 802.15.4 which can be coupled with RPL	1.Provide QoS using Multiple paths and improves packet delivery while minimizing overhead and energy consumption. 2.Must concentrate on high traffic networks.	The 6LoWPAN adaptation layer needs to be considered to perform further analysis of various type of data on multipath based routing.

Table 2.2: Literature Survey - RPL based on Multiple path Routing protocol

Author	**Title**	**Merits and Demerits**	**Observed work**
Iova *et al.* (2015)	Exploited Expected transmission count, denoting residual time of the nodes	1.Proposed to detect the energy-bottleneck nodes and spread the traffic uniformly among them to avoid single path. 2.Protocol overhead and maintaining the DODAG in a proposed algorithm is complex.	How RPL should integrate inaccuracies in the metric estimation is required to analyse in the future.
Somaa *et al.* (2017)	Validate accuracy of the Bayesian Model and compare it with MBM-RPL	1.Proposed framework MBM-RPL overcomes the limitation of BMP-RPL. 2.Proposed framework use more energy while maintaining alternative paths.	As a future work, MBM-RPL scheme should be tested with real applications.
Khaleghnasab *et al.* (2020)	An energy and load aware multipath routing protocol in the Internet of Things	1.Energy and Load aware RPL (ELaM-IoT) protocol has been proposed.	Improved proposed method by including composite metrics.

2.2.2 Load Balancing in RPL

One of the challenge due to resource constraint devices of IoT is Load balancing. Instead of simply saving energy randomly it is better to consume energy uniformly among the nodes. Imbalanced energy consumption may disrupt the network by Load Balancing can be performed during parent selection. Authors have used various methods to overcome imbalanced networking in a large area. The Table 2.3 and 2.4 depicts the work in the area of load balancing RPL.

The author Liu *et al.* (2013) mentioned the problem of uneven distribution of sensor nodes in large areas. In some networks, the sensor with a heavier workload leads to unbalanced workload distribution thus leading to network lifetime. The author proposed a load-balanced routing protocol based on RPL (LB-RPL) to achieve uniform load in the network. Here the node does not select the single parents, instead, the selection is based on pairwise link condition indicators. The results say that when the data collecter is at the center of the network, the workload on the node is high. But using the LB-RPL in the heavier workload node has a smaller forwarded packet when compared to RPL. Nodes that are a similar distance from the data collector have a similar workload using the proposed system when compared with RPL. The performance provides a 100% packet delivery ratio as compared with RPL.

In paper Kim *et al.* (2017) mentioned that congestion and load balancing happens under heavy traffic as packet loss increases. So the author proposed queue utilization-based RPL (QU-RPL) to perform load balancing and end-to-end packet delivery execution and compared it with the existing RPL. The proposed method is developed for each node to choose its parent node assessing the queue utilization of its neighbor nodes as well as the hop distances to the LLN border router(LBR). Based on load balancing ability, the proposed method is very useful in reducing queue losses and improving the packet delivery ratio. The experiment has been conducted on the real testbed on a multihop LLN over IEEE 802.15.4. This method lowers the queue loss to 84% and enhances the packet delivery ratio to 147% compared to the RPL.

The author Tripathi and De Oliveira (2013) defined a load imbalance metric which is applicable to any tree/hierarchy based data collection which can be applied to large scale LLN's and IoT. It requires only partial topology knowledge and works with RPL without adding extra control overhead and can also work in highly varying link condition. To minimize the variance, mean square error of load estimates the load imbalance, where higher the number of nodes in a particular rank or level of the tree, lesser will be the effect of imbalance traffic that is distributed amongst more forwarders. The simulation results achieves less variance in data traffic, low imbalance and help improve the network lifetime by considerable amount. Further analysis of the same at different levels or ranks is need to be verified.

In paper Kumar and Hariharan (2020), main intention is to address the issue of routing overhead, packet losses and load imbalance in RPL. To overcome the above problem, author proposed Dual Context-based Routing and Load Balancing in RPL based Network (DCRL-RPL). Initially ranking based grid selection process has been performed to select the optimal grid head node in each grid. The Reputation based Scheduling method has been scheduled in the grid head node in the network. For better routing performance the selected grid head categorizes the data obtained from its member using Adam Deep Neural Network (ADNN). The efficiency of the DCRL-RPL results better based on comprehensive validation.

In paper Arunachalam and Nallamothu the role of data aggregation is to assemble the collected sensor data from devices to avoid redundant data transmissions. Multipoint-to-Point generates hotspot problems and unproductive data aggregation. Due to the regular use of forwarding nodes and load imbalance network, the network layer impacts hotspot problems in RPL. The author proposed a Load Balanced RPL (LoB-RPL) protocol that uses composite metric-based parent selection. To bypass regular modifications in the DODAG structure, the proposed load balancing method determines the parent switching threshold. The author also ensures data aggregation in the IoT domain.

Table 2.3: Literature Survey - Load Balancing in RPL

Author	**Title**	**Merits and Demerits**	**Observed work**
Kim *et al.* (2017)	Tested on real test bed of a multihop LLN over IEEE 802.15.4.	1.Overcome packet loss due to congestion and load balancing problem in Routing parent selection and introduced QU-RPL. 2. Not suitable for large-scale networks.	Testbed needs to be compared with ContikiRPL and find the difference between TinyRPL and ContikiRPL.
Tripathi and De Oliveira (2013)	Applied Load imbalance metric on tree/hierarchy based data collection or data dissemination in highky varying link condition.	1.Low imbalance help to improve the network lifetime and achieve greater improvement when network is larger than the smaller one. 2.Imbalance metric needs to consider for small networks.	Required to provide similar load balance to the entire network instead of considering particular level or rank.

2.2.3 Energy Efficiency in RPL

In paper Zhao *et al.* (2016) defined traditional routing protocols that propagate through entire network to introduce reliable P2P route, which requires large amount of energy consumption. So authors proposed energy - efficient region based routing protocol (ER-RPL) which achieves energy- efficient data delivery without

Table 2.4: Literature Survey - Load Balancing in RPL

Author	**Title**	**Merits and Demerits**	**Observed work**
Liu *et al.* (2013)	Validated with workload imbalance detection and signalling and load balancing on data forwarding.	1.Proposed LB-RPL protocol where workload distribution and communication conditions are jointly considered to select optimal data forwarding paths. 2.Routing table of each node receives multiple copies of same DIO messages and provide slow recovery.	Consider nodes near sink having more load compared to other levels, the network lifetime decreases very fast as the energy of the nodes near sink decreases.
Kumar and Hariharan (2020)	DCRL-RPL: Dual context-based routing and load balancing in RPL for IoT networks	1.Proposed Dual Context-based Routing and Load Balancing in RPL based Network (DCRL-RPL).	Secure routing to further reduce the parameters exploited in RPL-based dynamic IoT network needs to be proposed.
Arunachalam and Nallamothu	Load Balancing in RPL to Avoid Hotspot Problem for Improving Data Aggregation in IoT	1. Proposes a Load Balanced RPL (LoB-RPL) protocol to avoid hotspot creation.	To achieve the performance of the RPL and data aggregation, include node capacity-related metrics in Objective functions.

compromising reliability. (i) PDR performance drops as the traffic flow increases. In RPL, root becomes the bottleneck when traffic is heavy and performance goes down. But ER-RPL still achieves an optimal value. (ii) Average hop count - in ER-RPL is 40% less than that of RPL. (iii) Routing overhead increases as the traffic flow increases. ER-RPL achieves 59% less control overhead than P2P-RPL with symmetric and asymmetric links. (iv)Energy consumption increases with the increase of P2P traffic flows. ER-RPL achieves great energy conversation compared to RPL and P2P-RPL. (v) End-to-End delay increases as the traffic flow increases. RPL suffer from longer delay than ER-RPL and P2P-RPL. This work can be extended from static networks to mobile networks in future.

The author Iova *et al.* (2014) studied that each node should consume same quantity of energy to improve the network lifetime. Expected lifetime routing metric has been introduced the time until the node will run out of energy. Author also detects energy bottleneck nodes and spread the traffic load uniformly among them using DAG structure of RPL. In expected lifetime(ELT) bottleneck node will be the first node to die. So the new node has to calculate its own traffic on the bottleneck's lifetime. Node needs to know the information about bottleneck in order to estimate ELT, which is sent along the path in a compact DIO's. Every time DIO is received, ELT of a node is repeated. Therefore each node maintains up to date information. In multipath Construction - assume that a node will send all its traffic to one single parent during preferred parent selection. Author prefer the worst case to balance more efficiently the energy consumption. After preferred parent selection, node has to compute its relative distance from the border router i.e Rank. But expected lifetime represents minimum metric along a path, so value cannot be used to compute the rank. Author proposed a constant step value to the rank of its prepared parent. Author also mentioned about load balancing where traffic is spread to all the bottlenecks. Searching a bottleneck node itself is time consuming and network lifetime needs to be considered even after detecting the bottleneck nodes.

RPL provides various metrics to guide the routing metric, one such is expected transmission count which focus on link reliability. So Kamgueu *et al.* (2013) implemented the use of nodes remaining energy for next hop selection and compare the result against ETX scheme. The proposed implementation increases the network lifetime and distributes energy evenly among nodes. But in accuracy of routing to collect the application data ETX promotes higher packet delivery ratio than proposed one. Energy and ETX has their own limitations, so needs to aim by combining both routing metric in future.

In paper Haque *et al.* (2020) mentioned that, the RPL has been standardized in IoT by IETF. Major drawbacks of RPL include network lifetime, limited power source, and reliability of the network. Different metrics have been used for the experimental results. The ETX and energy-based Objective Function have been implemented for energy efficiency and reliability. The topology includes one sink and nine senders. ETX OF is not reliable even though it is energy efficient as it takes fewer hops. Due to this, network does not take care of load balancing and link quality. For lesser hops energy OF works well but as the number of connecting devices increases, the number of hops increases.

The work of Safara *et al.* (2020) focuses on priority-based and energy-efficient routing in routing protocol for low power lossy networks (RPL) that determines routing through contents. The network uses timing patterns while sending the data to the sink node including network traffic, audio, video, and image data. Using proposed PriNergy method robustness of the routing protocol increases, and finally prevents congestion. The PriNergy technique lowers overhead, end-to-end delay and energy consumption.

Table 2.5: Literature Survey - Energy Efficiency in RPL

Author	**Title**	**Merits and Demerits**	**Observed work**
Zhao *et al.* (2016)	Makes use of region information of networks using hybrid of proactive and reactive routing protocol.	1.Introduced ER-RPL which requires a subset of nodes to do the job. 2.As traffic flow increases in a large network, energy consumption will be more and lead to load imbalance network.	Analysis can be extended from static networks to mobile networks in future.
Kamgueu *et al.* (2013)	Highlighted energy based objective function.	1.Focus on node remaining energy for next hop selection and increases the network lifetime and distributes energy evenly among nodes 1.Has low packet delivery ratio.	Energy aware scheme and ETX has their own limitations, so needs to aim by combining both routing metric in future.

Many authors have used various techniques to reduce the energy consumption of the nodes in the RPL. Based on the applications, choosing energy metric/Objective Functions is a tedious job. Using energy network lifetime of a node can be increased as well as the path towards the root node can be energy efficient. The Table 2.5 and 2.6 depicts the work in the area of energy efficiency in RPL.

2.2.4 Comparing Routing Protocols

Comparing the performance of the network helps to choose the right protocol with right metrics. So comparative analysis is important. The Table 2.7 depicts the work in the area of comparison of routing protocols.

Table 2.6: Literature Survey - Energy Efficiency in RPL

Author	Title	Merits and Demerits	Observed work
Iova *et al.* (2014)	Introduced proposed algorithm using preferred parent and load balancing.	1.New routing metric ELT has been proposed and focus on each node that should consume the same quantity of energy to improve network lifetime. 2.Testing each parent node for energy balancing would be time consuming.	Searching a bottleneck node itself is time consuming and network lifetime needs to be considered even after detecting the bottleneck nodes.
Haque *et al.* (2020)	An Energy-Efficient and Reliable RPL for IoT	1.ETX and Energy based OF have been evaluated in terms of energy-efficiency and reliability. 2. The OFs used does not assure energy efficiency and reliability at the same time.	Proposed a hybrid OF that provide load balancing with improved link quality in terms of RSSI.
Safara *et al.* (2020)	PriNergy: a priority-based energy-efficient routing method for IoT systems	1.Based on data transmission priority-based and energy-efficient routing (PriNergy) method is proposed.	Introduction to meta-heuristic algorithm is required to manage the transferring frames for routing in IoT nodes.

In paper Yi *et al.* (2013) mentioned the comparison between LOADng and RPL.

1. In data traffic flow assumption - RPL makes a-priori assumption of data traffic types and define three such pattern i.e MP2P, P2MP and P2P. But LOADng makes no assumption and provides only one general P2P mechanism.

2. In DODAG root requirement - RPL avoids single-point-of failure even if one or more router cease operation, other routers in the network should able to make global network continue to function. In LOADng no routers play a role because all routers exhibit the same behaviour.

3. In fragmentation - Applications such as AMI networks, originate small pack-

ets to avoid link-layer fragmentation. The maximum frame size is 127 bits. In storing mode, RPL increases the probability of fragmentation in downward traffic. To reduce the overhead of routing messages in LOADng, a generalized message format is considered. ROuting -related information added to the IP header is not required for LOADng.

4. Link bi-directionality - RPL operations are bi-directional links, but do not specify what mechanisms to use and how they should be used to avoid unidirectional links. In LOADng unidirectional link occurs but bi-directionality check is performed by using blacklist in loops.

5. Loops - In RPL loops are detected and fixed when data traffic is sent through network. In LOADng router share a single unique, increasing sequence number where only destination is permitted to respond to a route request, which ensures loop freedom.

The performance evaluation between LOADng and RPL presents different traffic patterns including P2P, MP2P and P2MP. In P2P scenario LOADng performs lower overhead compared to RPL and provides higher delay. But RPL has high loss rate in large scale. In MP2P scenario LOADng has higher overhead and extension of it i.e LOADng-CTP greatly reduces the overhead compared to RPL. In P2MP scenario RPL has higher overhead compared to LOADng but delay is more in LOADng than RPL. Author has compared the merits and demerits of two routing protocols for low power and lossy networks. Thus the required routing protocol needs to be selected based on the application.

In paper Dias *et al.* (2016) discussed evaluation of multi hop wireless network solution for smart grid metering in an industrial environment. It also supports TCP and UDP protocols to transfer traffic from DLMS/COSEM smart grid metering applications. Result and analysis tells that hop distance between LR and LBR where 95% of time the LRs were at a distance not higher than 4 hops. Variation of average RTT is near 50ms all time, with slight increase near the end of the test. The average ping loss ratio varies 10% and 30%. Increasing ping loss is due to material structures stored in warehouse. In duration of DLMS sessions - given the configured time outs and maximum number of DLMS retransmissions, the maximum delay of a successful DLMS session is 4s5s for UDP and 120s for TCP. In DLMS sessions failures per round will be 0.25% for TCP and 0.47% for UDP. With these results network solution are able to handle DLMS applications with requirement of low loss. Further analysis with respect to scalability of Local

Routers(LRs) and measure the power consumption of the LRs with both Control and data traffic.

The author Ee *et al.* (2010) gave information on routing header encapsulation in 6LoWPAN protocol stack. It includes dispatch header i.e new 6-bit sequence, routing header and payload. Existing 6LoWPAN routing protocols includes LOAD protocol which is a simplified version of on-demand routing protocol based on AoDV where it saves energy unlike AoDV and maximize bandwidth. Due to the increased memory and power consumption of DYMO-LOW, it cannot be used directly in 6LoWPAN routing. The proposed DYMO-Low operates on link layer instead using IP layer. Hi-Low supports increased network scalability. In routing operation, assume that every node knows its own path. A node is called a current when it receives an IPv6 packet. Suppose there is a link break in a route, Hi-Low doesn't support any recovery path mechanism as AoDV and LOAD. Limitations of existing 6LoWPAN protocols must be combined to create a standardised protocol in future.

In Paper Xie *et al.* (2014) presented the results by comparing three routing protocols such as AoDV, DYMO and RPL. Comparison was based on routing overhead, network topology change and average packet end-to-end delay. Routing overhead of RPL is higher than AoDV and DYMO because when non-conformance is detected by a network, the trickle timer will be triggered to carry on local routing repair which needs a large number of control packets. AoDV and DYMO protocol delay is higher than RPL. The delay is low as RPL needs less time to obtain the necessary path. Future work needs to compare RPL with other existing routing protocols already available for WSNs.

2.2.5 Multimodal Sensors

In paper Alvi *et al.* (2015), mentioned the recent research has been limited to scalar sensor data-based IoT systems, thus providing a void for multimedia things. An earlier version of RPL was utilized for scalar sensor data which was not practicable for multimedia things. The author observed that the increase in CO2 emissions demands green communication to reduce energy consumption and carbon footprint emissions. The main motto of the paper is to improve the RPL version for IoMT. The green-RPL routing protocol has been proposed for decreasing the carbon footprint. To calculate the performance of the proposed method, Green-RPL delivers good results for energy and delay.

The work in Kettouche *et al.* (2021) mentioned that RPL has to manage high

Table 2.7: Literature Survey - Comparing Routing protocols

Author	**Title**	**Merits and Demerits**	**Observed work**
Yi *et al.* (2013)	Comparison between RPL and LOADng protocol.	1.RPL provides different traffic pattern. LOADng is a loop free protocol and provides only P2P pattern. 2.Some mechanism must be used to avoid loop in RPL	Author has compared the merits and demerits of two routing protocols for low power and lossy networks. Based on the application, required routing protocol needs to be selected.
Ee *et al.* (2010)	Comparison between LOAD, DYMO Low and HiLow.	1.Comparison of existing 6LoWPAN routing protocols and uses HELLO messages which give higher delay in the packet routing. 2.There is a need for routing protocols that performs well in the established environment.	Limitations of existing 6LoWPAN protocols must overcome and creates a standardized protocol in future.
Dias *et al.* (2016)	Evaluation of test bed in an Industrial Environment.	1.Focus on multihop wireless networking solution. 2.IP packet loss ratio increases.	As future work needs to intend to test a network with 100 Local Router(LRs) and measure the power consumption of the LRs due to both control and data traffic.
Xie *et al.* (2014)	Performance Evaluation of RPL Routing Protocol with AODV and DYMO.	1.AODV and DYMO don't satisfy much of the requirements of LLN. Thus creation of New protocol called RPL. 2.RPL routing overhead is higher than AODV and DYMO. So measured should be taken to minimize it.	Future work needs to compare RPL with other existing routing protocols already available for WSNs.

bandwidth and powerful computation resources. So to provide sufficient bandwidth to handle high data rate applications, author extended RPL to enable disjoint multiple paths(DM-RPL). The performance has been done for real video clip transmission using FiTIoT-LAB testbed. Implementing DM-RPL has provided high bandwidth, increased PDR and less energy being consumed.

In the work Bidai (2021) mentioned the existing RPL supports the only scalar type of traffic in IoT applications. The need for huge data is called the Multimedia Internet of Things(M-IoT). RPL supporting M-IoT undergo challenges and certain requirements based on the Quality of Service (QoS) and the user's Quality of Experience (QoE). Due to the flexibility of RPL, the author proposed a multipath version of RPL(MP-RPL). The MP-RPL helps to create multiple end-to-end paths based on distinct qualities. It is useful when IoMT-based WMSN applications offer video traffic delivery and video traffic differentiation using the built paths as per priority levels. The novel work provides achievable and adequate QoS and QoE performance metrics while maintaining the RPL network for multimedia applications.

Since RPL supports scalar type of data, need for multimodal data is essential. Most of the authors concentrate on video as a multimodal data. So more work on image, audio is required. The Table 2.8 depicts the work in area of multimodal sensors.

2.2.6 Security in RPL

In paper Djedjig *et al.* (2015) described that the employed TPM (Trust Platform Module) to use trustworthiness between nodes which are not sufficient. Selfish node is also important to participate in the construction of RPL topology. To overcome this issue new trustworthiness metric has been introduced during construction and maintenance. This represents level of trust for each node and calculated selfishness, energy and honesty components. It will mention that whether a node has to trust or not the other nodes during topology creation. New metric allows node to communicate only with trusted nodes. But this is expensive in resource consumption and cannot apply to resource constrained IoT devices. To overcome this problem author introduced offload to all security computations and process into a TPM. RPL needs to analyse and evaluate efficiently with trust mechanism. Even though the selected path is secured, chances are more having longest path. Measures should be taken to have a secure shortest path in future work.

In paper Glissa *et al.* (2016) introduced new routing protocol based on RPL as secure-RPL(SRPL). This protocol prevents misbehaving nodes from maliciously changing control message values such as rank of a node that may disturb a network

Table 2.8: Literature Survey - Multimodal Sensors

Author	**Title**	**Merits and Demerits**	**Observed work**
Alvi *et al.* (2015)	Energy Efficient Green Routing Protocol for Internet of Multimedia Things	1.Proposed Green-RPL routing protocol that minimizes carbon footprints emission and energy consumption.	Despite the proposed solution consuming more energy than the default ETX, at the same time the Green-RPL transmits quite a number of packets.
Kettouche *et al.* (2021)	DM-RPL: Disjoint Multipath RPL for Bandwidth Provision in the Internet of Multimedia Things	1.Proposed multiple disjoint paths(DM-RPL) that maintains and are used by video sensors.	Improvement with multipath strategy is required to increase the probability of finding more than one path with the best quality.
Bidai (2021)	RPL Enhancement to Support Video Traffic for IoMT Applications	1.Introduced an enhanced video transport over RPL-based LLNs which is a novel solution that assists the video traffic and the multipath extension of RPL.	Need to focus on the priority level of each packet according to the frame type to improve the efficiency of the video delivery process in IoMT.

by creating a fake topology. SRPL requires authentication based on hashed values when moving through the DODAG and intervenes when changing initial values or threshold overrun, there by discarding excessive rank change requests. SRPL protocol is not suitable for all kind of attacks. Measures need to improve the performance of proposed protocol in future.

In paper Rakesh (2021) mentioned most of the Internet of Things(IoT) in reality use IPv6 routing protocol for low power and lossy networks (RPL). RPL is weak to many attacks which include password spoofing, rank attack and many more. Still work has not be achieved for high energy consumption, lack of authentication and packet loss. Inspired by these primary faults, Author has proposed the Novel Authentication and Secure Trust-based RPL Routing in Mobile sink-supported Internet of Things (SecRPL-MS). The procedure begins with registration process, followed by operating the sail fish optimization algorithm for secure routing. The SecRPL-MS provides high security outperforms 23% compared to the existing system.

In paper Ambarkar and Shekokar (2021) mentioned that the RPL protocol has an unsecured behavior existing from RFC 6550. Security concerning RPL is a challenging task as devices connected to RPL are Low power lossy networks. It is important to know the behavioral attack essential for IoT networks. The author has analyzed and proposed increased rank and decreased rank RPL attacks using ContikiOS. To prevent RPL of attacks paper describes the security model.

Table 2.9: Literature Survey - Security in RPL

Author	**Title**	**Merits and Demerits**	**Observed work**
Djedjig *et al.* (2015)	Introduced trust platform for RPL topology and objective function.	1.RPL Node trustworthiness(RNT) metric has been introduced and Trust is consider during the construction of topology. 2.Trust metric need to be used in routing.	Trusted RPL needs to analyze and evaluate effectively with trust mechanism.
Glissa *et al.* (2016)	Introduced verification phase and rank update phase in SRPL.	1.Introduced SRPL a new security scheme based on rank threshold and hash chain authentication. 2.SRPL intervention is only effective if the lost traffic is large or if the number of isolated nodes is important.	SRPL protocol is not suitable for all kind of attacks. Measures need to improve the performance of proposed protocol in future.
Rakesh (2021)	Novel Authentication and Secure Trust based RPL Routing in Mobile sink supported Internet of Things	1.Proposed the Novel Authentication and Secure Trust-based RPL Routing in Mobile sink-supported Internet of Things (SecRPL-MS).	It is intended to propose the trust-based secure routing mechanism by verifying the recommended trust received from the neighbour nodes.
Ambarkar and Shekokar (2021)	Impact Analysis of RPL Attacks on 6LoWPAN based Internet of Things network	1. Proposed the security model which will detect the attack and rectifies the network performance.	Implementation of the proposed security model and evaluation of the performance of the network.

RPL has basic security operations and has different security issues that occur at the network layer. Delivering security to IoT networks is hard, due to their constrained nature and connectivity to the unsecured Internet. The Table 2.9

depicts the work in the area of security in RPL.

2.2.7 Other Related Works in RPL

There are several related works in RPL that are listed in Table 2.10, Table 2.11, Table 2.12, Table 2.13, and Table 2.14.

Earlier RPL used to work in static networks but now Kharrufa *et al.* (2017) use dynamic networks has been introduced for different applications. Controlled reverse-trickle timer based on RSSI readings maintains high responsiveness with minimum overhead and approach the Objective function when a movement or an inconsistency is detected to help nodes to make an informed decision.By sensing RSSI values the hand-over delay is reduced by Dynamic RPL(D-RPL). Dynamic RPL(D-RPL) detects mobility or inconsistency while the proposed objective function D-OF is responsible of parent selection that aims to reduce the number of unnecessary hand-overs by comparing the calculated cost to the parent switching threshold. The combination of D-RPL and D-OF creates an optimization of these two crucial factors making it an adaptable solution for dynamic IoT applications. Dynamic techniques need to be applied for large networks.

In paper Accettura *et al.* (2011) demonstrated that RPL allows the development of advanced monitoring applications in critical conditions as it ensures very fast network set-up.Thus The total overhead incurred for RPL signalling is greater compared to the data traffic. This calls for further research and protocol optimization.Node distance from the sink give rise to Packet delays. So in any case delays are smaller than 2s, the future investigations will compare RPL regarding routing protocols already available for WSNs.

The paper Baccelli *et al.* (2011) analysed fundamental trade-offs inherent to RPL, which enables the protocol to require smaller routing state than other routing protocols. It requires sensor-to-sensor communication apart from sensor-to-sink. So reactive scheme is used to provide shorter paths on-demand, without necessarily going through the sink. Since RPL being proactive destination-initiated process is not compatible with many Home and Building automation scenarios. So reactive source-initiated process establish a sensor-to-sensor paths that are not necessarily along the DODAG. Result with respect to average route length is approximately half when using P2P-RPL on the same network. P2P-RPL also decreases traffic density near DODAG root. Needs to solve the problem of reliability.

The authors in Iova *et al.* (2016) analysed the present trends and identified the challenges that RPL must face so as to remain on the forefront of IoT technology.

1. Traffic pattern - RPL should support communication i.e P2MP, MP2P and P2P. But currently MP2P is supported by DODAG routing topology. P2P is costly because it greatly increases overhead and latency causing problems and also it creates congestion close to the root . To overcome these problems, reactive discovery of P2P routes in LLN (P2P-RPL) described in RFC 6697. Multicasting routing in P2MP communication, RPL supports only in storing mode. However RFC 7731 multicast protocol for low-power and lossy networks (MPL) has been standardized with two protocols: Trickle and plain flooding. Though MPL is highly reliable it can still have high delays and energy consumption.

2. Mobility - Routing protocol should allow the moving devices to connect to the static routing topology. To overcome this issue RPL allows a mobile node to attach as a leaf to any node belonging to the routing topology. But what is complex is the point to the multipoint communication . So as the mobile node moves from one parent to another, information spread via DAO's may quickly become out of date. Solution for this has not at been specified in any standard. Under specification also creates problem for MP2P. Currently if RPL implementation fails to detect the preferred parent of a mobile node, it becomes unreachable as it moves leading to high packet loss.

3. Resource heterogeneity - Routing protocols must considered heterogeneity devices from low end devices to high end devices such as smart watches, smart phones. But in today's scenario RPL explains two modes viz: storing and non-storing modes in order to address different resource capabilities of the network nodes. But RPL standard will not allow 2 nodes to mix in same network. In case if it exists then it has not standardized. Therefore RPL requires all devices in a network to run the same node of operation limiting heterogeneity.

4. Scalability - Different applications requires different scalability requirements. Eg: Home automation-250 devices, smart cities range from 10power2 to 10power7. Network should support upto thousand devices. But in storing mode memory available is a limiting factor to store neighbour and routing tables. In non-storing mode header is limited by 8 IPv6 address, but longer the header higher the overhead and route repair latency.

5. Reliability and robustness - Quality of radio links among devices can vary depending on urban setting due to wireless effect. While maintaining low

overhead and energy expenditure routing protocol has to react to change in connectivity by rapidly reconfiguring the topology. Eg: Home automation expected to coverage within 0.5s if no nodes have moved and within 4s otherwise. But currently trickle algorithm maintain the routing topology and reacts to connectivity changes while minimising overhead during stable condition. MP2P traffic yield reliability and good performance while the other two suffers from poor reliability.

Table 2.10: Literature Survey - Other related works in RPL

Author	**Title**	**Merits and Demerits**	**Observed work**
Kharrufa *et al.* (2017)	Used timers and new set of objective function for D-RPL.	1.Improves RPL Trickle timer and the performance of RPL Routing, also proposed new protocol D-RPL that provides higher routing efficiency and more reliable solution in both practical and simulation results. 2.Did not consider link failure during mobility.	Dynamic techniques need to be applied for large networks.
Accettura *et al.* (2011)	Consider behaviour of RPL under different conditiond like topology, overhead and packet delay.	1.RPL allows very fast network set-up and limited delays. 2.Overhead for RPL signalling is very high wrt data traffic.	Future investigations will compare RPL with respect to routing protocols already available for WSNs.
Baccelli *et al.* (2011)	Experiments carried out on a Senslab test bed with subset of 27 fixed nodes.	1.Reactive source-initiated process has been implemented instead of proactive and P2P-RPL provide shorter paths between sensors. 2.Single reply packet gets easily lost in multi-hop wireless networks.	Needs to solve the problem of reliability.

The paper Kim *et al.* (2015) presented an analysis on the performance of TCP over RPL in multi-hop LLNs. Results and analysis tells about (a) In IPv6 and link layer performance of each node - link layer ETX is very low for all nodes regardless of transport layer and traffic load.Each node is allowed to have a parent node by RPL with good link quality whether it is TCP/UDP used. (b) In number of packets dropped at the node, queue in IPv6 layer has varying arrival rate. TCP upstream experiences greater queue rate than TCP downstream because of the different RTO energy employed. (c) In end-to-end packet loss ratio - varies packet arrival rates when using UDP over RPL. At light load all nodes have negligible loss ratio. But when traffic load is increased,downstream loss ratio increases while uplink loss ratio remains low. (d) TCP re(transmission) overhead- At heavy load embedded TCP triggers end-to-end retransmissions more aggressively than Linux TCP because it does not adapt the RTO even when RTT increases significantly. Because of this reason it results in higher queue losses. (e) Achieved throughput - Even at heavy load UDP provides fair throughput for all nodes. But TCP provides lower throughput than UDP as traffic load increases. This is because TCP has extra overhead caused by ACK transmissions. Analysis must include feasible interoperation between TCP and RPL in LLNs.

Table 2.11: Literature Survey - Other related works in RPL

Author	**Title**	**Merits and Demerits**	**Observed work**
Iova *et al.* (2016)	Highlighted the behaviour of current status of each parameter required for RPL.	1.RPL supports MP2P data traffic with good performance and reliability. 2.RPL has serious scalability issues with P2MP traffic when configured in Storing mode.	P2MP and P2P communication received significantly less attention in RPL. Should also concentrate on resource constrained devices.
Kim *et al.* (2015)	Consider test bed network for the performance of TCP over RPL in an embedded IPv6 based LLN running over a 30-node multihop IEEE 802.25.4.	1.Link layer ETX is low for all nodes regardless of transport protocol and traffic load. 2.TCP achieves lower throughput than UDP as traffic load increases.	Analysis must include feasible interoperation between TCP and RPL in LLNs.

In paper Iova *et al.* (2017)bhighlighted that RPL simply forms a routing topology without prior knowledge about the topology created/formed at MAC layer. The overall performance of the routing protocol is hence impacted. So as to solve the above problem, this paper imposes the need for intermediate layer between MAC and Network layer. Drawback of star and Peer-to-peer topology introduced cluster tree topology. In medium access layer - accessing medium can be either in beacon-less or beacon mode.

1. Evaluation with respect to topology control tells that when a node chooses to communicate, decision made by MAC and routing layer might conflict. This results in network performance and recommends that MAC protocol only filters out bad links.

2. Evaluation with respect to routing topology dynamics says that the node has to reset trickle timer and generate more DIOs and energy consumption when it changes its parent frequently. One option is to reduce parent changes of MAC neighbours but this also limits routing diversity. But author recommends WMEWMA (Window mean with exponentially weighted moving average) - this provides highest performance.

3. Evaluation with respect to estimating link quality - In order to estimate the link quality with neighbour there are two approaches (i) Passive - Estimating link quality is done only for the neighbours when the node communicates with. (ii) Active - A node can send probe packets with extra overhead. In RPL, a node is communicated only with the preferred parent, so there is no way to estimate link quality with other neighbours. But RPL don't specify forwarding rule. Author recommends a node to use parents in the parent list to route packets to root.

4. Evaluation with respect to computing ETX- ETX of a link is explained as 1/PDR. PDR is the ratio between the number of ACKS received and the number of packets sent. Both Tinyos and Contiki compute ETX by counting the number retransmission, by not considering the packets dropped by MAC layer.

Author also mentioned detailed description of IEEE 802.15.4e TSCH and IETF 6TiSCH. The drawback of IEEE 802.15.4e TSCH mention standardization gap exists between IEEE 802.15.4e link layer standard and upper layer standards such as 6LowPAN. But IETF 6TiSCH standardization working group define mechanisms to manage TSCH communication schedule. Both centralized and distributed schedule management are supported by 6TiSCH. Results mention that peer-to-peer provides high performance than cluster-DAG topology. There is a need for mechanism so as to modify the schedule on-the-fly in a distributed fashion.

Table 2.12: Literature Survey - Other related works in RPL

Author	Title	Merits and Demerits	Observed work
Iova *et al.* (2017)	Introduced a new intermediate layer between IEEE802.15.4 and RPL.	1.Introduced 6TiSCH and supports both centralized and decentralized approach. 2.6TiSCH does not define the policy.	Need mechanism to modify schedule on-the-fly in a distributed fashion.
Khelifi *et al.* (2015)	Implemented with cooja simulator over contiki OS to reduce packet loss, energy consumption and increase lifetime.	1.Pro-RPL has been designed to predict failures before they occur and presents a scalable and energy efficient protocol. 2.Predicting a failure will not guarantee the right decision.	Needs to investigate in real time statistics.
Tripathi *et al.* (2010)	A real outdoor network was reproduced in simulation with the help of topology and link quality data.	1.Mention how trickle timer is useful in RPL. 2.Needs to concentrate on Routing table size and loss of connectivity.	Observation includes protocol operation needs to be modified for outdoor network.

The authors Xiao *et al.* (2014) mentioned about object function zero (OF0) for which minimum hop count is the basis and (MROF) minimum rank with hysteresis objective function based on ETX. As network size increases both OF0 and MROF will introduce long single hop which will lead to routing bottleneck that resists the entire network. Author introduced new routing metric PER-HOP ETX used to distribute ETX value to each node along the route. Results and analysis was done on Cooja, a comparison between new OF0 and original MROF. (i) Network latency - as the number of nodes increases in the network, PER-HOP-ETX can prevent delay. (ii) PDR - performance remains same for average hop which is small but PER-HOP ETX is slightly better than ETX. Therefore it is efficient. (iii) Energy consumption-When the network expands the total consumption of energy is less and when the network is small PER-HOP ETX may consume more energy. In future,in order to achieve greater optimisation for certain application there is a need to concentrate on dynamic topology structure with a proper evaluation metric capturing network latency or energy consumption changes.

Lack of proper broadcast mechanism needs to be identified. Authors in Clausen

Table 2.13: Literature Survey - Other related works in RPL

Author	Title	Merits and Demerits	Observed work
Kiraly *et al.* (2015)	Implemented the D-RPL using Cooja emulation over different synthetic toplologies.	1.D-RPL new mechanism overcomes scalability limitation and supports RPL networks with multiple roots. 1.Decrease in PDR with scale.	Further analysis is required to analyse how protocol works under higher traffic loads.
Xiao *et al.* (2014)	Implemented the new metric based on Contiki.	1.New metric PER-HOP ETX has been introduced and overcomes the drawback of long single hop when network size increases. 1.PER-HOP ETX consumes more energy and delay for small networks.	Need to concentrate on dynamic changing topology structure with a proper evaluation metric capturing network latency or energy consumption changes and achieve greater optimization for certain application.
Clausen and Herberg (2010)	Introduced hypothesis for data broadcasting in RPL	1.Classical flooding was a solution, due to lot of duplicate transmissions a new flooding mechanism called MPR-based broadcast mechanism has been discovered with lowest delay 2.Protocols are just addons to the existing RPL specification.	There is a necessity of making a standardized protocol for broadcasting.

and Herberg (2010) suggested two broadcast mechanism aiming at exploiting the existing routing state of RPL and requiring no additional state maintenance. For network-wide broadcast, the assumption is that broadcast is sent to the root using unicast, from where the root will launch the broadcast operation. In Parent Flooding(PF) broadcast operation is launched from DODAG root. To make sure that no router will forward a broadcast packet more than once, Preferred Parent Flooding(PPF) utilizes the existing relationship between RPL routers. Simulation results mention that collision ratio of the DIO messages is low.

1. In Unicast Data Traffic PDR is very high. Delay of the data transmission in-

creases due to longer path length. Average path length grows logarithmically with the number of nodes.

2. In Multicast Data Traffic due to redundancy of transmissions- PF has highest packet delivery ratio than PPF. The overhead is much lesser for PPF than for PF.

Future investigation says that there is a necessity of making a standardized protocol for broadcasting.

Kiraly *et al.* (2015) introduced D-RPL to overcome the scalability limitation by mending storing mode forwarding with multicast-based dissemination and they are used only when the limits of memory are reached. Root behaviour for each packet, the root first checks its routing table for normal IP forwarding. If there is no route entry for the destination address, instead of dropping the packet, the root forwards it to the D-RPL multicast channel. A junction node enables the delivery of packets from the root to all the destinations in its routing table, even those for which it received a DAO-NACK. D-RPL can make the network operate at scales where ContikiRPL would fail and does not alter performance in the conditions when ContikiRPL works. Further analysis is required to analyse how protocol works under higher traffic loads.

The work in paper Khelifi *et al.* (2015) highlighted about maintenance of all routing protocols. To enable the network to selectively predict and mitigate failures before they influence and affect network connectivity, author has designed and implemented proactive RPL (Pro-RPL) maintenance scheme. One of the most important characteristics of all routing protocols is repairing failures. But RPL has two mechanisms for repair - local and global repair. Single DODAG with one sink and varying number of nodes forms the topology of RPL. Each node will collect information of its current parent list and ETX. ETX mention the quality of links to the parent node. The proposed algorithm provide rapid discovery and migration to alter parent to replace the dead/failure parent (suffering parent). The failure node hinges on cost condition of its link to its parent, energy of its battery and aggregated cost on the path towards root. These parameters which are received from neighbouring nodes are obtained from DODAG information object (DIO) messages. Threshold is computed for the first time when topology is constructed with the motive of reducing the energy consumption and exchange messages. Results include packet loss, average energy consumption and lifetime of the network. Pro-RPL provides better results for the packet loss than RPL and Pro-RPL lifetime network is higher than RPL. Regarding Pro- RPL lifetime network as the size of the network increases it provides better results. Future analysis needs to investigate in real time statistics.

In the paper Tripathi *et al.* (2010) provides several routing metrics and performance metrics of RPL used discrete event simulator in real-life deployment scenarios. Simulation results in comparing RPL with shortest path routing. The performance of the number of Hops will be better only when sink/root is in the middle of the network. Total ETX along the path from all source to all destination remains same for both the protocols. In order to reduce the number of control plane packets, RPL makes use of trickle timer and eliminates redundant messages. Loss of connectivity, RPL has two mechanism for DAG repairs i.e Local and Global repairs. Observation includes protocol operation that needs modification for outdoor network.

In the paper (Taghizadeh *et al.*, 2020) mentioned that the under heavy traffic, RPL features high packet loss rate and decreased network lifetime during operation in IoT. To overwhelm the RPL constraint, the author proposed an Anycast Routing(EM-RPL) where the source node targets a set of destinations rather than a single one. During the simulation, unique rank computation and parent selection mechanism has been proposed different than the existing one. EM-RPL results in reduced environmental footprint of the network, achieves few QoS too.

In the paper Bouakouk *et al.* (2021) describe the standard routing protocol named RPL is designed mainly for LLNs. To exchange and make use of information in RPL, DUAL-MOP RPL has been developed. It helps the nodes of diff modes of operation(MOPs) to operate in the same network. To resolve long source header problem in DUAL-MOP RPL, a great quantity of source routing operations are executed which leads to a high processing load. To handle the above issue, the author proposed the extension of DUAL-MOP RPL called ODM-RPL(Optimized DUAL-MOP RPL). It trade-offs between the source routing header length and the storing nodes processing load by first optimizing the source routing header. Later introduces a concept of preferred source routing header maximum length. The simulation results better with the proposed method.

In the paper Estepa *et al.* (2021) reduces energy consumption in WSN based on IEEE 802.15.4 IoT devices with transmit power have proposed a novel cross-layer scheme. The method adopts RPL and nodes locate the neighbors. Based on this, they preserve fresh link statistics for each known transmit power. Later utilized the product of ETX and local transmit power as a single metric. Now each node chooses the parent node that minimizes the energy for packet transmission which goes with the root and optimizes local transmit power to be utilized. The implementation has been done on Contiki-NG using Z1 mote and two transmit power levels have been considered. The performance of the simulation says that there was a 25% energy reduction in transmission and reception of packets when compared to the existing RPL. However, the proposed process is much suited for a large network.

Table 2.14: Literature Survey - Other related works in RPL

Author	**Title**	**Merits and Demerits**	**Observed work**
Taghizadeh *et al.* (2020)	EM-RPL: Enhanced RPL for Multigateway Internet-of-Things Environments	1.EM-RPL protocol was proposed, in which it routes to one-in-a-set instead of a single destination 2. No guarantee when the same level of lifetime improves when used in large scale networks.	In the small scale network, the proposed method outperforms PDR, network lifetime and energy consumption when compared to RPL.
Bouakouk *et al.* (2021)	ODM-RPL: Optimized Dual MOP RPL	1.Introduced an optimized version of DUAL-MOP RPL, called ODM-RPL. 2. simulation doesn't take into account link failures.	Simulations and tests need to be conducted by considering mobile nodes instead of static sensors.
Estepa *et al.* (2021)	RPL Cross-Layer Scheme for IEEE 802.15.4 IoT Devices With Adjustable Transmit Power	1.Novel scheme for improving energy efficiency in IEEE 802.15.4 IoT devices with adjustable transmission power levels. 2. OF considers a single metric that may not be suited for some applications.	An extension to multiple power levels (More than 2)

2.3 Outcome of Literature Survey

A discussion point with using IPv6 over a link technology is around the area of broadcast domains and how to support them. There is a need for a routing protocol at the link layer to emulate broadcast domains. This is called "mesh under" as a fully connected network is emulated under a multi-hop mesh topology. But there are no mesh-under routing protocols defined by the IETF for 6LoWPAN networks.

The IETF (Winter, 2012) has defined a "route-over" architecture which implements the routing functionality at the network layer. In the route-over architecture the extent of an IPv6 link is a single link transmission i.e., immediate neighbors (e.g. radio range on wireless links). But RPL has several issues that must be overcome for it to be deployed more commonly in 6LoWPAN networks.

1. In Multiple Path Routing, the nodes/links within each route are different. Thus failure on a given path does not affect any other path. But maintaining all alternative paths requires a global knowledge of the network topology, thus resulting in a high energy consumption level.

2. In Load Balancing, various works have been achieved with respect to improving network lifetime, energy efficiency, maximizing the packet delivery ratio and and different load balancing techniques. But these parameter needs to improve a lot to make it more load balancing.

3. In Energy Efficiency, authors have worked to improve network lifetime as well as routing reliability. Still research is going on to make 100% energy efficient for a particular network.

4. 6LowPAN is designed for IPv6 over IEEE 802.15.4. Frame size and address sizes are primary issues even though Header compression is the key mechanism. Low-Power and Lossy Networks (LLN) Routers have constraints on processing, memory and energy, as a result the existing protocols are not suitable for multi-modal sensor nodes.

5. However routing protocols are vulnerable to many attacks. Security must be provided to both small and large networks. Trust metric should also be considered for routing protocols. Attacks targeting RPL networks require to be identified and prioritized according to their consequences in order to design efficient security solutions.

6. Other related networks include how to optimize the network, how broadcasting is necessary, or how a network maintenance needs to perform to get the best routing protocol.

7. Multimodal data communication: The focus of RPL thus far have been more on networks with scalar sensor nodes. Networks, that do not have a very strong bandwidth and latency requirement. Thus, the current design

paradigms in RPL do not scale well for a network with multimodal sensors. A network with such sensors have higher bandwidth and strict QoS requirements. In it's current state, RPL does not perform well for a network with such requirements. There is a need to improve the performance of RPL for multimodal sensor networks.

Chapter 3

Proposed HEE_OF for Image Data Transmission

Multimedia applications such as surveillance system, smart home system, smart vehicle communication system, disaster management systems, smart agriculture, and smart traffic systems in smart city etc., requires low cost devices with effective communication. Wireless sensor networks (WSN) (Kocakulak and Butun, 2017) has advantage of id based self configurable network. The nodes can be deployed statically or randomly. However, the Wireless sensor network is delay tolerant, battery operated and dynamic network. Addressing nodes with IP based communication and transfer of images or multimedia data over such large network requires sufficient added extra features to WSN with respect to QoS and latency.

The IEEE standard 802.15.4 (Kivinen and Kinney, 2017) support Wireless Personal Area Networks (WPAN) with ID based communication. Even though the standard supports Guaranteed Time Slots (GTS), further experiments on multimedia transmission over larger network is required.

The IEEE standard 802.15.3 (Gilb, 2004) supports multimedia communication. But the standard is mainly designed for the applications such as connecting digital still cameras to printers or kiosks, laptop to projector connection, Video distribution from a set-up box or cable modem, Video camera display on a television etc., which indicates the high data rate WPAN for a short range. The requirement of applications like disaster management and vehicular network with low power devices with multi modal data needs network with larger communication range in terms of multihop communication or wide range of communication for each node in the network.

6LoWPAN (Kushalnagar *et al.*, 2007*b*), (Al-Fuqaha *et al.*, 2015) provides higher layers for wireless communications for IoT and M2M. This provides IP based communication over low power lossy networks such as IEEE standard 802.15.4, which can extend the network for connecting different WPANs. However, the network is designed for delay tolerant, scalar type of sensor data communication. Behaviour of the network with respect to multi modal data communication and challenges with respect to same for the applications such as disaster management, vehicular management, smart agriculture, smart city applications with multimodal sensors yet to be analysed. Hence, the 6LoWPAN network is considered for these IoT applications.

6LoWPAN supports with Objective Functions (OF) for supporting routing, header compression and fragmentation to reduce the number of bits in IPv6 header, so that the packet can be transmitted over IEEE 802.15.4 MAC which has limitation of 127 bytes. A new hybrid OF is proposed after analysing the performance of OFs with respect to image transmission.

3.1 Related Work

The IoT has the ability to interconnect readable, recognizable, addressable, and controllable objects via Internet. In sensor networks IP connectivity mainly relies on two IETF standards: 6LoWPAN and RPL. 6LoWPAN is an acronym for IPV6 over Low Power Personal Area Networks.The IETF 6LoWPAN working group addressed the challenge of enabling wireless IPv6 communication over the newly standardized IEEE 802.15.4 low-power radio for devices with limited space, power and memory, such as sensor nodes.

6LoWPAN (Olsson, 2014) provides a WSN node with IP communication capabilities. It puts an adaptation layer above the IEEE 802.15.4 link layer and provides the ability of TCP/IP communication above the adaptation layer. The adaptation layer is necessary because stacking IP and above layers may not fit within one IEEE 802.15.4 frame.

3.1.1 Fragmentation and Reassembly in 6LoWPAN

The paper Awwad *et al.* (2013) presented about compression scheme for second and subsequent fragment headers for IPv6 header in 6LoWPAN Network. The overlap of network headers between the first and subsequent fragments is used in the developing the scheme. The headers which become redundant after transmission of the first fragment are not encoded in the following fragments. Second and

Subsequent Fragments Headers Compression Scheme (S&SFHC) can be used as a standalone compression technique or can be combined with other compression techniques. The results show the performance of S&SFHC is better than that of LOWPAN_IPHC.

In the paper Watteyne *et al.* (2010) presents the results of experiments with multi-hop transmission of video streams over a IEEE802.15.4 based network. A video is essentially a technology of capturing a sequence of still images. As the order in which these still images are presented to the application layer are important, it is essential for the transport layer to be able to handle out of order transmissions and reorder them before handing it out to the higher layers. In addition to the transport layer protocols, it is also important for the MAC layer to be able to allocate resources based on the requirements of the transport and application layers. The experiments show an inter-frame compression scheme yields better results in comparison to intra-frame compression. This primarily due to the fact that video streams are mostly static data with bursts of changes in each frame. So a scheme to identify and compress just the changes in each frame and transmitting that over the network would conserve bandwidth and also bring down the delays in transmissions of video streams.

The paper Hasbollah *et al.* (2009) describes the implementation of a gateway that interfaces between 6LoWPAN sensor network and IPv6. The performance of the gateway that acts as a bridge between the IEEE802.15.4 and wired IPv6 networks is measured by transmitting packets of varying sizes. The gateway uses two interfaces, one facing the external world and the other one facing the 6LoWPAN wireless sensor network. The gateway is responsible for performing compression and decompression operations on the IP headers to tunnel packets between the 6LoWPAN networks with a MTU of 128 bytes and the external world with MTU much larger than 128 bytes.

The Industrial Internet of Things (IIOT) in paper Bruniaux *et al.* (2021) provides directions to reliability in wireless connectivity. 6LoWPAN adaptation layer was presented to address its payload size limitations. However, the method does not support low link quality, hence the Forward Error Correction(FEC) and Network Coding FFC(NCFEC). NCFEC works well when high reliability is required and only low-quality links are available.

In the paper Tanaka *et al.* (2019) there is always a need to combine low-power wireless networks with IP-enabled networks. As such 6LoWPAN provides this facility. The main challenge is that the IPv6 packet does not fit in the link-layer frame. So fragmentation came into existence as one of the features of 6LoWPAN.

Usually, the IPv6 packet is fragmented and reassembled at every hop. Due to every hop, reassembly causes low end-to-end reliability and high latency. Considering the new implementation method results in 100% reliability, latency to half, and memory requirement comes down to 160B.

As the MTU of IEEE 802.15.4 MAC has a limitation for packet transmission of 127 Bytes and IPv6 has 1280 bytes, for the smooth transmission between these, 6LoWPAN has come to an existence that offers header compression, fragmentation and reassembly and routing.

3.1.2 Image Transmission

The paper Pham *et al.* (2013) identified the limitations in determining the performance of transmitting still images using sensor board hardware and 802.15.4 radio on a network with multiple hops. A latency in the order of 3 seconds is possible for an 128x128 image with the use of an optimized encoding scheme for images. This can satisfy the requirements of an example, an intrusion detection application. The latency increases to 7 seconds for a an image of size 200x200 and quality factor of 20 which is required instances such as situation awareness application.

The paper Pekhteryev *et al.* (2005) mentions the use of an image sensor based network platform that is developed to test the transmission of images over multi-hop ZigBee networks. The ZigBee is a technology used in the IEEE 802.15.4 MAC and PHY layers for short range communications that supports low data rates and requires low power for operations. The ZigBee networking (NWK) and IEEE 802.15.4 MAC layer protocols are implemented on a single M16C microprocessor. ZigBee NWK does support fragmentation and relies on the transport layer to provide the fragmentation service in the network. The best effort multi-hop transmission of JPEG and JPEG-2000 images are tested as the multiple access scheme is CSMA/CA.

The paper Adarsh *et al.* (2016) presents a scheme to use IoT devices running over 6LoWPAN based networks for designing a real time sericulture monitoring and disinfection actuating system that identifies the different stages in the life cycle of a silk worm using an image processing technology. The prototype is built with the TelosB motes capable of running the 6LoWPAN stack. These motes carry temperature and humidity sensors with an disinfection actuation system and a serial camera. The camera captures pictures that are transmitted over the 6LoWPAN network to analyse and determine the status of the sericulture process.

In the paper Li *et al.* (2019) mention issues with resource constraints of sensor nodes that use the symmetric algorithm for image encryption/decryption, which is used for WSN and the security of data transmission. The author has proposed a new image communication system for IoT and mentioned a compressed sensing model and corresponding parallel reconstruction algorithm. Implementation considers time and resource efficiency. For large-scale images, high flexibility has been examined in numerical experiments.

RPL is known for transmitting scalar data type, need for multimodal sensors are required that includes image, audio, video and many more. Few authors have considered image as multimodal data for IoT applications.

3.1.3 Objective Functions in RPL

6LoWPAN is a new and upcoming technology which implements a WSN using IPv6 addresses for sensors. 6LoWPAN networks generally use Routing Protocol for Low-power-loosy (RPL) as the preferred routing protocol. RPL uses an objective function to determine the best path to reach the root of the DODAG based network. There are two popular objective functions defined in RPL, Hysteresis Objective Function (MRHOF) and Objective Function Zero (OFO). Pradeska *et al.* (2016) focuses on the performance analysis of these two objective functions using COOJA as a WSN simulator. The research measures performance in the areas of network convergance time, latency, packet deliver ratio (PDR) and power consumption using different values of parameters such as hop count and ETX running various simulations. The author concludes MRHOF performs better than OF0 in terms of network quality based on the results of the simulation. MRHOF is determined to be preferable in sensor networks that require a reliable data delivery ration while OF0 is deemed preferable when there is a need for a fast forming sensor network with low power consumption.

In the paper Xiao *et al.* (2014), mentioned object function zero (OF0) for which minimum hop count is the basis and (MROF) minimum rank with hysteresis objective function based on ETX. As network size increases both OF0 and MROF will introduce long single hop which will lead to routing bottleneck that resists the entire network. Author introduced new routing metric PER-HOP ETX used to distribute ETX value to each node along the route. Results and analysis was done on Cooja, a comparison between new OF0 and original MROF. (i) Network latency - as the number of nodes increases in the network, PER-HOP-ETX can prevent delay. (ii) PDR - performance remains same for average hop which is small but PER-HOP ETX is slightly better than ETX. Therefore it is efficient. (iii) Energy consumption-When the network expands the total consumption of energy is less and when the network is small PER-HOP ETX may consume more energy . In future,in order to achieve greater optimisation for certain application there is a need to concentrate on dynamic topology structure with a proper evaluation metric capturing network latency or energy consumption changes.

In the paper Lamaazi and Benamar (2017) described objective function (OF) to choose the optimal route towards destination. Objective Function can operate according to a set of metrics and constraints used in a single or combined way. The use of a single metric in the OF can improve routing performances while degrades others. To overcome these limitations, author mentioned a new approach to enhance the RPL routing protocol. Author proposed OF-EC (objective function based combined metric using fuzzy logic method), a new objective function that considers both link and node metrics, namely ETX (expected transmission count), HC (hop count) and EC (energy consumption) based on fuzzy logic concepts. The results show that the new OF-EC in comparison to the OF based ETX and OF based energy consumption only and OF_FUZZY allows improving RPL performances in terms of PDR and overhead. In addition, this new metric allows equalizing the energy consumption of nodes throughout the network.

In the paper Kechiche *et al.* (2017) considered Smart Grid (SG) as an innovative concept that aims to implement a communication infrastructure for data exchange between the various entities connected to these networks. In this case, Wireless Sensor Networks (WSNs) have recently been considered as a promoting communication technology for SG applications. However, problems such as noise, interference and fading in SG environments, make reliable and energy-efficient multi-hop routing a challenging task for traditional WSNs routing protocols. Thus, IETF has proposed an IPv6 based routing protocol working under stringent low power and low-cost constraints. This Routing Protocol for Low power and Lossy Network (RPL), selects the ideal routes from a source to a destination node based on certain metrics injected into what is called an Objective Function (OF). In this work, author investigate basics OFs namely Objective Function zero (OF0) and Hysteresis Objective Function (MRHOF). Author also study the most influential parameters on the performance using Contiki COOJA simulator and then evaluate the RPL performance in terms of latency, packet delivery ratio, control overhead and supported throughput. The simulation results revealed that these parameters have a great impact and indicated that the performance of RPL within high density networks for OF0 can provide a better RPL behavior than MRHOF.

In the paper Eloudrhiri Hassani *et al.* (2021) proposed a new Objective Function called IRH-OF based on a combined metric for rank calculation. The proposed Objective Function results better when compared with the existing Objective Function in the ContikiOS. The proposal allows selecting the best parent among all the candidate parents based on defined metric cmIRH that combine the strength signal indicator and hop count along the path with an additive approach. The result shows better PDR, reduced latency, and power consumption.

In the paper Moradi and Javidan (2020) a new Objective Function called Time OF(T-OF) has been proposed that achieves the balance between the energy nodes to improve network lifetime. A new metric named NOCS has been introduced to select the parent that has a minimum value of the number of children and siblings. This new OF has been compared with MRHOF, OF0, and EN-OF. The proposed OF gives better results with respect to PDR, energy balancing and improves network lifetime.

Most of the authors have used one or two metrics for better results and concentrated on homogeneous network for analysis of their proposed methods. There is need for considering combined metric to reduce QoS in the heterogeneous network with respect to sensor data.

The following are the research gaps related to literature survey.

1. The analysis of Multimodal data over 6LoWPAN with IPv6 is required.

2. Objective Function for Multimodal communication in 6LoWPAN is not yet defined and needs further research.

3.2 Factors Influencing Data Transmission in IPv6 based 6LoWPAN for Image Data Transmission

The IPv6 protocol is used as the network layer protocol in 6LoWPAN. Since the IPv6 network layer's Maximum Transmission Unit (MTU) is not compatible with the MAC layer of IEEE 802.15.4, an adaptation layer is introduced between the network and MAC layers. It performs fragmentation, reassembling, IPv6 header compression, and addressing mechanism to enable compatibility. Therefore the development of 6LoWPAN provides IP communication capability to nodes in WSN, thereby enabling connectivity with other IP based networks. This eliminates the use of gateways in the network and hence reduces the delay involved in data forwarding. Further the type of sensor data transmission also matters for performance in communication.

Suppose if we want to transfer data from one node to another such as video or audio, then we need a system to convert into visual format. So such simulator is required to do the task.

3.2.1 Need for Adaptation Layer

The 802.15.4 defines Maximum Transmission Unit (MTU) 127 bytes while IPv6 requires the link layer to support 1280 bytes packets. As shown in Figure 3.1, the maximum 802.15.4 frame overhead is 25 bytes, resulting in the maximum frame size at MAC layer is 102 bytes. After imposing 21 bytes link layer security header, there leaves only 81 bytes space for IP packets. Besides, with 40 bytes IPv6 header and 8 bytes User Datagram Protocol (UDP) header, only 33 bytes are available for upper-layer data (Huiqin and Yongqiang, 2010). The transmission efficiency for the upper layer data is less than 26%. Packet fragmentation and header compression is thus necessary for LoWPAN to reduce header overhead and save space for upper-layer data.

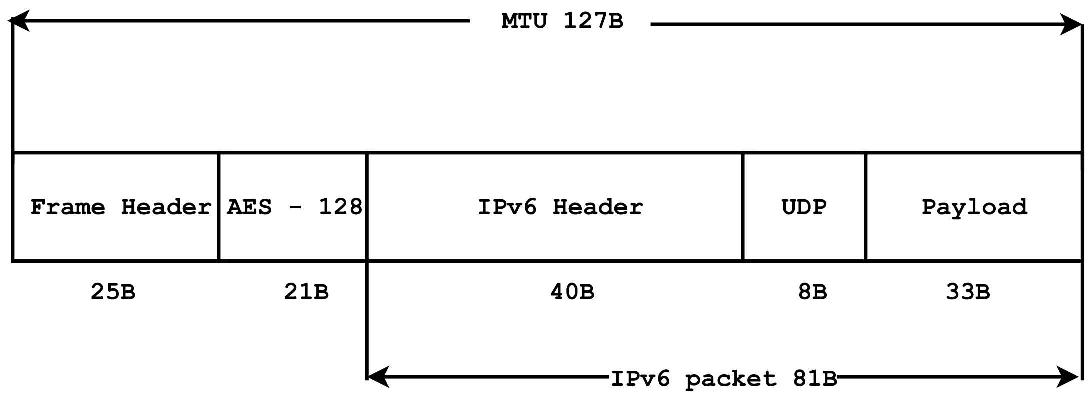


Figure 3.1: IEEE 802.15.4 Frame (Huiqin and Yongqiang, 2010)

In order to smoothly transmit data packet between IPv6 and 802.15.4 networks, IETF 6LoWPAN working group proposes an adaptation layer between 802.15.4 MAC layer and IPv6 layer. The adaptation layer is the main component of 6LoWPAN. The 6LoWPAN adaptation layer uses stateless compression which compresses the overlapping values of adaptation, network and transport layer header fields to a few bytes (Hasbollah *et al.*, 2009). Three main functions of the adaptation layer are header compression, fragmentation and layer-2 forwarding.

The major function of this layer is the TCP/IP header compression. The IEEE 802.15.4 frame has a maximum packet size of 128 bytes, whereas IPv6 header size is 40 bytes, User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) header sizes are both 4 bytes, fragmentation header adds another 5 bytes overhead. However, without compression, it is not possible to transmit any payload effectively.

A second major function of the adaptation layer is to handle packet fragmentation and reassembling. IEEE 802.15.4 has a maximum frame size of 128 bytes, while IPv6 requires a maximum transmission unit (MTU) of 1280 bytes. This mismatch is handled in the adaptation layer.

The third major function of the adaptation layer is routing. Routing is the ability to send a data packet from one device to another device, sometimes over multihops.

Depending on what layer the routing mechanism is located, two categories of routing are defined: Mesh-Under(Link-Layer) or Route-Over(Network Layer).

1. Mesh-Under : The network layer does not perform any IP routing inside a LoWPAN. The adaptation layer performs the mesh routing and forwards packets to the destination over multiple radio hops.

2. Route-Over : All routing decisions are taken in the network layer where each node acts as an IP router. In route-over, each link layer hop is an IP hop.

3.2.2 IPv6 Header Compression in 6LoWPAN

The reason for IP Header Compression (Shacham *et al.*, 2001) is to compress the common values present in headers before transmitting them on link and later uncompressed to their original state during reception. Three standard compression techniques has been proposed so far in ContikiOS.

3.2.2.1 LOWPAN_HC1

Figure 3.2 shows the LoWPAN_HC1 encoding technique proposed for 6LoWPAN. All fields in IPv6 format can be compressed except the hop limit, which needs to be carried inline. Therefore the compressed header results in 16 Bits (Header(8)+ Dispatch header(8)) instead of 40 Bytes of the uncompressed header. However it does not efficiently compress header when communicating outside of link-local scope or when using multicast.

LoWPAN_HC1 Dispatch Header (8)	SA (2)	DA (2)	TF (1)	NH (2)	HC2 (1)

Figure 3.2: LoWPAN_HC1 Encoding [RFC 4944] (Montenegro *et al.*, 2007)

1. IP Version : 6 for all packets.
2. Traffic class and Flow label : All zero.
3. Payload Length : Inferred either from Link-layer or the Fragment header.
4. Next Header : 2 bits to indicate TCP, UDP and ICMP.
5. Source and Destination Address : They are Link-local.

3.2.2.2 LOWPAN_HC2

LOWPAN_HC2 as shown in Figure 3.3, only defines the compression of UDP header. The UDP Length field can be compressed and inferred from IPv6 header. The source or destination port can be reduced to 4 bits if it is based on 0xF0B0. The full port is calculated by 0xF0B0 plus the 4 bits compressed port value.

S_Port (1)	D_Port (1)	Length (1)	Reserved (5)

Figure 3.3: LoWPAN_HC2 Encoding for UDP [RFC 4944] (Montenegro *et al.*, 2007)

For multicast and global communication, it has to carry the full 128bits address. In addition, it uses 2 bits to define the next header type and LOWPAN_HC2 can only compress UDP, TCP and ICMP which has poor extensibility. If there is extension header between IP and UDP, UDP header can't be compressed, as the compressed headers must be consecutive.

3.2.2.3 LOWPAN_HC1g

It is an extension of LOWPAN_HC1. It is modeled to compress IPv6 global addresses as shown in Figure 3.4. When source or destination address matches the default one, it can be compressed (Hui and Culler, 2007).

SC (2)	DC (2)	VTF (1)	NH (2)	L4C (1)

Figure 3.4: LoWPAN_HC1g Encoding [RFC 4944] (Montenegro *et al.*, 2007)

1. SC: IPv6 source address compression.
2. DC: IPv6 destination address compression.
3. VTF: Version, Traffic Class, and Flow Label.
   (a) 0 - Full 4 bits for Version, 8 bits for Traffic Class, and 20 bits for Flow Label are carried in-line.
   (b) 1 - Version, Traffic Class, and Flow Label are elided and assumed to be zero.
4. NH: Next Header field carried in-line which can be UDP, ICMP or TCP.
   (a) 00 - Next header field carried in-line.
   (b) 01 - UDP
   (c) 10 - ICMP
   (d) 11 - TCP
5. L4C: Layer 4 Compression
   (a) 0 - Full layer 4 header is carried in-line. An HC2 encoding does not precede the layer 4 header.
   (b) 1 - Layer 4 header is compressed. An HC2 encoding follows the IP header but precedes the layer 4 header. Currently, this indicator only supports UDP compression.

LoWPAN_HC1g can compress global unicast address when communicate intra-6LoWPAN. But when devices communicate with external 6LoWPAN or internet, the full address must be carried in line. Furthermore, the multicast address can't be compressed yet by LOWPAN_HC1g.

3.2.2.4 LOWPAN_IPHC

It is used to compress the link-local and global unicast addresses as shown in Figure 3.5.

011 (3)	TF (2)	NH (1)	HLIM (2)	CID (1)	SAC (1)	SAM (2)	M (1)	DAC (1)	DAM (2)

Figure 3.5: LoWPAN_IPHC Encoding [RFC 4944] (Montenegro *et al.*, 2007)

1. 011: 3 bit Dispatch Code
2. TF: Traffic class and Flow label
3. NH: Next Header uses LowPAN_NHC
4. HLIM: Hop limit
   - if 1: compress, encoding is 01
   - if 64: compress, encoding is 10
   - if 255: compress, encoding is 11
   - else do not compress
5. CID: Context Identifier Extension. Present when communicating with global address.
   - 0 = Default
   - 1 = Adds source context and Destination Context.
6. SAC / DAC: Source Address Compression and Destination Address Compression
   - 0 - Stateless Compression
   - 1 - Context-based Compression
7. SAM / DAM: Source Address Mode - 2 bits to indicate the length of source address carried inline.
8. M: Multicast Destination
   - 0 - Unicast Address Compression
   - 1 - Multicast Address Compression

LOWPAN_IPHC provides a mechanism to compress link-local, global unicast and multicast address, while both intra and external 6LoWPAN communication is context based compression.

3.3 IPv6 Fragmentation and Reassembly

IP Fragmentation and reassembly is one of the mechanisms of IP. Under certain circumstances, when a packet is small enough, it is originally transmitted as a single unit and arrives at its final destination. When a packet is larger than the MTU size, then the packet is broken into several fragments and traversed along the link and at the receiving, host must accumulate these fragments until completely reconstitute the original packet.

The developed Adaptation Layer between IPv6 Network Layer and IEEE 802.15.4 MAC layer will perform the Fragmentation and reassembly mechanisms. When an IPv6 packet is broken into multiple link fragments, routing processes of Route-over and Mesh-over routing are different.

The maximum size of an IP packet in 6LoWPAN network is equal to the MTU associated with IPv6 which is 1,280 bytes. When the frame sizes are close to the maximum allowed size, they can lead to buffer overflows on the nodes that receive the packets. And in the event that they do not cause buffer overflows, they still increase the load on the nodes to store and reassemble packets. This can bring down the forwarding rate of the fragments in the network increasing the latency. It also causes the devices to use more energy. The fragments will be stored by the receiver for up to 60 seconds in order to receive all fragments for reassembly.

There are two types of fragments that are used by the 6LoWPAN layer - FRAGMENT 1 Figure 3.6 and FRAGMENT N Figure 3.7.

FRAGMENT 1 contains the IPv6 compressed header and can contain a part of the payload. FRAGMENT N packets are the fragments that are send subsequently which must contain the rest of the IPv6 payload.

1. Datagram Size : Size of the original IPv6 packet.

2. Datagram tag : A unique identifier of the IPv6 fragmented packet. Usually it is used in conjunction with the source address of the device to establish network wide uniqueness of the packet. It links all the fragments together.

3. Datagram Offset : This field is present only in the subsequent fragments and contains the offset of the fragment relative to the original packet in multiples of 8 bytes. This way the receiver know where to copy the information in the reconstruction of the original IPv6 packet.

Another important characteristic of fragmentation is that fragments may not necessarily arrive in the order they are sent. 6LoWPAN can reliably reassemble

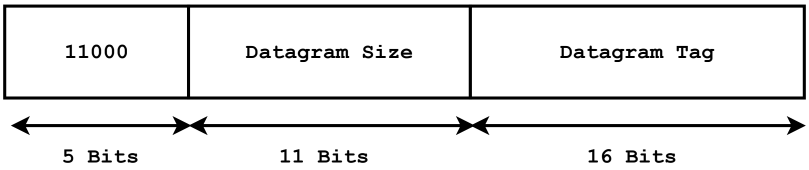


Figure 3.6: First Fragment Header [RFC 4944] (Montenegro *et al.*, 2007)

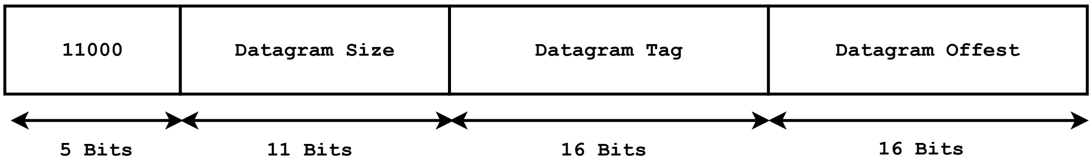


Figure 3.7: Subsequent Fragment Header [RFC 4944] (Montenegro *et al.*, 2007)

the original packet regardless of the order in which the fragments arrive. The only necessary condition is that all fragments must be received at the destination.

3.4 Scalar versus Multimodal data

As images are usually with large size compared to scalar data, and a single image needs to be fragmented into a number of small packets, image transmission is a real challenge for many IoT applications, due to resource constraints and wireless communication. (Pham *et al.*, 2013).

The maximum size of a frame that can be transmitted out of a 802.15.4 device is 128 bytes. An image is generally a few kilobytes in size. Hence to transmit an image successfully over a 6LoWPAN network, it must first be transformed into a stream of bytes, serialized and then transmitted in chunks over multiple IPv6 frames. On the receiving side, the chunks of image data are reassembled and transformed back to the original image as shown in Figure 3.8.

3.5 Objective Function

In RPL, Objective Function module basically describes how a node uses metric to either optimize or constrain a network. Contiki RPL construct DODAG based on Objective Function. Objective Function includes, path metric, node's policies and rules used for avoiding loop which centred on the rank value. The Objective Function is designed using some process to select best parent for each child using any metric suitable for the application. In RPL, every instance of the DODAG formation is connected to an Objective Function, which the nodes use to route

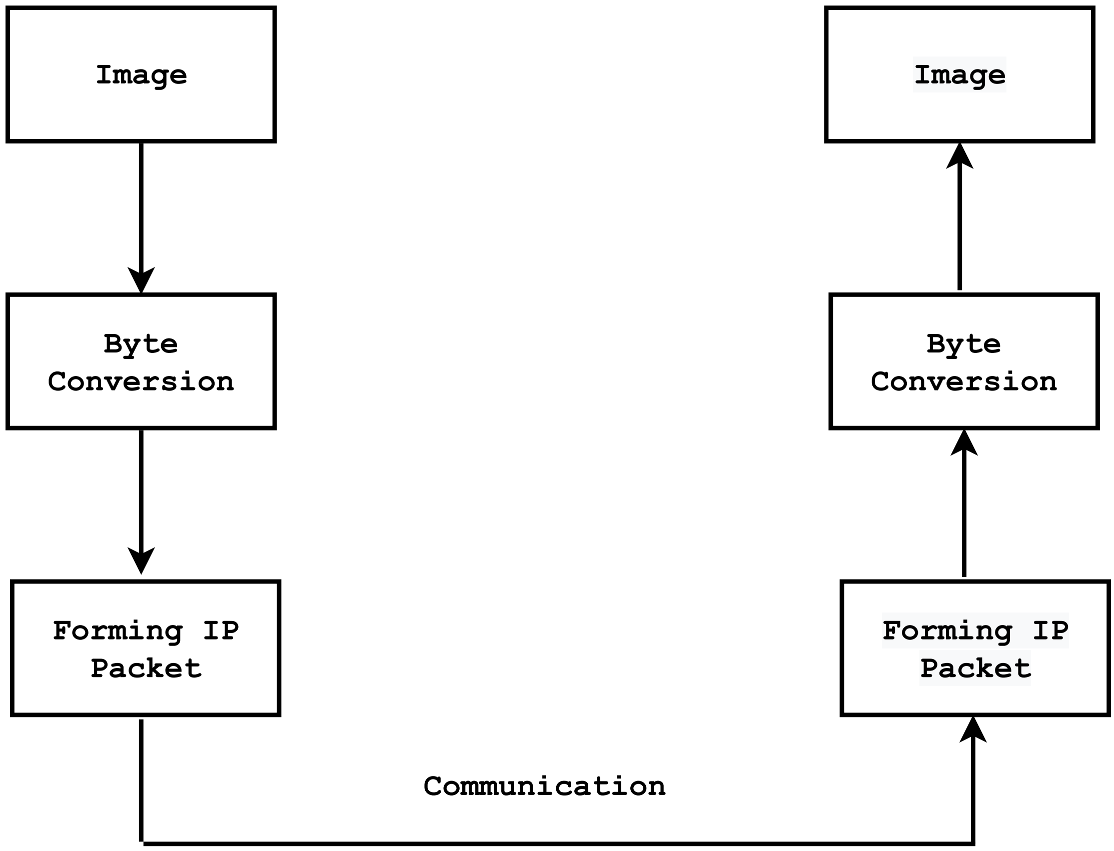


Figure 3.8: Proposed work

information through the best path to its destination. RPL relies on an objective function which uses routing metrics to construct routes and select the best parent for each child node.

To maintain the DODAG; each node calculates its rank and selects its preferred parent. The node's rank progressively decreases on each path towards the DODAG root. RPL uses the OF to determine how parent selection and forwarding decision are made. In fact, the OF defines, (i.) how to compute the path cost, (ii.) how to select parents, (iii.) how to compute the rank and (iv.) how to advertise the path cost.

Contiki RPL implements two objective functions, which are OF0 and MRHOF. OF0 uses hop-count as a metric to assign rank to nodes while MRHOF is basically come up with ETX and ENERGY metric. MRHOF uses link quality called ETX to assign rank. MRHOF-ENERGY node select parents with Maximum remaining energy. Moreover, several metrics have been previously used within RPL and other routing protocols. They include end to end delay, received signal strength indicator (RSSI), and local traffic.

3.5.1 Objective Function Zero

OF0 i.e. Objective Function Zero is the most basic Objective Function (Thubert, 2012) used in RPL. The goal of OF0 is to identify a parent node amongst different neighbours. The root node in the network is assigned the least rank. This information is then carried over to the rest of the network using the DIO multicast control messages. All the nodes that are in range of the root node receive the DIO messages. They identify the root node as their parent and calculate their rank. The rank of a node is determined as rank of its preferred parent plus one. The nodes then multicast DIO messages of their own. The process is repeated at every hop of the network until all the nodes in the network that are in range have joined the DAG. When nodes have to choose their preferred parent, they use the ranks associated with each potential parent and choose the one with the lowest rank as the preferred parent. Thus OF0 determines the network path to the root of the network as the path with the lowest hop count. OF0 is also referred to as minimum hop count objective function.

Each node calculates its rank upon receiving the parent rank. Rank is the summation of parent rank and DEFAULT_MIN_HOP_RANK_INCREASE, which is defined in. Thus, node's rank increases linear to Hop Count and can be computed as follows as mentioned by authors in Equation 3.1, 3.2, 3.3, and 3.4 has been considered from (Winter, 2012):

$$R(N) = R(P) + DEFAULT\_MIN\_HOP\_RANK\_INCREASE \tag{3.1}$$

where R(N) is the node's rank and R(P) is the node parent's rank.

3.5.2 Minimum Rank with Hysteresis Objective Function

This Objective Function (Gnawali and Levis, 2012) tries to choose the path with an optimized value of some routing metric but it gives an advantage of more network stability by using a new concept of "Hysteresis". While any changes occur to the DODAG, the node updates its parent node only if the difference between the new and the previous metric values is more than some given threshold value.

3.5.2.1 Minimum Rank with Hysteresis Objective Function - ETX

The data such as Image needs reliable transmission. As a result ETX OF is used for analysis. It is an objective function that use minimum value of Expected

Transmission Count (ETX) on parent node selection. It is a link metric that predicts the number of retransmissions needed for a packet to be successfully received at the destination. It aims to find path that provides less ETX which means high throughput. The ETX of the entire path is calculated by adding the ETX values of the connecting links along the path (route is the total ETX of each link in the route) and best reliable path is chosen for the data delivery. It can be calculated as the product of the forward (Df) and reverse (Dr) delivery ratio. Df is the probability of a packet to reach the destination while (Dr) is the probability of an ACK to be successfully received.

$$Minimize\ ETX = \frac{1}{D_f * D_R} \tag{3.2}$$

D_f is forward Delivery Ratio

D_R is Reverse Delivery Ratio

Then a given node N calculates its rank as following:

$$R(N) = R(P) + ETX(N) \tag{3.3}$$

where R(P) is the Parent rank and ETX is the Expected Transmission Count to the node P. Therefore, lesser ETX value indicates the good quality of a link in terms of reliability.

3.5.2.2 Minimum Rank with Hysteresis Objective Function - ENERGY

Energy is essential parameter for considering lifetime of the network in case of resource constraint network, so energy is used as OF. MRHOF can use energy as the metric for best parent selection instead of ETX. It chooses that path from source to destination that involves the nodes which are energy efficient. The energy consumed by each node along the path is summed up and the path with least sum is chosen for the data flow.

In Energy metric, nodes try to select parents with the maximum remaining energy. Thus, the best path is selected through an implied Max function because to maximize residual energy for concerned nodes. The node Energy metric (E_E) can be calculated as following

$$E\_E = P\_max/P\_now \tag{3.4}$$

where P_max is the desired max power (initial energy E_0 divided by desired lifetime T) and P_now is the actual power. This Objective Function metric is available in ContikiOS - 3.0 version only.

Algorithm 1 Proposed HEE_OF for Image data Transmission over 6LoWPAN

Input: Candidate Parents
Output: Best Path

Set $S = \{cp_1, cp_2, cp_3, ..., cp_n\}$
Select Candidate Parents cp(HOP, ETX, ENERGY) which are lesser than avg_hops
$S_H = \{cp_{h1}, cp_{h2}, ..., cp_{hn}\}$
$P = min\_hop(S_H)$
Select Candidate Parents from S_H which are having $ETX < avg\_ETX$
$S_{ET} = \{cp_{ET1}, cp_{ET2}, ..., cp_{ETn}\}$
if $S_{ET} \neq \phi$ **then**
    $P = min\_ETX(S_{ET})$
else
    $P = min\_hop(S_H)$
end if
Select Candidate_Parents from S_{ET} which are having max energy
$S_{EY} = \{cp_{EY1}, cp_{EY2}, ..., cp_{EYn}\}$
if $S_{EY} \neq \phi$ **then**
    $P = max\_energy(S_{EY})$
else
    $P = min\_hop(S_H)$
end if

3.6 Proposed HopCount, ETX and ENERGY selection based Objective Function (HEE_OF) for Image transmission

RPL - mainly designed to work in low power and lossy environments. When examining Objective Function like OF0, it only considers the minimum number of hops. The OF0 chooses the path that includes the minimum number of hops, where the path may contain even those links which are unreliable, and this may lead to a lot of retransmissions pointing towards the higher packet losses. Secondly, nodes in shorter paths used frequently will be heading towards the reduction of their battery levels very soon and thus inadequately affecting the lifetime of the network. The choice of shorter paths may also increase the traffic in the selected path. However, for average image data transmission over 6LoWPAN, the Objective function which contains the features of OF0, ETX and Energy is required for providing best effort service along with quality of service.

The proposed HEE_OF for image data transmission over 6LoWPAN is given in Algorithm 1 and the complexity is O(n). In RPL routing protocol, each node selects its parent from the list of candidate parents based on Objective Function. Let S be the set of candidate parents for ith node denoted as $S = \{cp_1, cp_2, cp_3, ..., cp_n\}$

Initially, node selects its candidate parents based on average number of hops to destination, $S_H = \{cp_{h1}, cp_{h2}, ..., cp_{hn}\}$. From the set of selected candidate parents S_H, choose a parent P, where hopcount to reach destination is minimum compared to over candidate parents $P = min\_hop(S_H)$. Now, select the candidate parents from set S_H where the ETX value of node is less than average_ETX value, which is represented as $S_{ET} = \{cp_{ET1}, cp_{ET2}, ..., cp_{ETn}\}$. Now, choose the parent node based on ETX. If $S_{ET} \neq \phi$, otherwise select parents based on min_hopS_H. Now, consider the energy of the candidate node and select parent node with maximum energy. Basically, the proposed HEE_OF selects a parent node with hopcount less than average hopcount, with lesser ETX value and having maximum energy. In worst case scenario, if ETX and higher Energy nodes not available, the proposed algorithm selects OF0(minimum hopcount) as the Objective Function. The proposed algorithm selects reliable, Energy based path with average hopcount, which supports better path selection, thereby supporting image data transmission over reliable link.

In Figure 3.9 example, Node 5 is trying to select it's parent. Based on it's range, it has a list of 4 candidate parents to choose from which include nodes 2, 3, 4 and 8. S = 2, 3, 4, 8

The fixed lines indicate the path from each candidate parent to the root. Thus, Node 5 will have a hop count of 2 via nodes 2, 4 and 8 and a hop count of 3 via Node 3. avg_hops = ((2 + 2 + 2 + 3) / 4) = 2

It first eliminates any nodes that have a hop count greater than the average hop count. Thus, Node 3 which has a hop count of 3 is eliminated from the list. SH = 2, 4, 8

Next, Node 5 calculates the average ETX amongst all remaining candidates. The ETX of nodes 2, 4 and 8 are 192, 512 and 256 respectively. avg_ETX = (192 + 512 + 256) / 3 = 320

Node 5 now eliminates any node that has an ETX value greater than the average ETX. Thus Node 4 is now eliminated from the candidate parent list. SET = 2, 8

Finally, Node 5 then determines the node with the highest energy. Energy of nodes 2 and 8 are 90% and 70% respectively. Thus, Node 8 is eliminated. S_{EY}

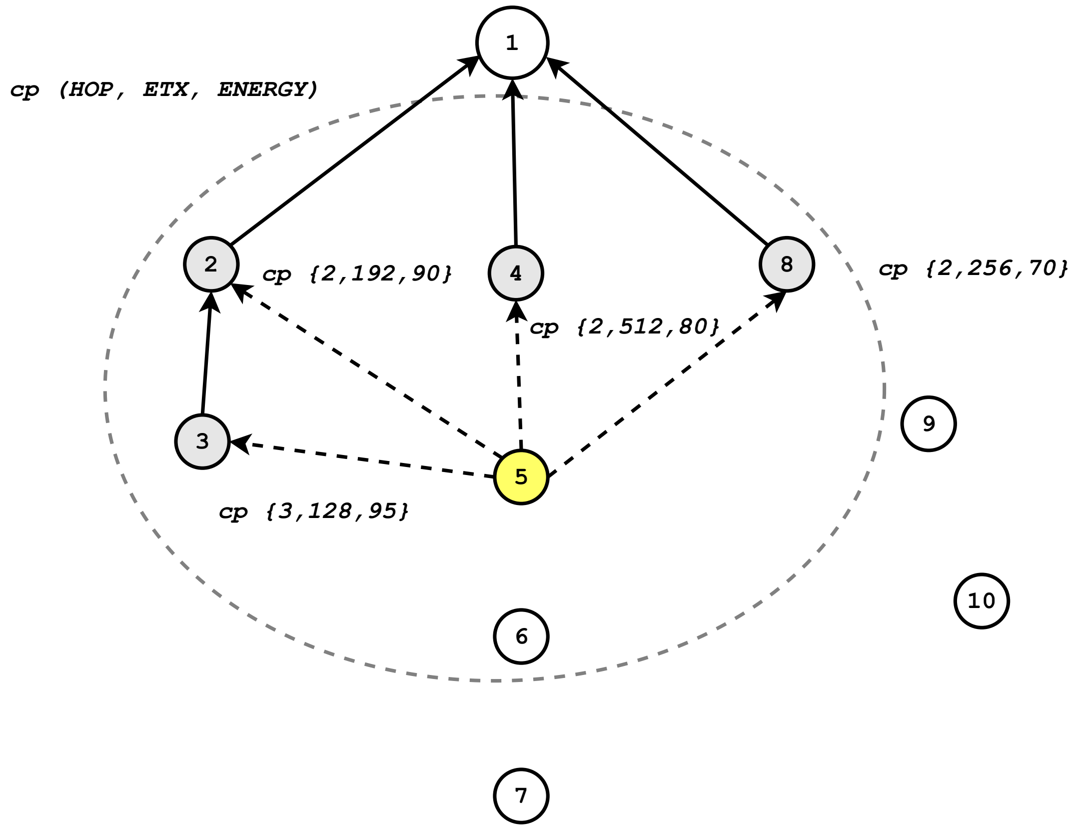


Figure 3.9: HEE_OF example

= 2. Node 5 chooses Node 2 as it's parent. In this way the proposed hybrid OF considers three Objective Functions for parent selection

3.7 Results and Discussion

Cooja simulator with ContikiOS is used for analysing the Objective Function for image Transmission over 6LoWPAN. The simulation experiments are conducted to analyze two things.

1. To analyse effect of existing Objective Function for singlehop and multihop network.

2. To analyse and compare proposed HEE_OF with existing Objective Function like OF0, MRHOF-ETX, and MRHOF-ENERGY.

Experimental setup for the performance evaluation of existing OFs are described in section 3.7.1. Section 3.7.2 says about the evaluation of performance parameters. Results and corresponding analysis are briefly mentioned in 3.7.3 The performance evaluation of proposed HEE_OF with the existing OFs are described in section 3.7.4.

3.7.1 Distance and Hop

WSNs has two types of deployment- Structured and Unstructured.

1. Structured: The sensors are deployed in a standard, fixed, pre-determined way that has thoroughly been decided. The advantage of a structured network is that fewer nodes can be deployed with lower network maintenance and management cost.

2. Unstructured: Implies a dense random deployment within an area. In an unstructured WSN, network maintenance such as managing connectivity and detecting failures is difficult due to several nodes.

The two ways of communication in WSNs are the single-hop and the multi-hop. Both of them are designed based on the energy conservation of the sensors.

1. Single-hop: In this method all the sensors send the information collected, directly to the Destination.

2. Multi-hop: In this Method the sensors send the data to a neighbour node (called aggregation node) and then those nodes collect the information and finally send them to the Destination.

3.7.2 Experimental Setup

In this section, topology and simulation experiment details are explained.

Table 3.1: Simulation Parameter.

Simulation Parameter	**Values**
OS	ContikiOS 3.0
Radio model	Unit disk graph model
Mote type	Sky Mote
Distance	r/4, r/2, 3r/4, r
Hops	Singlehop, Multihop
Network size	100 m x 100 m
Application Program	Examples/ipv6/rpl-collect
Simulation time	60s

The Table 3.1 summaries the simulation settings. Table 3.2 mention the fragments with respect to IPv6 packet.

Table 3.2: Fragments with respect to IPv6

Fragments	**Fragments*IPv6 Size**
2	2*127 bytes
3	3*127 bytes
5	5*127 bytes
7	7*127 bytes

The Contiki operating system and Cooja simulator is used to evaluate the energy consumption of the RPL implementation is used. Contiki can be freely used both in commercial and non-commercial system. For communication, it provides powerful low-power Internet communication and supports fully standard IPv6 and IPv4, along with the recent low-power wireless standards: 6LoWPAN, RPL, CoAP. Cooja is open source software, which is compatible with our needs for this study. Cooja offers the possibility to simulate each node independently using either hardware or software. It can operate at the network level, the operating system level, and the machine code instruction level. It can run on different platforms such as Sky, TelosB, native and can simulate each node separately. The flexibility of Cooja makes it possible to add some extensions in the simulator. The topology considered for image transmission using SingleHop and Multihop are shown in Figure 3.10 and Figure 3.11.

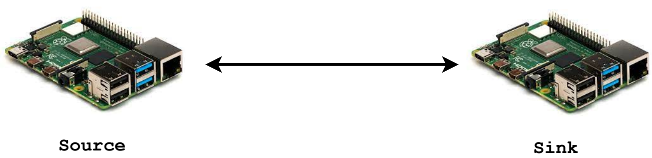


Figure 3.10: SingleHop Topology

Figure 3.11: MultiHop Topology

SingleHop: In this method, two nodes have been considered, sink and source node. Calculation is based on varying the distance from source node with r/4, r/2, 3r/4 and r respectively. The nodes can communicate with less error rate when the nodes are within their communication range. The error rate increases as the distance between the node in communication range increase. To verify the error rate of communication when the nodes are very near(r/4) or very far(r) from the receiver, the distance is selected as multiple r/4.

Multihop: As the number of hop increases, reaching packet to destination is time consuming which results in packet loss. With the distance 3r/4, the test results for 2, 3, 4 and 5 hops for 2, 3, 5, and 7 fragments with performance metrics.

From Figure 3.12 - 3.19, comparison of the existing Objective Function is done by considering the four parameters mentioned below. When considering singleHop, all three existing Objective Functions provide almost same results. But when considering multiHop, as the number of hop increases,

1. Packet reaching the sink decreases.
2. Control overhead increases.
3. Energy consumed by the nodes nearer to the sink node will be high.
4. Delay in reaching packet to the sink increases.

By considering the above constraints, proposed a new RPL-OF called as HEE_OF that considers ETX, OF0 and ENERGY. So the comparison of the existing OF is executed with the HEE_OF as seen in section 3.7.4.

3.7.3 Performance Parameters

Following are the various performance parameters used for evaluation of the communication in 6LoWPAN network.

1. Packet Delivery Ratio: It is the ratio of the number of successful receiving of packets at the sink node to the total number of packets transmitted.

$$Maximize\ PDR = P1/P2 \tag{3.5}$$

   Where P1 is the sum of all the data packets received by each destination, and P2 is the sum of total number of data packets produced by each source.

2. Control Traffic Overhead: It is one of the important parameter in LLNs (RFC 6687). It is recognized as a necessary component of the network as control packets required for building and repairing routes in the network. The concept of trickle timer to update and repair the routes helps to reduce the number of unnecessary control packets (Tripathi *et al.*, 2012).

3. Energy Consumption(mJ): As the nodes of 6LoWPAN are highly resource constraint network, Energy consumption is one the important aspect in IoT (Wang *et al.*, 2018). The energy consumption of a node depends on power consumed for transmission and reception. In most of the cases the communication cost is more than the computation cost in terms of energy consumption. The ContikiOS provides a tool called powertrace which provides details regarding power consumption. The energy consumption is calculated as shown in equation 3.6.

$$\begin{aligned} Minimize\ Energy(mJ) = (&Transmit * 19.5mA \\ &+ Listen * 21.5mA \\ &+ CPU\_time * 1.8mA \\ &+ LPM * 0.0545mA) * 3V/Rtimer \end{aligned} \tag{3.6}$$

Equation 3.6 Winter (2012) where Transmit is the time taken to transmit all the packets, Listen is the time taken to receive all packets and CPU is the time taken for computation at CPU and LPM is the power consumption during Low Power Mode. Rtimer represents the number of ticks per second (=32768 ticks/s).

4. Latency(ms): It is the term used to indicate any delay that happens in data communication over a network. It takes average time for a data packet to arrive at the destination. Therefore it involves all possible delays produced by buffering during route discovery latency and queuing at the interface queue. This metric calculates by deducting time at the first packet that was transmitted by the source from the time at the first data packet arrived at the destination. Mathematically, it can define as:

$$Average\ L = S2 - S1/N \tag{3.7}$$

Where S1 is the first packet transmitted and S2 is the first packet arrived at the destination. N is the number of packets obtained by all destination nodes.

3.7.4 Results and Analysis

The simulation experiments are conducted considering singlehop and mutlihop scenario. Results with respect to each parameter are analysed in this subsection.

1. PDR

   In case of SingleHop communication, the results are as shown in the Figures 3.12a 3.12b 3.12c with respect to MRHOF_ETX, OF0 and MRHOF_ENERGY. As all the packets reach the destination and receive the ACK, so there is 100% delivery of packets from source to destination.

   The result of Multihop communication, is shown in the Figures 3.13a, 3.13b, 3.13c with respect to MRHOF_ETX, OF0 and MRHOF_ENERGY. The nodes are kept at the distance of 3r/4. The multihop communication results shows that as the number of nodes in the path increases, PDR value drops due to the increased load at each node as each node performs data transmission to sink node. It is obtained that effect of number of fragments is more from second to third fragment and later the PDR value is maintained constantly.

   If a node is within one hop distance of the sink node, the PDR is close to 100% due to lack of any congestion. However, when nodes are deployed in the network, the source and destination are generally multi-hop away. The intermediate nodes become bottlenecks when relaying data for multiple sink nodes causing packet drops. Thus the PDR drops below 100%.

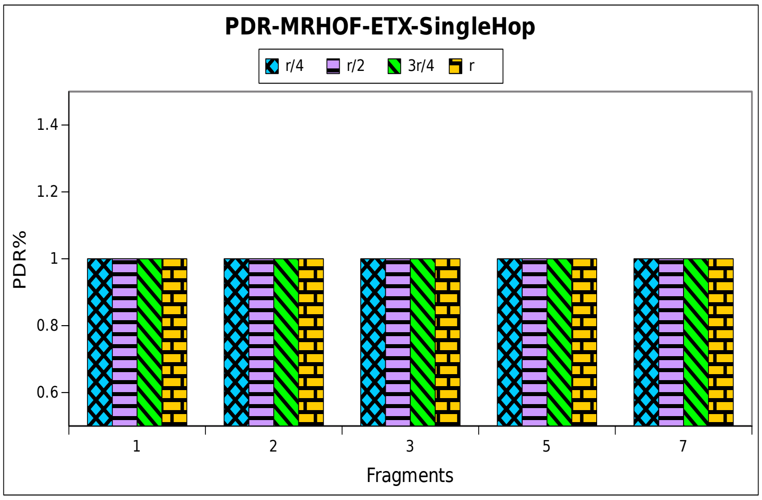
2. Control Traffic Overhead

   The calculated packet overhead is the total number of control messages, i.e., DIS, DIO, DAO, DAO-ACK transmitted until the end of the simulation. In case of Singlehop communication, the results are as shown in the Figures 3.14a, 4.13, 3.14c. The overhead value is less compared to Multihop because transmission of packets occurs between only two nodes. Therefore Objective Function MRHOF-ETX has slightly more packet overhead compared with the other two OFs.

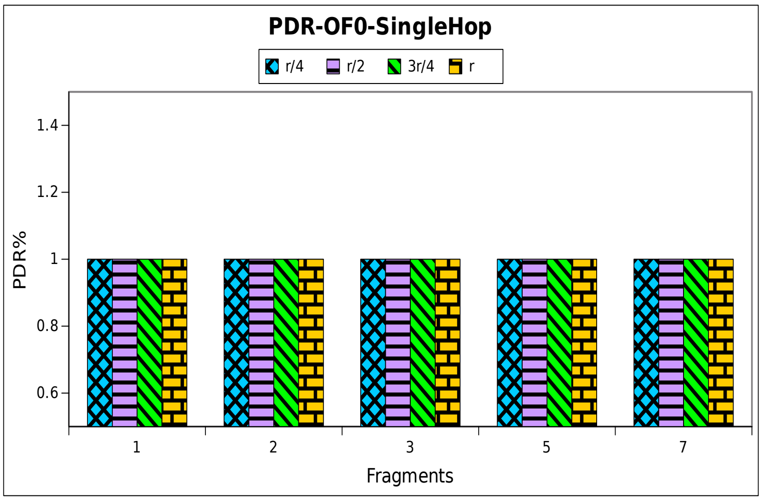
   In case of Multihop Packet communication, the results are as shown in the Figures 3.15a, 3.15b, 3.15c. Therefore, Packet overhead increases as the number of nodes increases. 3rd, 5th and 7th fragments in all Hops remain with the same value in ETX, OF0 and ENERGY metrics. Variation occurs in the 3rd fragment. It needs further Analysis on why there is low load with respect to 3rd fragment.

3. Energy Consumption

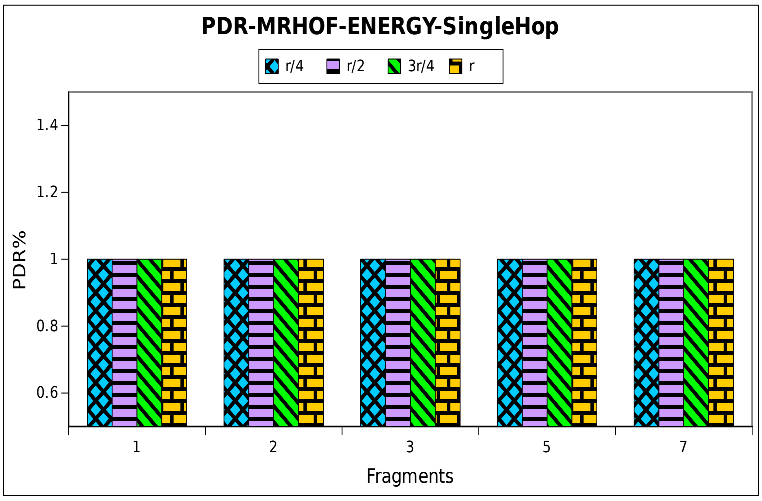
   In case of Singlehop communication, the results are as shown in the Figures



(a) MRHOF-ETX

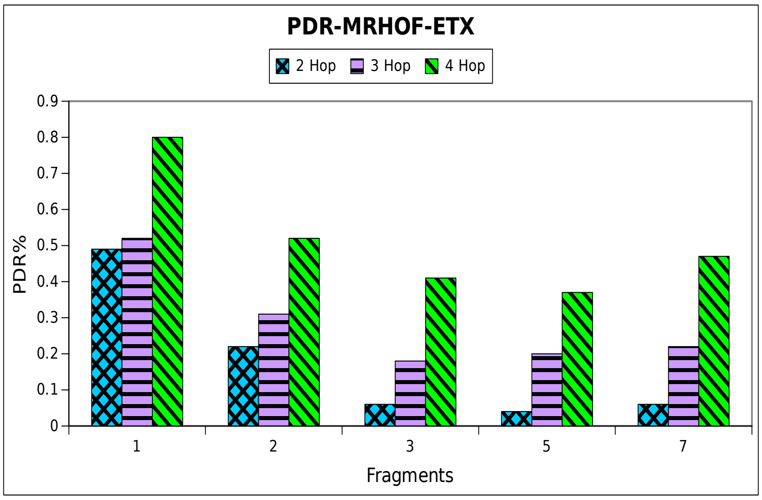


(b) OF0

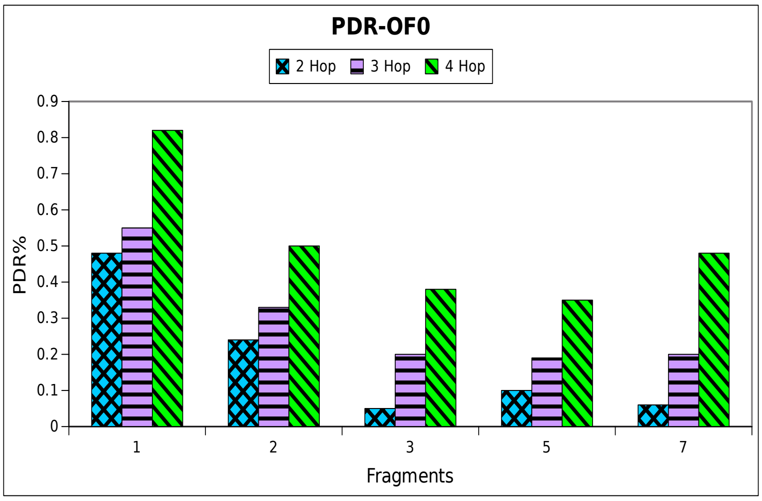


(c) MRHOF-ENERGY

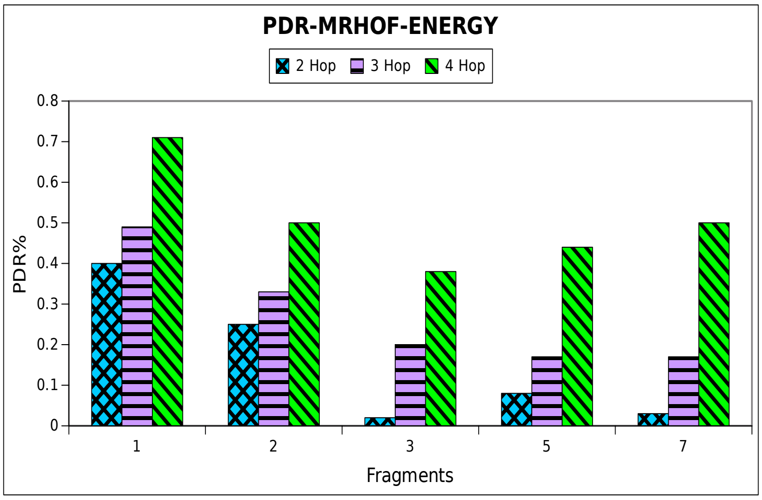
Figure 3.12: Performance Analysis of PDR in Singlehop



(a) MRHOF-ETX

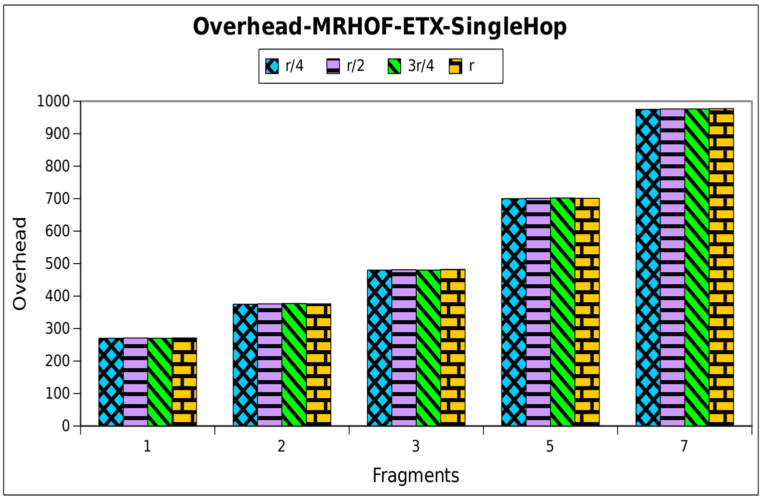


(b) OF0

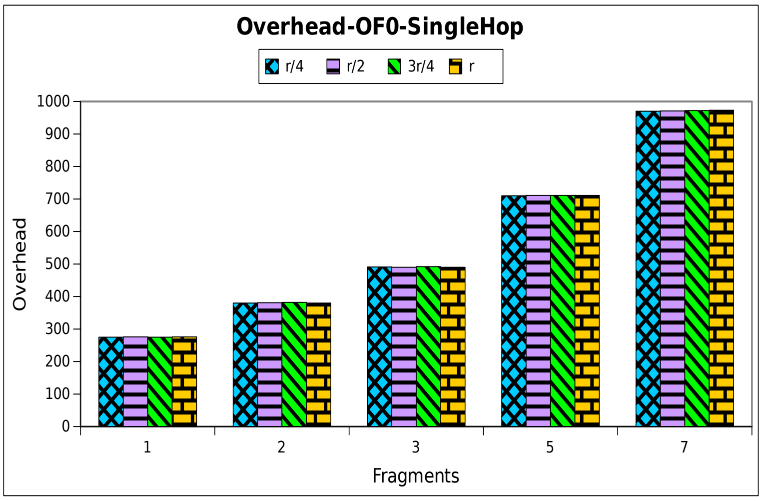


(c) MRHOF-ENERGY

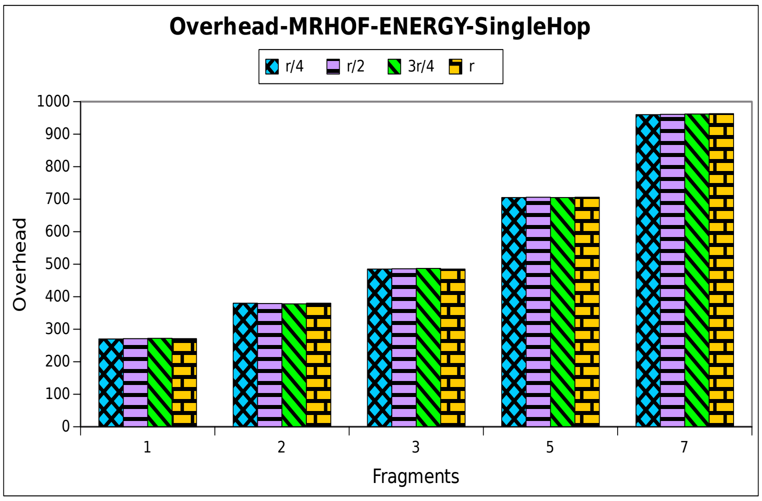
Figure 3.13: Performance Analysis of PDR in MultiHop



(a) MRHOF-ETX

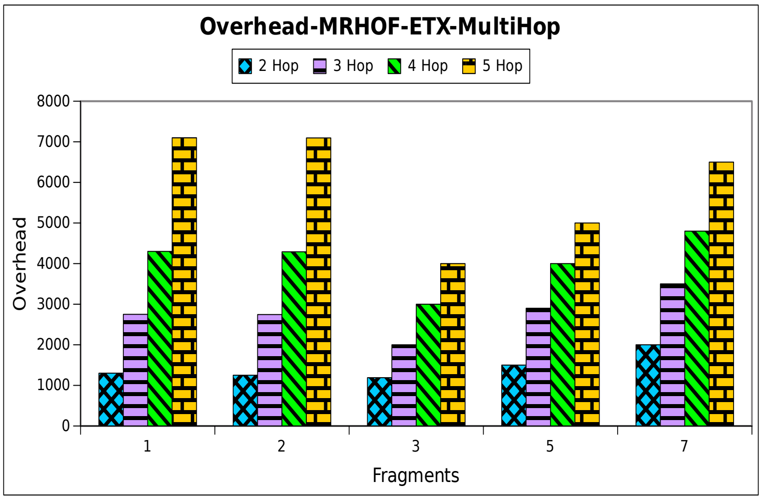


(b) OF0

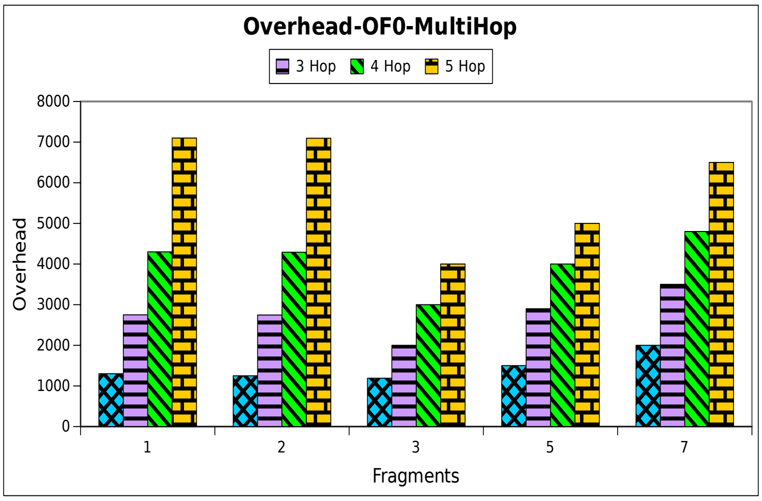


(c) MRHOF-ENERGY

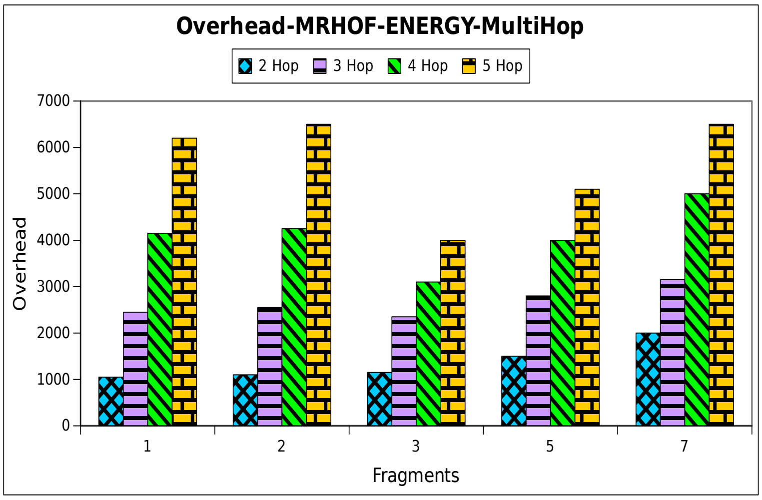
Figure 3.14: Performance Analysis of Overhead in Singlehop



(a) MRHOF-ETX

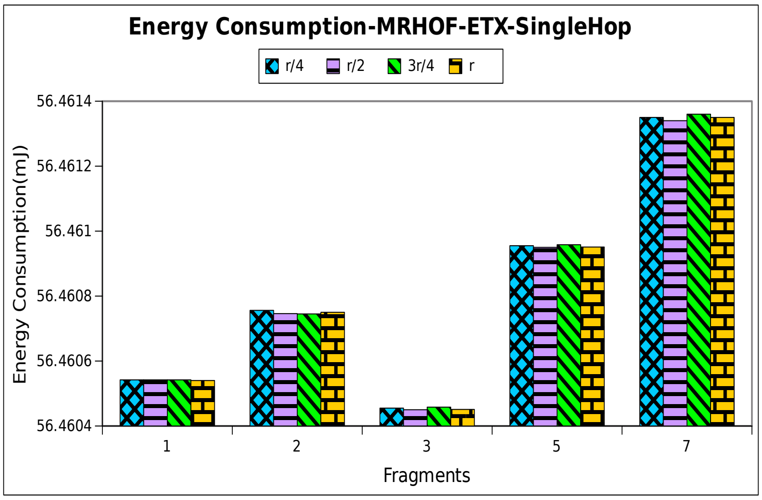


(b) OF0

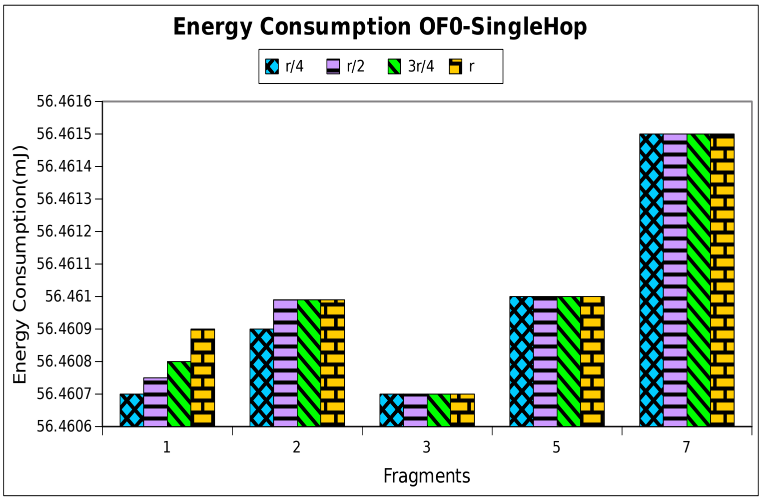


(c) MRHOF-ENERGY

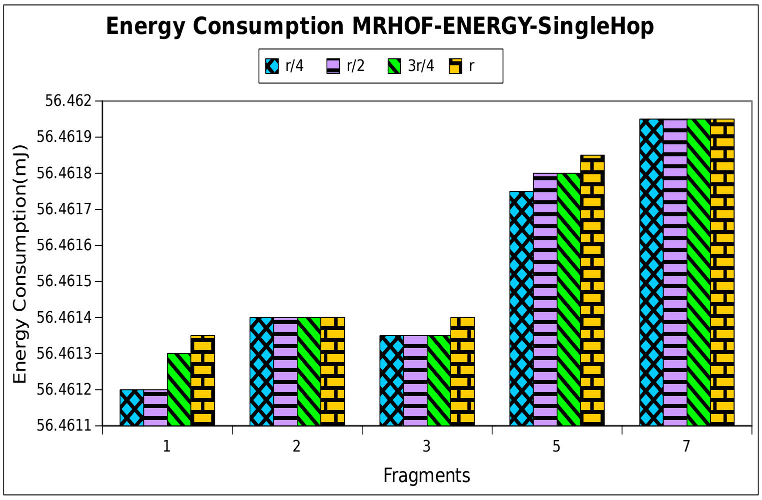
Figure 3.15: Performance analysis of Overhead in Multihop



(a) MRHOF-ETX

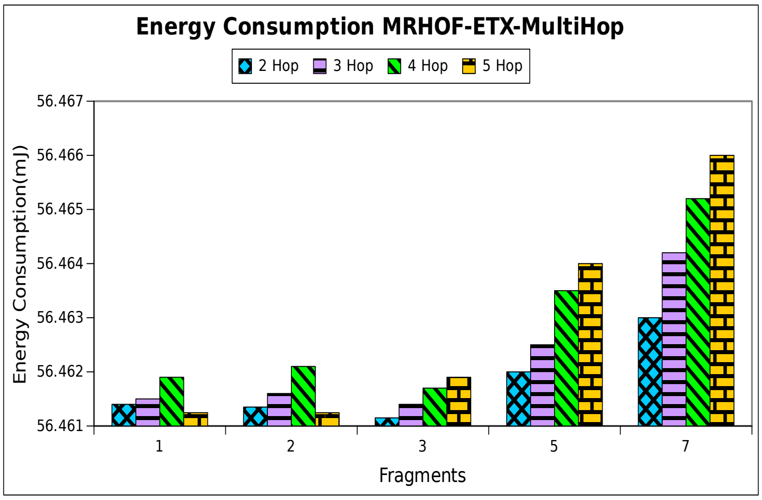


(b) OF0

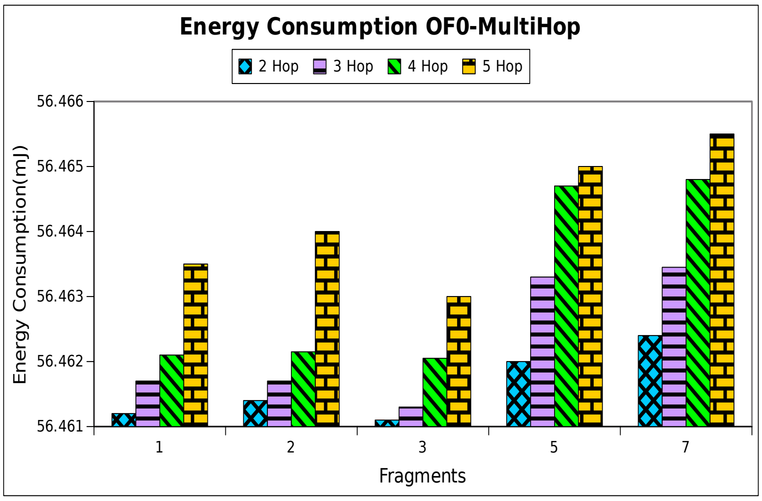


(c) MRHOF-ENERGY

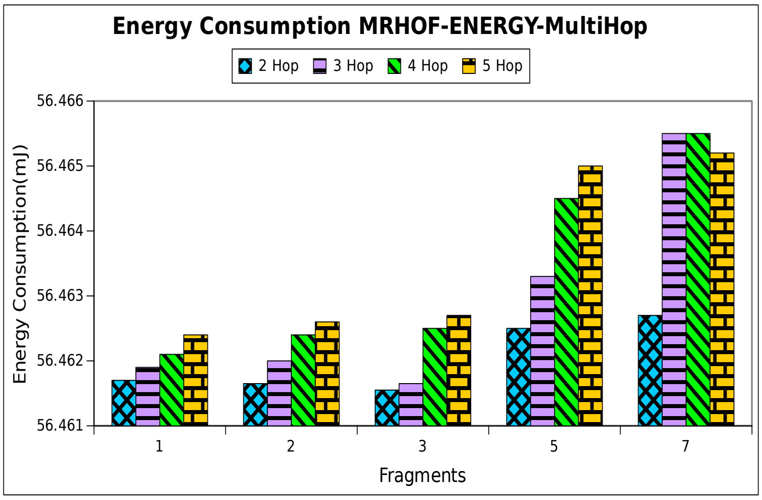
Figure 3.16: Performance Analysis of Energy Consumption in Singlehop



(a) MRHOF-ETX

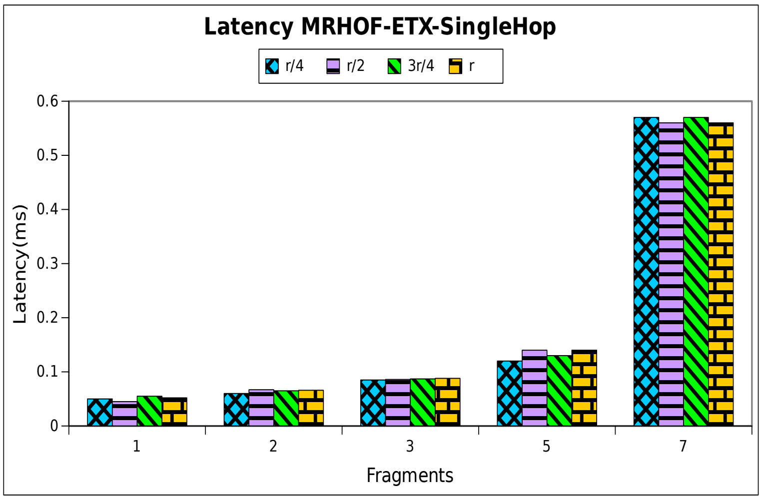


(b) OF0

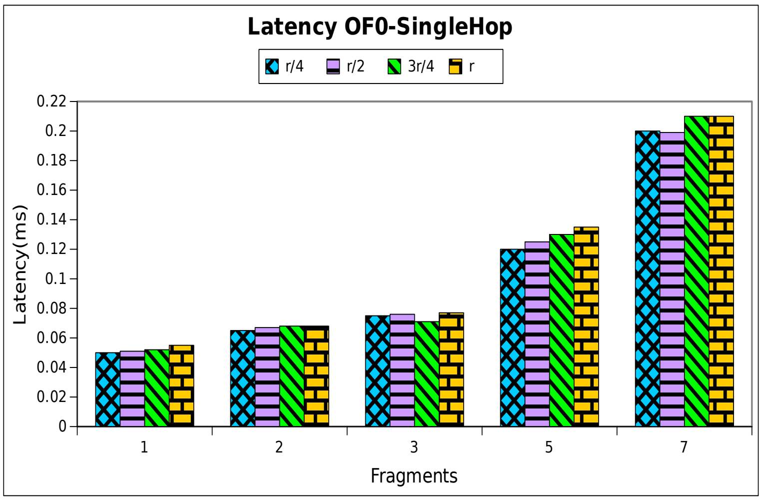


(c) MRHOF-ENERGY

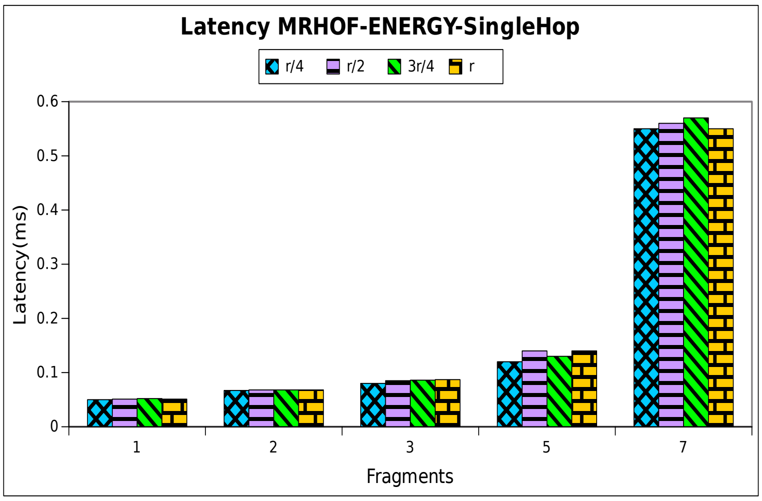
Figure 3.17: Performance analysis of Energy Consumption in Multihop



(a) MRHOF-ETX

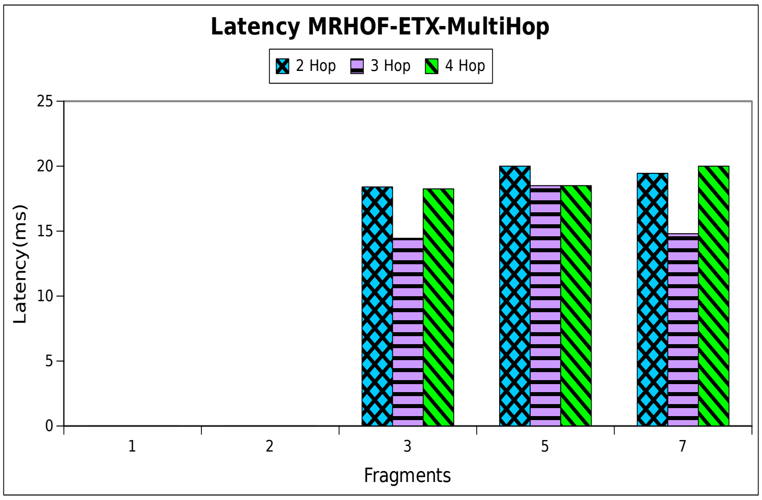


(b) OF0

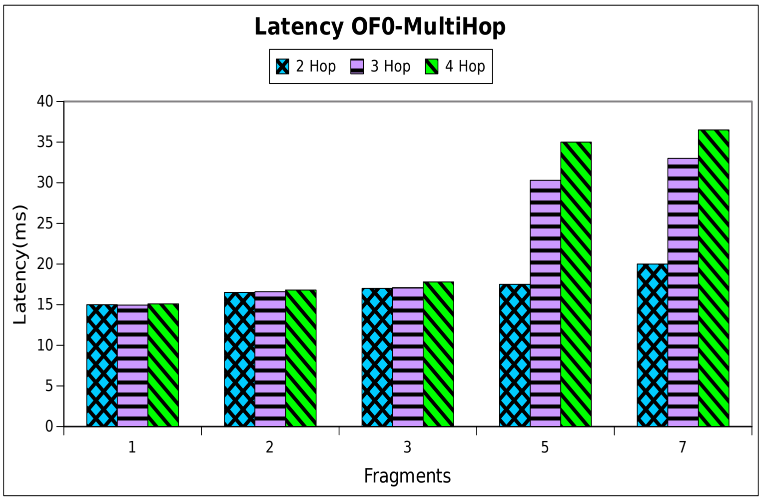


(c) MRHOF-ENERGY

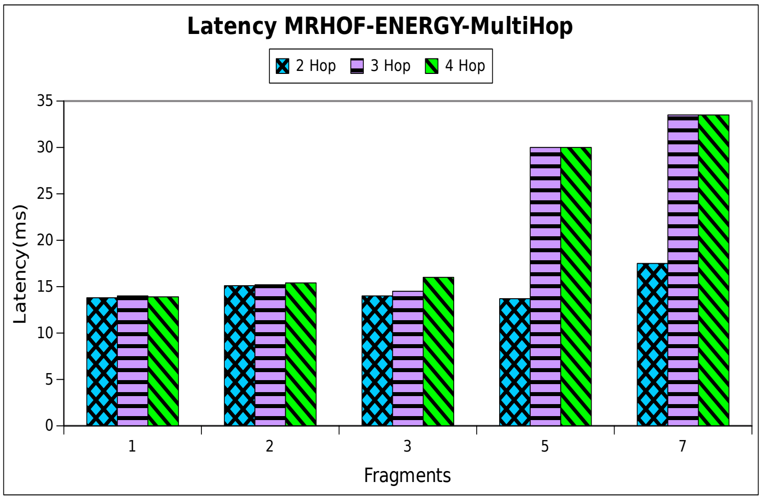
Figure 3.18: Performance Analysis of Latency in singlehop



(a) MRHOF-ETX



(b) OF0



(c) MRHOF-ENERGY

Figure 3.19: Performance Analysis of Latency in Multihop

3.16a, 3.16b, 3.16c. Energy consumed by all Objective Functions of different fragments with varying distance are similar.

But in the case of Multihop communication, the results are as shown in the Figures 3.17a 3.17b,3.17c less hop leads to less energy consumed. As the fragment size increases, energy consumption is more.

4. Latency

In case of Singlehop communication, the results are as shown in the Figures 3.18a, 3.18b, 3.18c. The Latency naturally increases along with the distance to the sink. OF0 gives 40% less latency compared with ETX and ENERGY.

In case of Multihop the results are as shown in the Figures 3.19a, 3.19b, 3.19c. The results were recorded for 2 Hop, 3 Hop and 4 Hop for 60seconds. As the hop increases packet reaching destination takes a lot of time. When 5 Hop experiment was carried, at the 50th seconds the system used to stop responding. It is observed that a lot of load in each node results in the suspension of the experiment. OF0 and ENERGY metric gives a better result with respect to ETX. Even though latency is good for 2 hop 2nd fragment in ETX, later 3rd, 5th, and 7th fragment will have a rapid increase in latency.

3.7.5 Performance Evaluation of Proposed HEE_OF

The topology considered for image transmission is shown in Figure 3.20.

Table 3.3: Simulation Parameter

Simulation Parameter	**Values**
OS	ContikiOS 3.0
Radio model	Unit disk graph model
Mote type	Sky Mote
Distance	Random
Network size	100 m x 100 m
Application Program	Examples/ipv6/rpl-collect
Simulation time	60s

The Table 3.3 mention the simulation settings to conduct HEE_OF Objective Function.

Proposed HEE_OF (HopCount-ETX-ENERGY) gives slightly better result in terms of performance metrics. When calculating PDR, ENERGY metric drops

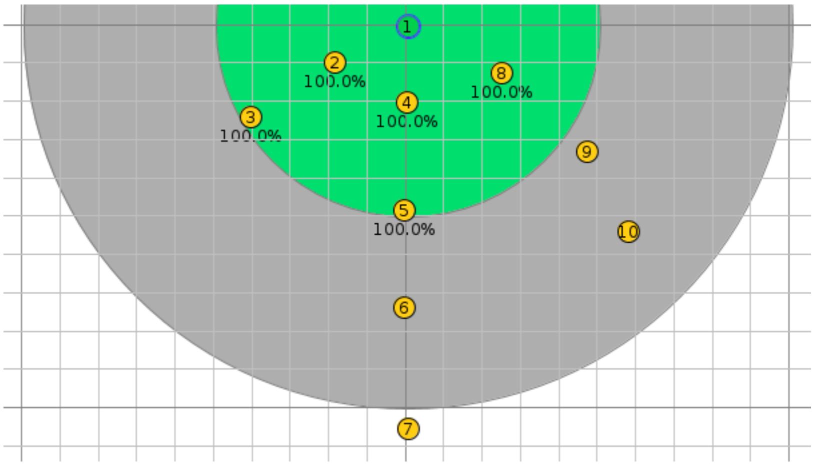


Figure 3.20: Proposed Topology

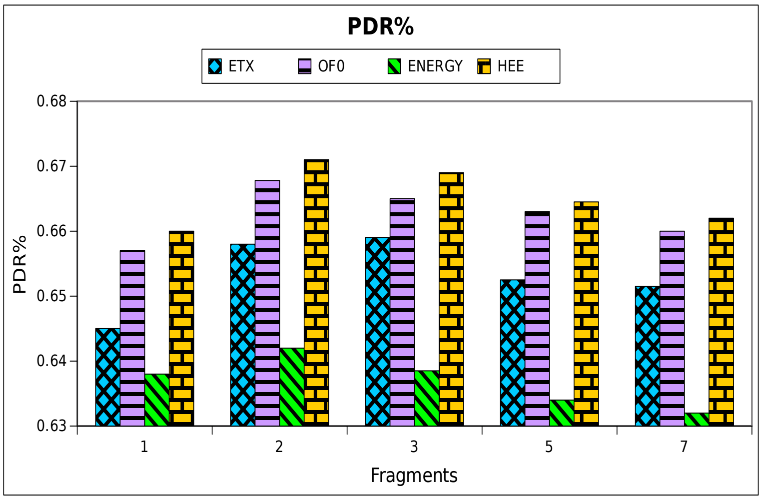
when comparative to other metrics. Proposed HEE_OF is shown in Figure 3.21a gives better performance as it considers both node energy and link quality with respect to hop count. Therefore, Compared to fragments PDR value decreases as the number of fragments increases. Approximately ETX, OF0 and ENERGY metrics gives 0.013%, 0.004% and 0.03% PDR with respect to proposed HEE_OF.

As the number nodes increases in the DODAG, nodes control overhead increases based on Objective Functions. So the proposed HEE_OF is shown in Figure 3.21b gives equivalent performance with respect to OF0. Therefore around 17% of overhead is more when compared to ETX and ENERGY metric.

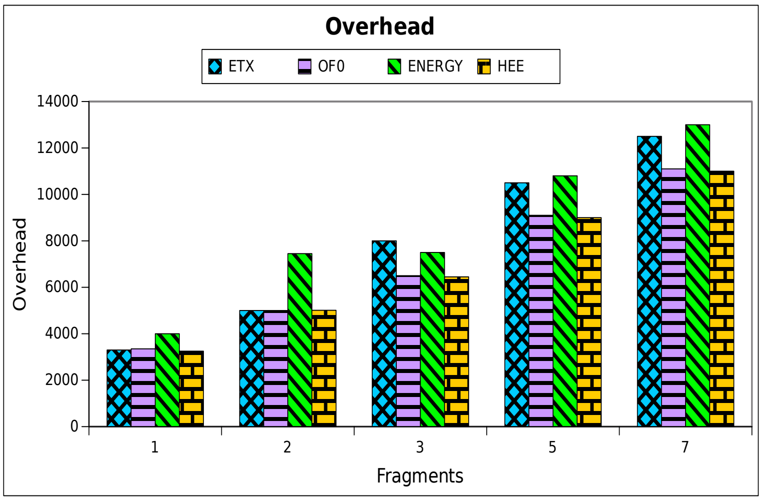
As energy is an important feature of networking, energy consumption is shown in Figure 3.22a. Proposed HEE_OF is slightly better than ETX, where with respect to ETX, OF0 and ENERGY proposed HEE_OF gives 2%, 4% and 3% better results.

Figure 3.22b explains when MRHOF-ETX is analyzed, selecting the path with a reliable link will necessarily not lead to a decrease in end-to-end delay since the chosen pathway to the root node may be longer. The end-to-end delay progresses proportionally to the propagation time. Moreover, the task of OF0 is to reduce the number of hops to the DAG root, and it does not significantly present delay conversion when some intervening nodes are congested. When considering these limitations, the performance of latency in proposed HEE_OF provides a better result than OF0 and ENERGY metric. Proposed HEE_OF provides 1.35% and 1.7% better results with OF0 and ENERGY metric. Latency needs to be improved with respect to ETX, as it gives a better result of 0.1% than Proposed HEE_OF.

As many papers in the last few years, compare existing Objective Functions with the proposed Objective Functions for particular applications. Table 3.4 suggest the comparison of different RPL OFs with the proposed OF.



(a) PDR



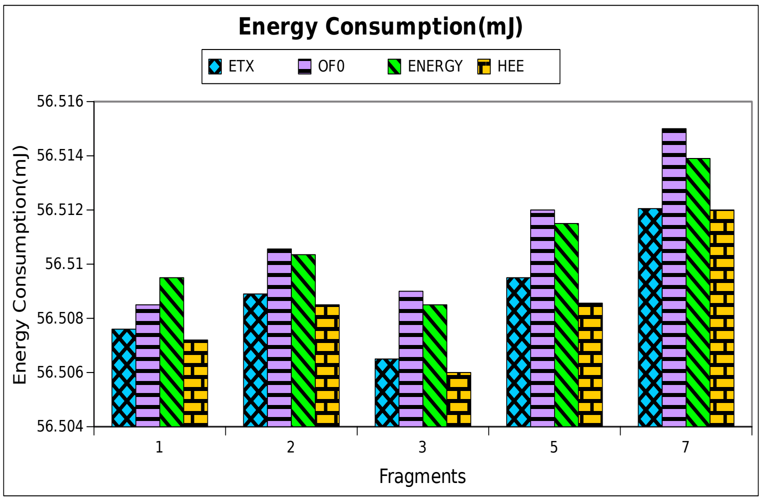
(b) Overhead

Figure 3.21: Comparative Study of Objective Functions with HEE_OF

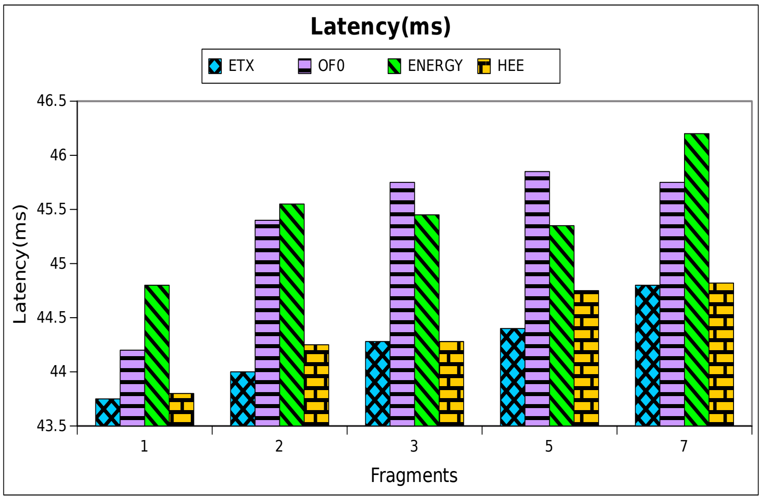
1. HEE_OF: The proposed RPL mainly concentrates on image data for image transmission. Following papers concentrate only on scalar data.

2. RPL-FZ: (Sonia Kuwelkar, 2021) combines three metrics (ETX, Delayand Residual Energy) by using the Fuzzy Logic process. The three metrics are combined using fuzzy inference system to evaluate the Quality of each neighbor node. The aim of the proposed RPL is for make routing decisions.

3. SIGMA-ETX: (Sanmartin and et.al, 2018) is more efficient with networks containing large number of nodes per unit of area in the LLN routing in terms of quality of service.



(a) Energy Consumption



(b) Latency

Figure 3.22: Comparative Study of Objective Functions with HEE_OF

4. OF-EHE: (Soukayna and Abdellatif, 2019) helps to improve the quality of service by combining several metrics necessary for the decision making concerning the selection of the best path using Fuzzy logic process.

5. T-OF: (Moradi and Javidan, 2020) is used to select preferred parent of the nodes and also increase the network lifetime.

6. ERAOF: (Sousa and et.al, 2017) is used for energy efficiency and reliability in data transmission for IoT applications.

3.8 Summary

IoT as an emerging model supports integration, transfer and analytic of data created by smart devices(e.g., Sensors). As the number of devices joined to the Internet increases, there is a necessity to identify each device. Devices need to be low power low cost, for ease of deployment and hence, Low Power Lossy Networks for information gathering. To transfer data from Sensor nodes-to-Sink or Sink-to-Sensor nodes, efficient routing protocol has to be designed, by considering resource utilization, communication overhead, and delay. Sometimes even multimodal sensors are required such as image, video and audio devices, temperature, humidity, and many more scalar sensors.

Performance evaluation of Singlehop and Multihop topology are carried for the image transmission over 6LoWPAN with IPv6. Based on the analysis, a hybrid HopCount-ETX-ENERGY(HEE_OF) is proposed for improving the performance for image data transmission. The effectiveness of communication is validated against static deployments with various radius. The results indicate the proposed Objective Function works for both structured and unstructured types of deployments. It provides a better result at an average of 4%, 6% and 3% with respect to PDR, control traffic overhead and energy consumption. Latency needs to be improved by 0.1%. While there is improvement, it isn't substantial enough. Additionally, a network is heterogeneous with a mix of scalar and multimodal sensors and topologies with mix of both must be considered. To achieve further gains in performance, there is a need to reduce the size of the network header to allow more application data to be accommodated in a frame. Also, there is scope to improve performance with the use of other data types when considering an objective function especially in the context of multimodal data. Performance can also

Table 3.4: Comparison of different RPL OFs with HEE_OF

OFs - RPL	**PDR**	**EC**	**Overhead**	**Latency**	**PC**	**Lifetime**	**Image data**	**Comparison with OFs**
Proposed HEE_OF	✓	✓	✓	✓			✓	MRHOF-ETX,-ENERGY, OF0
RPL - FZ	✓			✓	✓			MRHOF, OF0
SIGMA - ETX	✓	✓		✓		✓		MRHOF, OF0, PH-ETX
OF -EHE	✓	✓						MRHOF, OF0
T - OF	✓			✓		✓		OF0, ETX,EN-OF
ERAOF	✓	✓						MRHOF, OF0

be enhanced with defining better routing models in both Multipoint-to-Point and Point-to-Multipoint topologies.

Chapter 4

New Bit Pattern based IPv6 Address Compression Techniques for 6LoWPAN Header Compression

The Internet has gone beyond its definition in which the term communication devices are not just the routers, computers or mobile phones. It can be any "thing" connected to any other "thing" over the Internet. For example, soil can communicate with the water pump! That is, in an automated irrigation system using IoT, sensors are used to measure the humidity of soil and this data is sent for processing which finally turns on/off the water pump. Thus, the Internet of Things provides a platform for connecting anything, anytime, anywhere to the internet. To achieve this, it also needs certain aspects to be incorporated into communication technology standards. IPv4 is the de facto standard for IP address assignments. But due to the limited range of IPv4 addresses, to connect all the things to the Internet, the address bits in IPv4 are extended to 128 bits in IPv6. Hence, IPv6 is considered as the Internet Protocol layer standard for Internet of Things. IPv6 contains a minimum number of fields in the fixed header and places the rest of the fields in extension header compared to IPv4. IPv6 design also focuses on decreasing the packet processing time at each intermediate node and increasing address space. These aspects made the size of the IPv6 header 2 times larger than the IPv4 header. IPv6 mandates the minimum Maximum Transmission Unit (MTU) as 1280 bytes. Even though the fixed 1280 bytes packet is a nominal packet in the traditional internet, the packet transmission is a challenge in resource constrained networks like Internet of Things as the devices are battery operated in certain applications.

The protocol suite for IoT for Data link layer can consider IEEE 802.11, Bluetooth or IEEE 802.15.4. Among these communication protocols, the IEEE 802.11 standard consumes more energy and hence, the protocol can be used when sufficient energy source is available for the nodes. In case of Bluetooth technology, it uses master-slave technique and also has limitations on number of devices that can be connected to master node. IEEE 802.15.4, which is a specification that defines MAC and PHY layer for low power, resource constrained devices, is suitable for connecting a large number of devices, but the basic idea was to form an id based network. To connect a large number of devices or things, IPv6 protocol is best at the network layer. IEEE 802.15.4 supports 127 bytes of MTU in the data link layer. Hence, in order to support the IPv6 based network over IEEE 802.15.4, an adaptation layer is essential in between network layer and Data link layer. 6LoWPAN is the adaptation layer to support IPv6 over IEEE 802.15.4 which is proposed in the RFC 4944 Montenegro *et al.* (2007).

6LoWPAN which provides the support for IPv6 over IEEE 802.15.4, with functions such as Header Compression, Fragmentation and Mesh Routing. Compression techniques focus on eliding the fields in the header that are redundant or which can be derived from the other layers of the protocol stack. For example : Length field in IPv6 can be derived from Physical layer header or from fragment or datagram offset. Similarly, MAC address expanded IPv6 address can be derived from MAC address. RFC 4944 Montenegro *et al.* (2007) defines Two broad categories of Header Compression techniques : Stateless Header Compression and Context Based Header Compression. Stateless Header Compression techniques provide compression and decompression information in the packet itself. It is basically flow independent. Stateless Header Compression is supported by HC1 and HC2 header compression. HC1 defines the IPv6 header compression process and HC2 defines Next Header Compression process. Currently UDP header compression is well defined in RFC 4944 Montenegro *et al.* (2007) for HC2.

6LoWPAN also supports fragmentation Lenders *et al.* (2021) between Network layer and Data link layer. The fragmentation defined in IPv4 is totally different from the fragmentation defined in the IPv6 extension header and 6LoWPAN adaptation layer. Fragmentation in IPv6 is end-to-end fragmentation, between source and destination, whereas fragmentation in 6LoWPAN is between the Network layer and Data Link layer of the same system. As IEEE 802.15.4 supports 127 bytes of payload, and the size of the IPv6 packet is 1280 bytes, 6LoWPAN adaptation layer supports fragmentation of IPv6 packet to transmit over IEEE 802.15.4. 6LoWPAN also supports the mesh routing with mesh under and mesh over based on the decision handling layer of protocol stack.

The Robust Header Compression (ROHC) mainly compresses the large protocol header overheadGomez *et al.* (2020). RFC 8824Minaburo *et al.* (2021) provides a generic framework for Static Context Header Compression and Fragmentation of IPV6/UDP/CoAP packets to allow their transmissions over the Low-Power Wide Area Networks (LPWAN). Initially the packet is sent uncompressed and later the communication is based on context which is obtained by Rule Identifiers. Even though RFC 8824Minaburo *et al.* (2021) provides a generic framework for packet compression, the formation of the Rule Identifier (RuleID) is yet to be defined or standardised for IPv6 over IEEE 802.15.4.

Header compression techniques compress the bits in the header to provide more space for data bits in the packet. The motivation for this work is to compress the number of leading zeros in the addresses to perform further address compression, even after performing stateless or context based header compression. Hence, this research work focuses on address compression techniques by considering the number of leading zeros in the source and destination IPv6 address. We propose two different techniques for address compression: (1) Double colon based address compression and (2) Bit pattern based address compression.

4.1 Related Work

In the paper (Huiqin and Yongqiang, 2010), the author describes the need for an efficient packet header compression scheme when using IPv6 over IEEE 802.15.4-based low-power wireless personal area networks that have limited bandwidth, energy and memory. An improvement over existing header compression scheme is proposed. The proposed scheme improves the compression in the IPv6, UDP, ICMP and routing extension headers.

In the paper (Nam *et al.*, 2015), the author explores different packet header compression techniques for better QoS in wireless sensor networks for use in Ship Area Sensor Networks (SASN). In a SASN network, the location of the sensor nodes are fixed. They data transmitted in frames generally differ very little from the previous frames. The characteristics of different packet header compression techniques are described. The techniques include Payload Header Suppression(PHS), Robust Header Compression(ROHC) and IPv6 over Low power Wireless Personal Area Network Header Compression(6LoWPAN HC). Simulations are also run with two different BER (Bit Error Rate) with each technique and the results are compared for performance with respect to throughput. The author determines the suitable packet header compression technique for SASN using the results from the simulations.

In the Paper Soro *et al.* (2007) discussed the header compression techniques widely used in wireless and satellite communications. It highlights the draw back of all the techniques with respect to bit error in packets or packet losses. Corrupted or missing headers lead to failures when decompressing consecutive fragments. This in turn leads to disconnection of communication. The paper reviews the header compression protocols that are standardized for an unidirectional link. A simple generic header compression model is built using parameters that characterize other header compression protocols. The proposed model is evaluated to draw initial inferences when choosing header compression techniques for satellite communications.

In the paper (Nam *et al.*, 2015) the author mentions that for higher Quality of Service (QoS) for wireless sensor networks for applications such as bulkhead of ship area, packet header compression techniques support resource utilisation efficiently. As the sensor nodes are deployed in fixed locations, sensor nodes can transmit consecutive data with small differences compared to previous packets. Therefore it is useful to use packet header compression techniques to Ship Area Sensor Networks (SASN). The authors follow the trend of packet header compression techniques and describe the characteristics of some well-known compression techniques which are Payload Header Suppression(PHS), Robust Header Compression(ROHC) and IPv6 over Low power Wireless Personal Area Network Header Compression(6LoWPAN HC). The simulation results show promising improvement with header compression technique.

In the paper Soro *et al.* (2007) Header Compression techniques are widely used in wireless and satellite communications. The author stresses on the importance of header compression and issues with respect to decompression of packets when the header gets influenced by noise and header is received with error.

In the paper Hasbollah *et al.* (2009) implemented a gateway that interacts between the 6loWPAN sensor network and IPv6. Different packet sizes are transferred to measure the performance of the connection of technology of IEEE802.15.4 and wired IPv6 network. The gateway needs to contain two interfaces to connect the movement of data between IPv6 and 6LoWPAN wireless sensor networks. The compression and decompression of IP headers are performed by the gateway to permit tunneling of tiny 6LoWPAN packets to the wireless sensor network. Transferring larger packets is a constraint in IEEE 802.15.4 because it allows 127 bytes of packet size.

In the paperGarg and Sharma (2016) describes the 6LoWPAN protocol for transmission of IPv6 packets over LoWPAN. LoWPAN contains a vast amount of resource constrained devices that are connected over a wireless link to assemble real-time information and transfer it to the chosen application. Only 28 bytes of the actual payload are left in large-sized headers like IPv6, TCP, and UDP. IEEE 802.15.4 uses MTU only 127 bytes whereas the IPv6 packet uses 1280 bytes. Therefore header compression and fragmentation are essential in 6LoWPAN to deliver a fair number of bits for payload. The author describes the different header compression techniques for compressing the IPv6 header. Comparison is based on the techniques on the total number of bits getting compressed under different methods.

IPv6 in a LoWPAN requires careful application and needs to concentrate on limited bandwidth, memory, and energy resources in (Ludovici *et al.*, 2009). Using 6LoPWAN protocol describes how to maintain IPv6 packets over IEEE 802.15.4. IEEE 802.15.4 uses only 102 bytes out of MTU 127 bytes due to overhead. An additional reduction is due to security, network, and transport protocols header overhead. Only 33 bytes are used by IPv6 and UDP for application data. Usage of compression algorithms is very important to decrease the overhead and save more space in the data payload. Therefore the author has compared the proposed IPv6 header compression mechanisms for 6LoWPAN.

In RFC 8724 Minaburo *et al.* (2020) mentioned SCHC is presented mentioning generic structure for header compression and fragmentation. In Gomez and Minaburo (2022), the SCHC compresses packets over IEEE 802.15.4 networks technique is presented. It mentions that both star and mesh topology can be considered for Static Context Header Compression (SCHC) over IEEE 802.15.4. However, for the IPv6 address compression, it refers to the address compression technique provided in RFC 8724Minaburo *et al.* (2020), in section 10. It mentions that the address fields are compressed based on prefix and Network Identifier (IID). Both source and destination addresses must be configured with appropriate prefixes. If the Rule is intended to compress packets with different prefix values, match-mapping needs to be used. If the Device IID is based on an L2 address, then the IID can be reconstructed with SCHC information coming from the L2 header. It also mentions that in case of sending IID entirely, then the rules are not set and the value of IID is sent in a packet. Further compression of addresses is also applicable to SCHC when the IPv6 address is sent entirely or only prefixes or IID of 64 bits need to be sent with appropriate Rule Identifier.

4.2 Header Compression Techniques in 6LoWPAN

Low power Wireless Personal Area Networks(LoWPAN) comprises devices that have lower capacities in terms of bit rate and power, in order to support low cost devices. The protocol stack of the 6LoWPAN adaptation layer is as shown in Figure 4.1. LoWPAN has three variants : Simple, Adhoc, Extended. Simple LoWPANs are the ones that are connected to the Internet via an edge router. Adhoc LoWPANs are standalone types of devices which are not connected to the internet. Extended type of LoWPAN is interconnecting multiple simple LoWPAN with multiple edge routers. LoWPAN has different variants of devices : 1)Personal Area Network (PAN) coordinator, which are normally non-mobile and have responsibility to create, coordinate and maintain the network, 2)Reduced Function Devices(RFD), which are simple devices used to sense and forward data, 3)Fully Function Devices(FFD), which has routing capacity along with sensing and forwarding data. PAN coordinators are having fully functional features.

To understand the concept of need for header compression in 6LoWPAN, let's consider a scenario in which a LoWPAN device sends a sensor value to the cloud. Assume that the Constrained Application Protocol(CoAP) is used for data communication. CoAP considers a fixed size of 4-byte header followed by variable-length token value of 0-8 bytes. Token value is followed by 0 or more option fields followed by payload. Assume that the payload is about 8 bytes in size and the token is 8 bytes. In this example, total CoAP packet size becomes 4 bytes Header + 8 bytes token and 8 bytes of payload = 20 bytes. In the transport layer, UDP adds 8 bytes of header. In the network layer, the IPv6 header adds 40 bytes. So, total number of bytes in IPv6 packet is 40 bytes of IPv6 header, 8 bytes of UDP header and 20 bytes of CoAP packet=68 bytes According to IEEE 802.15.4 MAC header, the PHY layer provides 127 bytes for payload. Out of 127 bytes, 60 bytes are occupied by COAP (12 bytes), UDP (8 bytes) and IPv6 header (40 bytes) that leaves 67 bytes for the actual data and lower layer headers. IEEE 802.15.4 MAC header is 25 bytes in size and Link Layer security overhead would be 21 bytes (Considering AES-CCM-128bit). Now the final overhead bytes is 21(AES-128)+25(802.15.4 MAC header)+40(IPv6 header)+8(UDP header)+12 (CoAP Header and token)=106 bytes. This leaves only 21 bytes for the actual payload.

If the data is considered in IEEE floating point notation, it means 2.6 floating point values or only two floating point numbers can be sent in payload. The calculation with this example shows overhead posed by the headers added to the actual data. One possible and feasible solution is to reduce the header overhead by performing header compression. The information in the IEEE 802.15.4 header can be well utilized to derive some redundant fields in the upper layer headers. Hence redundant information can be elided and compressed. Another major concern in 6LoWPAN with respect to IPv6 is with respect to minimum MTU of 1280 bytes which is fixed to avoid low MTU links that result in overall inefficiency in the network. As IPv6 follows end-to-end fragmentation and reassembly, intermediate hops do not do any fragmentation of the packet. Compared to 21 bytes of data supported by IEEE 802.15.4, MTU of IPv6 with 1280 bytes is clearly much larger for transmission. Hence, 6LoWPAN provides header compression techniques to provide more number of bits available to payload at lower layers.

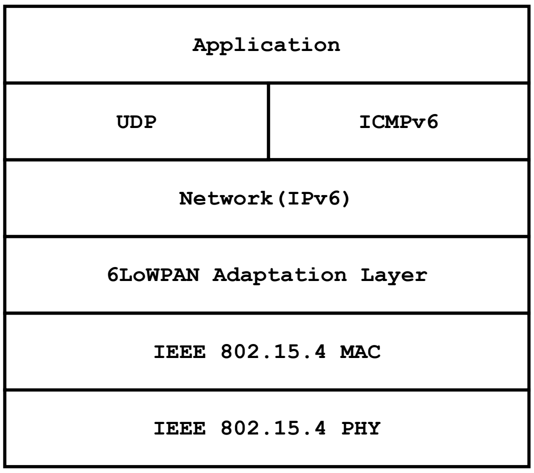


Figure 4.1: 6LoWPAN Protocol Stack

Figure 4.2: 6LoWPAN Encapsulation

The 6LoWPAN encapsulation of packet is as shown in figure 4.2. The values of Dispatch byte and their description are as follows:

1. 00 xxxxxx : NALP - Not a LoWPAN frame

2. 01 000001 : IPv6 - Uncompressed IPv6 Addresses

3. 01 000010 : LOWPAN_HC1-IPv6 Header Compression - stateless
4. 01 010000 : LOWPAN_BC0 - Broadcast
5. 01 1xxxxx : LOWPAN_IPHC - IPv6 Header Compression - context based
6. 01 111111 : ESC - Additional Dispatch byte follows
7. 10 xxxxxx : Mesh Header
8. 11 000xxx : FRAG1 - Initial fragment
9. 11 1100xx : FRAGN - Subsequent fragments

The dispatch value for stateless header compression is 01000010 and for context based header compression is 011xxxxx. The subsections 4.2.2 and 4.2.3 explains the stateless header compression and context based header compression in detail.

4.2.1 Stateless Header Compression

There are two Header Compression techniques defined in 6LoWPAN:

1. Stateless Header Compression
2. Context Based Header Compression.

4.2.2 Stateless Header Compression

Stateless Header compression is also called HC1 and HC2 header compression Kushalnagar *et al.* (2007*a*). HC1 header compression compresses the IPv6 Header with respect to the fields which can be elided and derived from other layers. It does not consider compressing multicast or global IPv6 addresses. Stateless header compression also provides provision for compressing UDP header and it is called HC2 header compression. The compression technique is called stateless, as it does not intend to store any state or flow information at the hops along the path towards destination, The routing protocols selects the route to destination with no effect on the compression efficiency. Another benefit of stateless header compression is that it is a simplified algorithm and there is no requirement for any kind of synchronization.

The field of stateless header compression is shown in figure 4.3. Eight bit dispatch bits indicate that it is stateless header compression. As part of HC1 header compression, Source Address (SA) and Destination Address (DA) encoding bits indicates whether the 128 bit address is inline with the packet (00), whether IID is elided as it can be derived from MAC address (01), whether prefix can be elided as the source and destination are part of the same network (10) and whether both prefix and IID can be elided and can be derived from other layers (11). Traffic Class and Flow label (TF) indicates whether the content of this field is zero (TF=1) or not (TF=0). Most of the time the packet within an IPv6 packet is UDP, ICMP or TCP. Hence instead of using 8 bits for the next header (NH), it can be compressed to 2 bits. HC2 header compression compresses the UDP header. If the source and destination port addresses are within the range (61616-61631), the port bits are compressed to 5 bits from 16 bits. If length field information can be obtained from lower layers then Length field is elided (L=1). With stateless header compression, in best case, HC1 header compression compresses 289 bits (source address, destination address, Traffic flow and next header), and HC2 compression technique compresses 38 bits (Source port, destination port and length). So, in the best case scenario, the stateless header compression provides 289+38=327 bits or 40 bytes of compression.

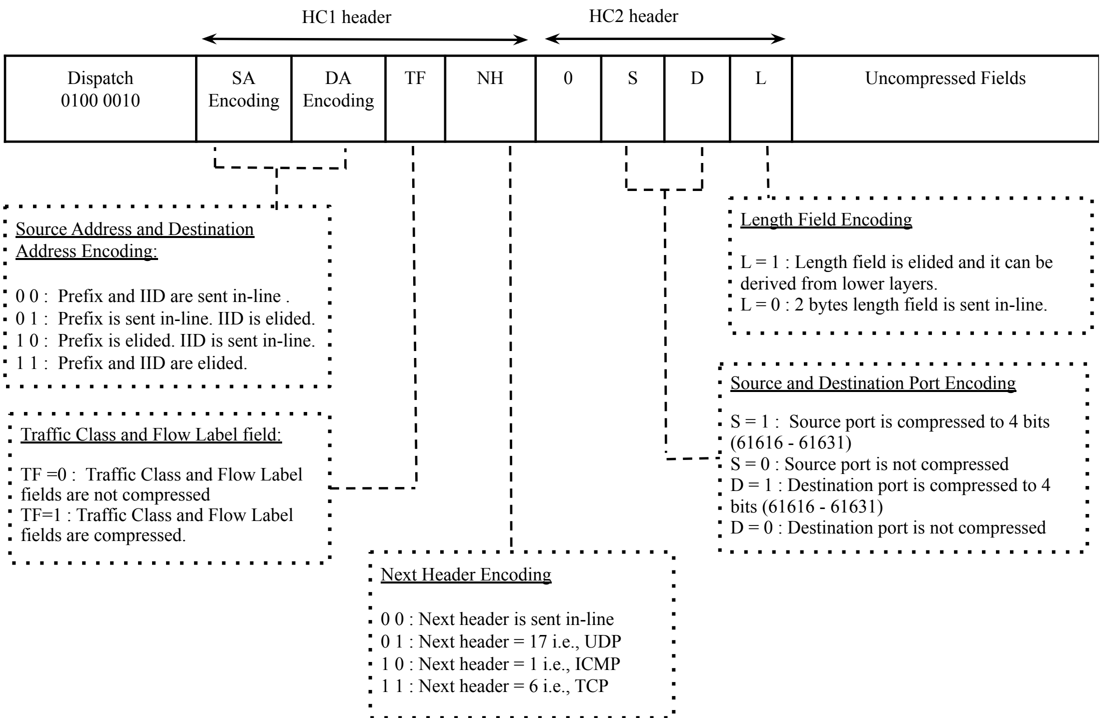


Figure 4.3: Stateless Header Compression

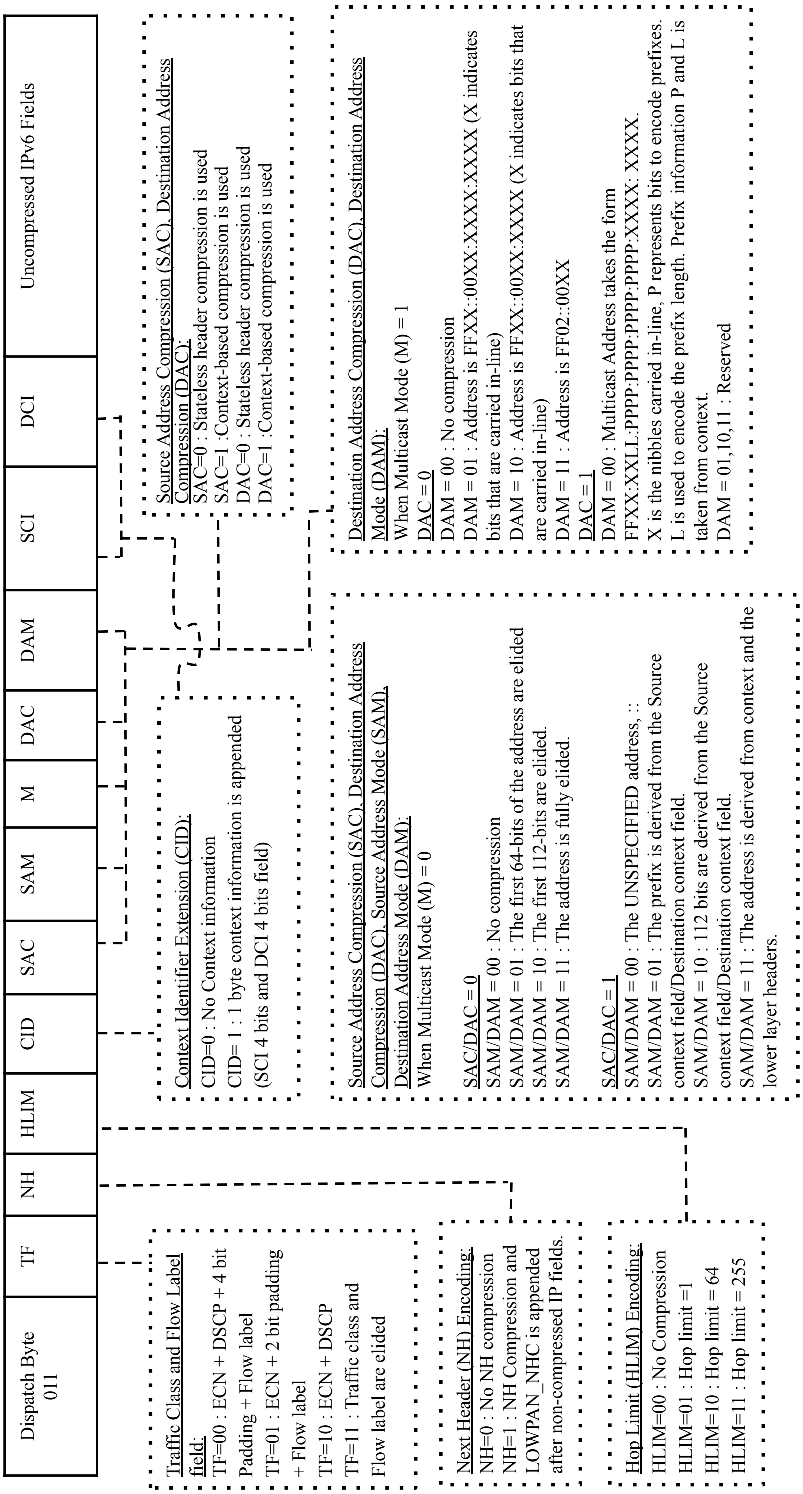


Figure 4.4: Context based Header Compression

4.2.3 Context based Header compression

RFC 6282, Hui *et al.* (2011) provides compression format for IPv6 packet based on shared context to allow compression of arbitrary prefixes. The context based header compression format is as shown in figure 4.4. The Dispatch byte with '011' indicates context based header compression. Two bits are used to compress the Traffic class and Flow label (TF). The Next Header(NH) compression is present or not indicated by one bit. Hop Limit (HLIM) is compressed to indicate inline, 1, 64, or 255 using two bits. One bit Context Identifier Extension (CID) is used to indicate whether an additional 8 bit context CID is used or not. One bit SAC indicates whether source address compression is stateless or context based. Two bit source address Mode (SAM) specifies the number of address bits compressed based on SAC. Whether the destination is a multicast address or not is specified by one bit M. Whether Destination Address Compression (DAC) is stateless or context based is specified by Destination Address Mode(DAM). If CID value is set to '1' then additional octet is considered with Source Context Identifier (SCI) and Destination Context Identifier (DCI). After this uncompressed field of the IPv6 packet follows the compressed header.

4.3 Proposed IPv6 Address Compression for 6LoWPAN Header

In this section, header compression based on IPv6 address is proposed. In Stateless header compression of IPv6 over 6LoWPAN, the header bits are compressed in order to accommodate more number of payloads in the MAC frame. The HC1 header compression considers compression of Source address and destination address. Two bits are used to represent address compression status:

- 00 – Prefix is uncompressed and IID is uncompressed
- 01 – Prefix is compressed and IID is derived from L2
- 10 – Prefix is FE80::/80 and IID is uncompressed
- 11 – Prefix is FE80::/64 and IID is derived from L2

In this case, when the address status is 00, then prefix and IID are not compressed. If source address and destination address both are uncompressed then total 256 bits are required for address in one IPv6 packet. Hence, we propose a further compression of addresses at address fields by considering other parameters of the address such as the number of zeros present in the address. The compression rate depends on the number of zeros present in the address.

The IPv6 address contains a total 128 bit address for source and destination address as follows:
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX where each X represents a digit in hex value.
The 6LoWPAN stateless header compression performs address compression of source and destination addresses as follows:

- If the address can not be compressed then the SA/DA bit is represented as 00 and the complete 128 bit address is mentioned inline in the packet.
- If the IID can be obtained from MAC address, then SA/DA bits are mentioned as 01 and IID is elided. Only the upper 64 bit prefix is specified in the packet.
- If source and destination addresses are in the same LoWPAN network, then SA/DA bits are mentioned as 10 and prefix is elided and only lower 64 bit IID is specified in the packet.
- If the source and destination are in the same LoWPAN network and IID can be obtained from MAC address, then SA/DA bits are mentioned as 11 and both prefix and IID are elided. No address is specified in the network.

However, many times the IP address contains continuous zeroes. Hence, the address compression techniques to compress the continuous zeroes in the address helps to reduce the number of bits in the 6LoWPAN packet by providing extra bits to send payload in the MAC frame. Hence, address compression technique to compress continuous zeroes is proposed in following subsections.

4.3.1 Proposed Double Colon based Address Compression Technique

The IPv6 address size is 128 bits. The preferred IPv6 address representation is as follows:
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX,
where each X is a hexadecimal value of the eight 16-bit pieces of the address.
The range of IPv6 addresses are as follows:

0000:0000:0000:0000:0000:0000:0000:0000 to
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
In addition to this preferred format, IPv6 addresses might be specified in two other shortened formats:

1. Omit leading zeros : Specify IPv6 addresses by omitting leading zeros. For example, IPv6 address 10a0:0000:0000:0000:0007:0600:300c:646b can be written as 10a0:0:0:0:7:600:300c:646b.

2. Double colon : Specify IPv6 addresses by using double colons (::) in place of a series of zeros. For example, IPv6 address ff07:0:0:0:0:0:0:b4 can be written as ff07::b4. Double colons can be used only once in an IP address.

Among these two techniques, the double colon method can be used to compress the address in 6LoWPAN network as shown in Figure 4.5. Extra 7 bits are used to identify the position of the double colon (::) in the address. The field SCm indicates whether Source address double colon compression is performed or not (1/0). The field SCn indicates double colon position in multiples of 16 bits. The SCz indicates the total number of leading zeros in terms of 16 bit blocks. Similarly, DCm indicates destination double colon compression is performed or not (1/0). The field DCn indicates double colon position in multiples of 16 bits. The field DCz indicates total number of leading zeros in terms of 16 bit blocks.

The address compression of IPv6 using double colon Technique is as follows: Consider the following source address (SA) and destination address(DA).
SA: $2001:0000:0000:FE01:0000:0000:0000:0000$
DA: $2001:0000:0000:B345:0000:0000:0000:0000$
According to stateless header compression (HC1), the SA and DA bits becomes 0000 as the 128 bit cannot be further compressed. Hence the complete $128+128=256$ bit address will be specified in the packet.
In the case of the proposed double colon address compression technique, SCm is indicated as 1, to represent double colon source address compression. $SCn = 100$, which indicates that double colon is represented after the 4th set of 16bit address portions. $SCz = 011$ which indicates that the total number of leading zeroes are $(3 + 1) * 16 = 64 bits$. $SCm = 1$, $SCn = 100$, $SCz = 011$. Hence, the source address double colon compressed address becomes $2001 : 0000 : 0000 : FE01 ::$ Similarly, DCm is indicated as 1, to represent double colon destination address compression. $DCn = 100$, which indicates that double colon is represented after the 4th set of 16 bit address portions. $DCz = 011$ which indicates that the total number of leading zeroes are $(3 + 1) * 16 = 64 bits$. $DCm = 1$, $DCn =$

100, $DCz = 011$. Hence, the destination address after double colon compression becomes $2001 : 0000 : 0000 : B345 ::$

The proposed double colon compression technique provides Best case Compression of 128 bits with overhead of 7 bits and worst case with no compression and overhead of one bit SCm/DCm to indicate that double colon based compression is not performed.

Dispatch 01000010	SA (2)	DA (2)	TF (1)	NH (2)	0	S (1)	D (1)	L (1)	SCm (1)	SCn (3)	SCz (3)	DCm (1)	DCn (3)	DCz (3)	Uncompressed Fields

Figure 4.5: Proposed Double Colon Address Compression for Stateless Header Compression

Dispatch 011	TF (2)	NH (1)	HLIM (2)	CID (1)	SAC (1)	SAM (2)	M (1)	DAC (1)	DAM (2)	SCm (1)	SCn (3)	SCz (3)	DCm (1)	DCn (3)	DCz (3)	Uncompressed Fields

Figure 4.6: Proposed Double Colon Address Compression for Context based Header Compression

In case of context based header compression technique, $SAC/DAC = 1$ and $M = 0$ indicates context based address compression. In this case when $SAC/DAC = 1$ and $SAM/DAM = 00$, the uncompressed address is specified inline. Similarly, when the $DAC = 0, M = 1$ and $DAM = 00$, multicast address is uncompressed. In both these cases, the address can be verified for the number of leading zeroes and compressed according to double colon based address compression. The overhead bits or control bits for address compression is as shown in Figure 4.6.

4.3.2 Bit Pattern Based Address Compression Technique

The proposed double colon based address compression performs compression of leading zeroes only once in the source or destination address. For example, source address $2001 : 0000 : 0000 : FE01 : 0000 : 0000 : 0000 : 0000$ and Destination address $2001 : 0000 : 0000 : B345 : 0000 : 0000 : 0000 : 0000$
is compressed as $2001 : 0000 : 0000 : FE01 ::$ and
$2001 : 0000 : 0000 : B345 ::$ respectively by considering longest leading zeroes as (::) colon can be represented only once in the address. But, the compressed address still contains leading zeroes. Hence, to overcome drawback of double colon based compression, Bit pattern based address compression technique is proposed. The compression of leading zeros in the address is performed as shown in figure 4.7. The IPv6 address can be represented as group of 16 bits as follows:

$ADDR7 : ADDR6 : ADDR5 : ADDR4 : ADDR3 : ADDR2 : ADDR1 : ADDR0$ The address groups are also shown in figure 4.7.

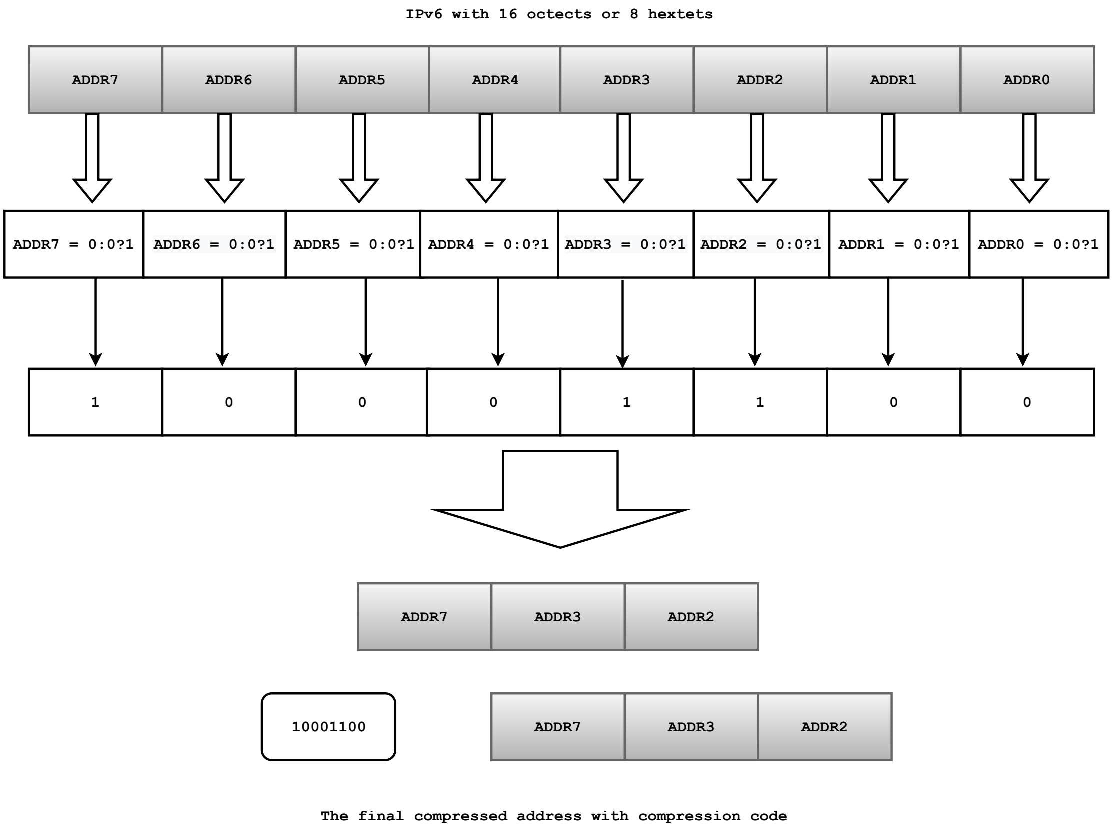


Figure 4.7: Bit Pattern based Address Compression

A parallel compactor can be implemented to check whether the hextets are equal to 0 ($ADDR == 0$) or not. If the hextet value is equal to '0' then the compression control bit is considered as 0, otherwise the bit is represented as 1. Based on this bit pattern, only the non zero hextet is considered as an address and all hextet which are zero are elided. For example, consider source address (SA) and Destination Address (DA) as follows:
SA $2001 : 0000 : 0000 : FE01 : 0000 : 0000 : 0000 : 0000$ and
DA $2001 : 0000 : 0000 : B345 : 0000 : 0000 : 0000 : 0000$
According to bit pattern based address compression the control bits for source address is 10010000 and the compressed source address is $2001 : FE01$. Similarly, the control bit for destination address is 10010000 and compressed destination address is $2001 : B345$.

At receiver side, the node scans the control bits from MSB to LSB, and attaches hextet from compressed address if control bit is 1 and attaches hextet with zeroes if the control bit is zero.

Bit pattern based technique can be used both in stateless header compression as well as context based header compression.

4.4 Results and Discussion

The proposed techniques are analysed as follows.

1. Based on certain case studies by considering few IPv6 addresses
2. Based on SCHC header Compression with proposed technique
3. Based on Multipoint to Point communication using cooja simulator

4.4.1 Based on Certain Case Studies by Considering Few IPv6 Addresses

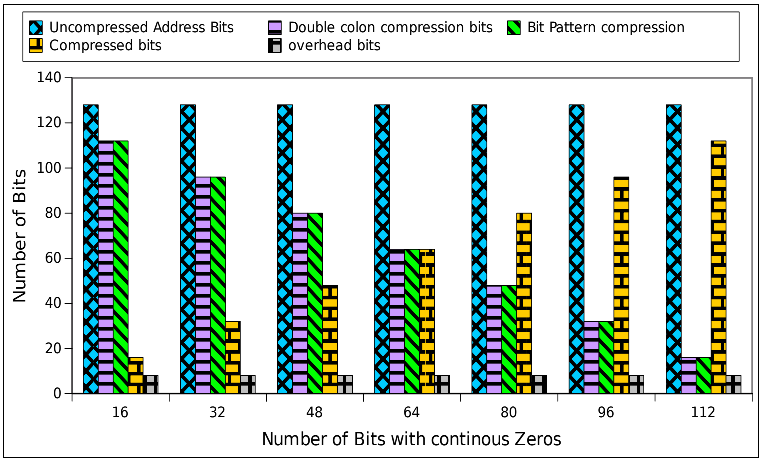


Figure 4.8: Proposed Double Colon Address and Bit Pattern based Address Compression

To compare the proposed compression techniques, some examples of addresses with leading zeroes are considered as tabulated in Table 4.1. In all these cases, if stateless address compression is used, the SA/DA bit will be 00, indicating the address is inline and not compressed, which indicates, all 128 bits will be inline in the header. The comparative analysis shows that the double colon address compression and Bit pattern based address compression techniques compresses the leading zeroes in the IPv6 address. Both techniques compress the same amount of bits if the leading zeroes are continuous. However, if the leading zeroes are not continuous, then the bit pattern based compression provides a better compression

Table 4.1: Analysis of Proposed Double Colon Address and Bit Pattern based Address Compression

				Double Colon based IPv6 Address Compression				**Bit pattern based IPv6 Address Compression**			
Case	No. of Leading Zeroes	IPv6 address format	SA/DA bits in stateless Header Compression	Double colon based address Compression control bits	Compressed address pattern	Total overhead (Bits)	Total Compressed (Bits)	Bit Pattern based address Compression control bits	Compressed address pattern	Total overhead (Bits)	Total Compressed (Bits)
When Number of leading zeroes are in consecutive locations											
1	0	x:x:x:x:x:x:x:x	00	Scm/Dcm=0	x:x:x:x:x:x:x:x	1	0	11111111	x:x:x:x:x:x:x:x	8	0
2	16	x:x:x:x:x:x:x:0	00	Scm/Dcm=1	x:x:x:x:x:x:x::	7	16	11111110	x:x:x:x:x:x:x::	8	16
3	32	x:x:x:x:x:x:0:0	00	Scm/Dcm=1	x:x:x:x:x:x::	7	32	11111100	x:x:x:x:x:x::	8	32
4	48	x:x:x:x:x:0:0:0	00	Scm/Dcm=1	x:x:x:x:x::	7	48	11111000	x:x:x:x:x::	8	48
5	64	x:x:x:x:0:0:0:0	00	Scm/Dcm=1	x:x:x:x::	7	64	11110000	x:x:x:x::	8	64
6	80	x:x:x:0:0:0:0:0	00	Scm/Dcm=1	x:x:x::	7	80	11100000	x:x:x::	8	80
7	96	x:x:0:0:0:0:0:0	00	Scm/Dcm=1	x:x::	7	96	11000000	x:x::	8	96
8	112	x:0:0:0:0:0:0:0	00	Scm/Dcm=1	x::	7	112	10000000	x::	8	112
9	128	0:0:0:0:0:0:0:0	00	Scm/Dcm=1	::	7	128	00000000	::	8	128
When Number of leading zeroes are not in consecutive locations											
10	16,16	x:0:x:x:x:x:x:0	00	Scm/Dcm=1	x:0:x:x:x:x:x::	7	16	10111110	x:x:x:x:x:x	8	32
11	32,32	x:0:0:x:x:x:0:0	00	Scm/Dcm=1	x:0:0:x:x:x::	7	32	10011100	x:x:x:x	8	64
12	32,48	x:0:0:x:x:0:0:0	00	Scm/Dcm=1	x:0:0:x:x:	7	48	10011000	x:x:x	8	80
13	32,64	x:0:0:x:0:0:0:0	00	Scm/Dcm=1	x:0:0:x::	7	64	10010000	x:x	8	96
When Number of leading zeroes are in the middle of the address											
14	64	x:0:0:0:0:x:x:x	00	Scm/Dcm=1	x::x:x:x	7	64	10000111	x:x:x:x	8	64
15	80	x:0:0:0:0:0:x:x	00	Scm/Dcm=1	x::x:x	7	80	10000011	x:x:x	8	80

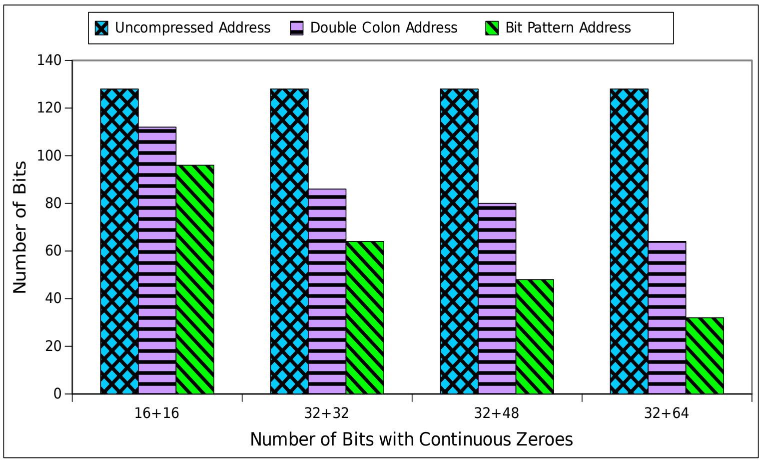


Figure 4.9: Proposed Double Colon Address and Bit Pattern based Address Compression

rate. The comparison of total compression and overhead bits with respect to uncompressed addresses is shown in Figure 4.8. The results show that the number of compressed bits for proposed double colon address and bit pattern address compression are the same. But the number of address bits compressed as the number of leading zeroes increases is more compared to uncompressed addresses. The benefit of the bit pattern based compression can be observed in Figure 4.9. The figure shows the number of bits in the address when the address is uncompressed, compressed with double colon compression techniques and compressed with bit pattern techniques. When the number of leading zeroes are not contiguous like 16 bit contiguous zeroes at one side and another 16 bit contiguous zeros in other side which is represented as 16+16, the double colon based compression compresses only the sub sequence of leading zeros which contains large number of zeroes. For example, if 16 bit and 32 bit zeroes are contiguous, but as two different subsequences, then as 32 is greater than 16, and double colon can be considered only once in the address, and hence, only 32 bits are compressed. However, in the case of bit pattern based compression technique, $16 + 32 = 48$ bits gets compressed.

4.4.2 Based on SCHC Header Compression with Proposed Address Compression

The RFC 8724 Minaburo *et al.* (2020) provides details on SCHC format for header compression and fragmentation and Gomez and Minaburo (2022) provides the details on SCHC compresses packets over IEEE 802.15.4 networks. The SCHC header compression technique is mainly based on RuleID formation which pro-

Table 4.2: Rule 1: SCHC Mode 0: Global Communication

Rule1: SCHC Global Communication						
IPv6 Field	**FP**	**FL**	**DI**	**TV**	**MO**	**C/D**
Version	1	4	Bi	6	Equal	Elided
Traffic Class	1	8	Bi	0	Equal	Elided
Flow label	1	20	Bi	0	Ignore	Elided
Payload Length	1	16	Bi	None	Ignore	Elided
Next header	1	8	Bi	17	Equal	Elided
Hop Limit	1	8	Bi	32	Ignore	Elided
Prefix of Source	1	64	Bi	None	Value	Send
IID of Source	1	64	Bi	None	Value	Send
Prefix of Destination	1	64	Bi	None	Value	Send
IID of Destination	1	64	Bi	None	Value	Send

Table 4.3: Rule 2: SCHC Mode 1: Global Communication with IID Elided

Rule2: SCHC Global Communication						
IPv6 Field	**FP**	**FL**	**DI**	**TV**	**MO**	**C/D**
Version	1	4	Bi	6	Equal	Not Sent
Traffic Class	1	8	Bi	0	Equal	Not Sent
Flow label	1	20	Bi	0	Ignore	Not Sent
Payload Length	1	16	Bi	None	Ignore	Not Sent
Next header	1	8	Bi	17	Equal	Not Sent
Hop Limit	1	8	Bi	32	Ignore	Not Sent
Prefix of Source	1	64	Bi	None	Value	Send
IID of Source	1	64	Bi	None	Compute	Elided
Prefix of Destination	1	64	Bi	None	Value	Send
IID of Destination	1	64	Bi	None	Compute	Elided

Table 4.4: Rule 3: SCHC Mode 2: Local Communication with Prefix Elided

Rule3: SCHC Local Communication						
IPv6 Field	**FP**	**FL**	**DI**	**TV**	**MO**	**C/D**
Version	1	4	Bi	6	Equal	Not Sent
Traffic Class	1	8	Bi	0	Equal	Not Sent
Flow label	1	20	Bi	0	Ignore	Not Sent
Payload Length	1	16	Bi	None	Ignore	Not Sent
Next header	1	8	Bi	17	Equal	Not Sent
Hop Limit	1	8	Bi	32	Ignore	Not Sent
Prefix of Source	1	64	Bi	Address	Equal	Elided
IID of Source	1	64	Bi	None	Value	Send
Prefix of Destination	1	64	Bi	Address	Equal	Elided
IID of Destination	1	64	Bi	None	Value	Send

Table 4.5: Rule 4: SCHC Mode 3: Local Communication with Prefix and IID Elided

Rule4: SCHC Local Communication						
IPv6 Field	**FP**	**FL**	**DI**	**TV**	**MO**	**C/D**
Version	1	4	Bi	6	Equal	Not Sent
Traffic Class	1	8	Bi	0	Equal	Not Sent
Flow label	1	20	Bi	0	Ignore	Not Sent
Payload Length	1	16	Bi	None	Ignore	Not Sent
Next header	1	8	Bi	17	Equal	Not Sent
Hop Limit	1	8	Bi	32	Ignore	Not Sent
Prefix of Source	1	64	Bi	Address	Equal	Elided
IID of Source	1	64	Bi	None	Compute	Elided
Prefix of Destination	1	64	Bi	Address	Equal	Elided
IID of Destination	1	64	Bi	None	Compute	Elided

Table 4.6: Rule 5: SCHC_DC Mode 0: Global Communication

Rule5: SCHC_DC Global Communication						
IPv6 Field	**FP**	**FL**	**DI**	**TV**	**MO**	**C/D**
Version	1	4	Bi	6	Equal	Not Sent
Traffic Class	1	8	Bi	0	Equal	Elided
Flow label	1	20	Bi	0	Ignore	Elided
Payload Length	1	16	Bi	None	Ignore	Elided
Next header	1	8	Bi	17	Equal	Elided
Hop Limit	1	8	Bi	32	Ignore	Elided
Source DC Code	1	8	Bi	None	Value	Send
Prefix of Source	1	V	Bi	None	Compute	Send
IID of Source	1	V	Bi	None	Compute	Send
Destination DC Code	1	8	Bi	None	Value	Send
Prefix of Destination	1	V	Bi	None	Compute	Send
IID of Destination	1	V	Bi	None	Compute	Send

Table 4.7: Rule 6: SCHC_BC Mode 0: Global Communication

Rule6: SCHC_BC Global Communication						
IPv6 Field	**FP**	**FL**	**DI**	**TV**	**MO**	**C/D**
Version	1	4	Bi	6	Equal	Not Sent
Traffic Class	1	8	Bi	0	Equal	Elided
Flow label	1	20	Bi	0	Ignore	Elided
Payload Length	1	16	Bi	None	Ignore	Elided
Next header	1	8	Bi	17	Equal	Elided
Hop Limit	1	8	Bi	32	Ignore	Elided
Source BC Code	1	8	Bi	None	Value	Send
Prefix of Source	1	V	Bi	None	Compute	Send
IID of Source	1	V	Bi	None	Compute	Send
Destination BC Code	1	8	Bi	None	Value	Send
Prefix of Destination	1	V	Bi	None	Compute	Send
IID of Destination	1	V	Bi	None	Compute	Send

vides details about each field and compression/decompression strategies. Based on communication types such as global/local communication, the SCHC RuleID are designed and explained in tables 4.2 to 4.5. The different fields of the IPv6 header are listed in the table along with the information of whether the value is sent along with the packet or elided. Each RuleID contains the information about FieldID (FID) of the packet which is unique for the protocol and the field. Field Length (FL) represents the length of the original field. Field Position (FP) represents the position of the specified field in the packet. Default value of FP is 1. Direction Indicator (DI) represents the direction of communication (Up, Down or Bidirectional). Target Value (TV) is the value used to match against the header field. Matching Operator (MO) is the operator used to match the field value and the target value. Compression/Decompression Action (C/D) describes the actions that are to be performed for compression or decompression.

Table 4.2 contains the details of a SCHC rule (Rule 1) for Global Communication with the internet which is similar to Mode 0 of HC1 compression. Version value of IPv6 is 6 and hence the MO is mentioned as Equal and the value is elided in the packet. Traffic class and flow labels are also elided. Payload length can be calculated from other layer headers, hence it is elided. Most of the time the next header is UDP, hence value 17 can be assigned. For different next header values either we can set different RuleID or we can use mapping index operation for identifying the next header. Hop limit can be considered fixed or mapping index based. In this case, the hop limit is considered with value 32. One of the major parts of the IPV6 header is representation of addresses. HC1 header compression of 6LoWPAN uses four different modes for identifying compression of prefixes and IID. To represent the same, the prefix and IID field of source address are represented separately in RuleID for source address and Destination address namely, prefix of Source (64 bit) and IID of Source (64 bit), Prefix of Destination (64 bit) and IID of Destination (64 bit). In case of Rule 1 with Mode 0, all the fields are elided except for the source and destination IPv6 addresses. Both the prefix and IID of an IPv6 address are sent uncompressed in the frame. Hence, size of the IPv6 packet gets compressed to 17 bytes with one byte RuleID and 8+8=16 bytes for address (128 bit source address and 128 bits destination address).

Mode 1, 2 and 3 are shown in table 4.3 to 4.5, which is similar to mode 0 as shown in Table 4.2, but some of the address fields gets elided based on Global or local communication and whether IID can be inferred from MAC address. In RuleID 2, 4.3, the type of the communication is Global communication with Internet, but the IID can be inferred from MAC address, hence the source and Destination IID can be elided and only prefix of the source and destination address is sent in the packet header. Hence, the size of the IPv6 packet gets compressed to 9 bytes with one byte RuleID and 4+4=8 bytes for address (64 bit source address and 64 bits destination address). In RuleID 3, 4.4, the type of the communication is Local communication without connecting to the Internet, hence the prefix of source address and destination can be elided. Only IID of the source and destination address is sent in the packet header. Hence, the size of the IPv6 packet gets compressed to 9 bytes with one byte RuleID and 4+4=8 bytes for address (64 bit source address and 64 bits destination address). In RuleID 4, 4.5, the type of the communication is Local communication without connecting to the Internet. Here, prefix of the source and destination address can be elided as the communication is in the same network and the IID can be inferred from MAC address. Hence the complete address gets elided and size of the IPv6 packet gets compressed to 1 byte.

The RuleID 1 to 3 of SCHC shows that at certain conditions 128 bits address or 64 bit address will be sent along with the packet as it is not further compressed. The proposed Double colon address compression and Bit pattern based address compression can be incorporated in SCHC to further reduce the number of bits to be transmitted. Table 4.6 shows RuleID for SCHC for proposed double colon based address compression (SCHC_DC). Rule 5 is similar to Rule1 with Mode 0, along with address compression. Hence two different fields are added to RuleID, namely Source DC code and Destination DC code with one byte for each as mentioned in Figure 4.5 and 4.6. Since the leading zeroes get compressed, the number of bytes get varied , hence the Field value is mentioned as Variable (V) and the Mode of Operation is Compute to compute the actual address based on DC code and corresponding address sent in the packet. The Rule 5 which is SCHC_DC can be extended to Mode 1 and 2 by performing operation to compress based on prefix or IID elided. SCHC_DC for Mode 3 is same as SCHC Mode 3 as the complete address gets elided.

Table 4.7 shows RuleID for SCHC for proposed bit pattern based address compression (SCHC_BC). Rule 5 is similar to Rule1 with Mode 0, along with address compression. Hence two different fields are added to RuleID, namely Source BC code and Destination BC code with one byte for each as mentioned in Figure 4.7. Since the leading zeroes get compressed, the number of bytes get varied , hence the Field value is mentioned as Variable (V) and the Mode of Operation is Compute to compute the actual address based on source and destination BC code and corresponding address sent in the packet.The Rule 5 which is SCHC_BC

Table 4.8: Comparison of HC1 and SCHC Header Compression Only for IPv6 (in Bytes) with Proposed Techniques

Modes	IPv6	HC1	HC1_DC	HC1_BC	SCHC	SCHC_DC	SCHC_BC
Mode 0	40	34	02-34	02-34	33	01-33	01-33
Mode 1	40	18	02-18	02-18	17	01-17	01-17
Mode 2	40	18	02-18	02-18	17	01-17	01-17
Mode 3	40	02	02	02	01	01	01

can be extended to Mode 1 and 2 by performing operation to compress based on prefix or IID elided. The SCHC_BC for Mode 3 and SCHC for Mode 3 are the same as the complete address gets elided.

The number of bytes which gets compressed in IPv6 header based on different modes and compression techniques are compared in the table 4.8. The original IPv6 packet is 40 bytes. HC1 compression takes 2 bytes for representing dispatch and HC1 header. For Mode 0, assuming all other fields of the IPv6 packet are compressed except address, then the IPv6 packet gets reduced to 2+16+16=34 bytes. In mode 2 and mode 3 prefix or IID gets elided, hence packet size becomes 2+8+8=18 bytes. In mode 3 since both addresses are elided, the packet size becomes 2 bytes. HC1 with Proposed Double Colon (DC) and Bit Pattern (BC) Compression further reduces the size of the packet based on continuous zeroes present in the address. Hence the range of size of the packet is mentioned in the table 4.8. The SCHC compression technique elides most of the fields based on communication. If all fields are elided, then only RuleID of 1 byte is sent to the destination. Hence, for mode 3 only 1 byte is transferred. For mode 0, SCHC takes 33 bytes and with proposed address compression the packet size varies from range 01 to 33 bytes. For mode 1 and 2 the packet size ranges from 01 bytes to 17 bytes. SCHC provides better compression compared to HC1 and proposed double colon and bit pattern techniques further compresses the addresses based on the number of continuous zeroes.

4.4.3 Based on Multipoint-to-Point communication using cooja simulator

A multipoint-to-Point communication using RPL is considered in Cooja simulator to analyse the results of double colon based and bit pattern based communication. The simulation parameters considered are as shown in Table 4.9. The experiments are conducted for HC1 and SCHC header compression based on proposed address compression techniques.

Table 4.9: Simulation Parameter

Simulation Parameter	Values
OS	ContikiOS-ng
Radio model	Unit disk graph model
Mote type	Z1 Mote
Network size	100 m x 100 m
Application Program	Examples/ipv6/rpl-udp
Simulation time	5mins

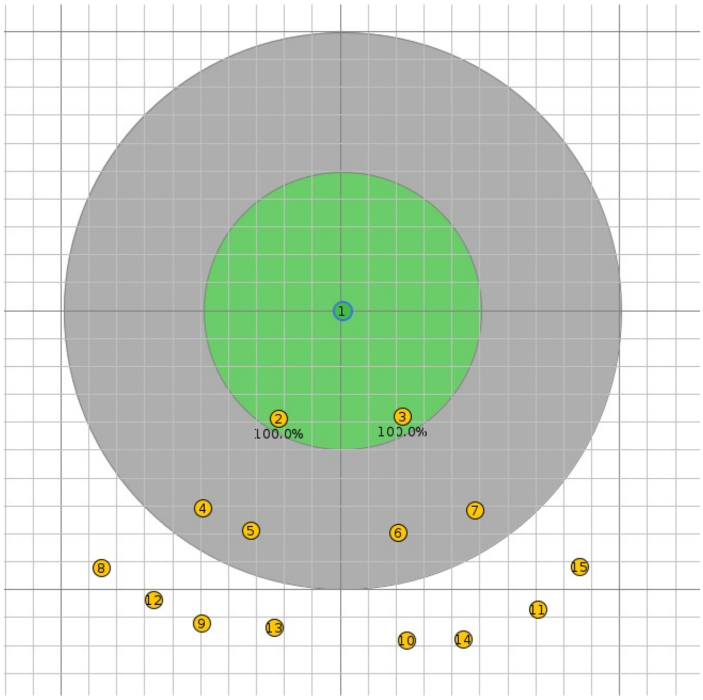


Figure 4.10: Deployment of Nodes

An experiment is run in Cooja with the topology shown in figure 4.10. The network has 15 nodes, one root node and 14 sensor nodes. The simulation is run for a varying number of leading zeroes and results are compared with HC1 and SCHC header compression and proposed double colon and bit pattern based compression techniques. The number of leading zeroes considered for simulation experiments are 0 bits, 32 bits, 64 bits and 80 bits continuously and two more conditions with 16 bit and 32 bit (16+32) and 32 bits and 48 bits(32+48) contiguous leading zeros in same address at two separate locations. The table 4.10 depicts the different header sizes in the data packet for different number of leading zeros and compressed bits with respect to HC1 and SCHC header compression with double colon based address compression and bit pattern based address compression for

Table 4.10: Number of bytes in 6LoWPAN header and SCHC header for different Compression Techniques (IPV6 Header): HC1: Stateless Header Compression, SCHC: Static Context Header Compression, DC: Double Colon Compression, BC: Bit Pattern Compression

# Continuous Zeores	HC1_M0 (Bytes)	HC1-M1 (Bytes)	HC1-M2 (Bytes)	HC1-M3 (Bytes)	SCHC-M0 (Bytes)	SCHC-M1 (Bytes)	SCHC-M2 (Bytes)	SCHC-M3 (Bytes)
0	35	19	19	3	33	17	17	1
32	35	19	19	3	33	17	17	1
64	35	19	19	3	33	17	17	1
80	35	19	19	3	33	17	17	1
16+32	35	19	19	3	33	17	17	1
32+48	35	19	19	3	33	17	17	1
# Continuous Zeores	HC1-DC-M0 (Bytes)	HC1-DC-M1 (Bytes)	HC1-DC-M2 (Bytes)	HC1-DC-M3 (Bytes)	SCHC-DC-M0 (Bytes)	SCHC-DC-M1 (Bytes)	SCHC-DC-M2 (Bytes)	SCHC-DC-M3 (Bytes)
0	35	19	19	3	33	17	17	1
32	29	13	13	3	27	11	11	1
64	21	5	5	3	21	3	3	1
80	17	5	5	3	15	3	3	1
16 + 32	29	13	13	3	27	11	11	1
32 + 48	25	9	9	3	25	7	7	1
# Continuous Zeores	HC1-BC-M0 (Bytes)	HC1-BC-M1 (Bytes)	HC1-BC-M2 (Bytes)	HC1-BC-M3 (Bytes)	SCHC-BC-M0 (Bytes)	SCHC-BC-M1 (Bytes)	SCHC-BC-M2 (Bytes)	SCHC-BC-M3 (Bytes)
0	35	19	19	3	33	17	17	1
32	29	13	13	3	27	11	11	1
64	21	5	5	3	21	3	3	1
80	17	5	5	3	15	3	3	1
16+32	25	9	9	3	21	11	11	1
32+48	17	9	9	3	15	7	7	1

Mode 0, Mode1, Mode 2 and Mode 3. The IPV6 Packet header size is 40 bytes and UDP header is 8 bytes. For simulation 30 bytes of data is considered. The results are analysed for considering all four modes: uncompressed address(mode 0), IID elided (mode 1), Prefix elided (mode 2) and both prefix and IID (mode 3) elided. The table 4.10 shows that the compression is same for the Mode 3 and mode 0 without address compression. For other cases the proposed technique provides further compression of address bytes for HC1 and SCHC.

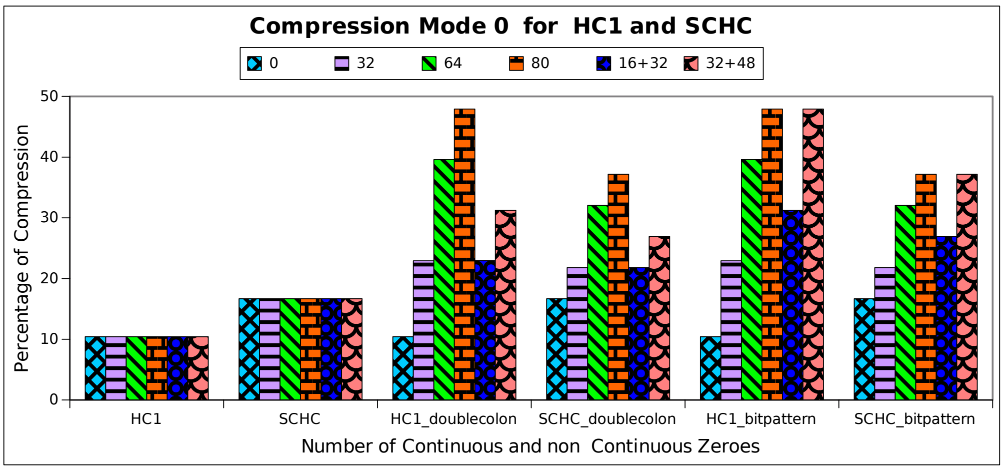


Figure 4.11: Comparison of HC1 and SCHC Mode 0 Compression Rate

The IPv6 packet contains 40 bytes header and 30 bytes of data. The header is

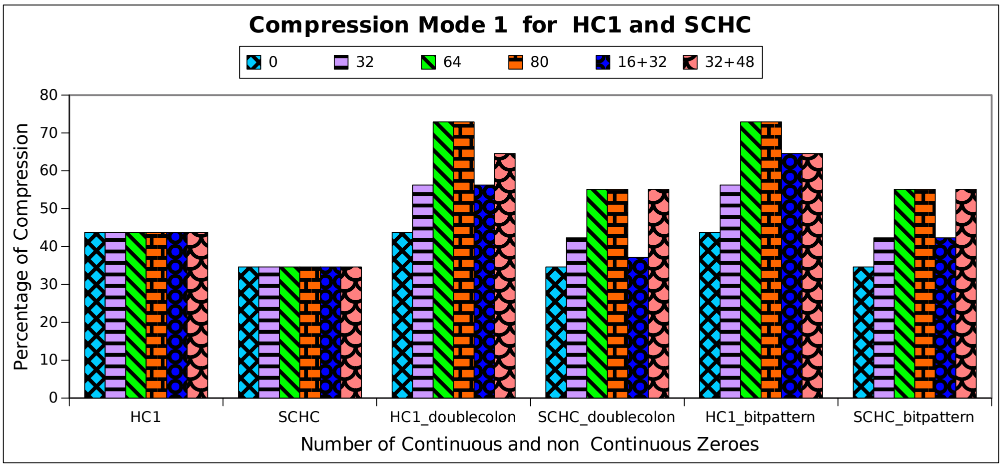


Figure 4.12: Comparison of HC1 and SCHC Mode 1 Compression Rate

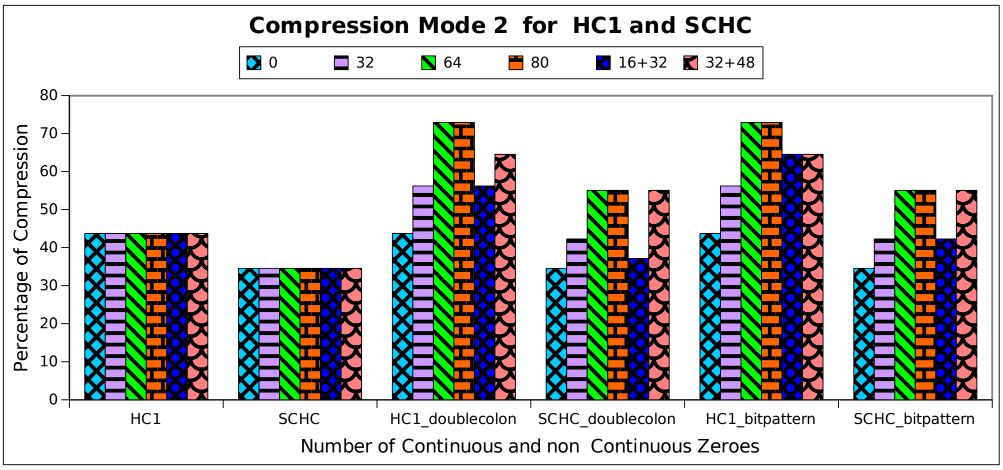


Figure 4.13: Comparison of HC1 and SCHC Mode 2 Compression Rate

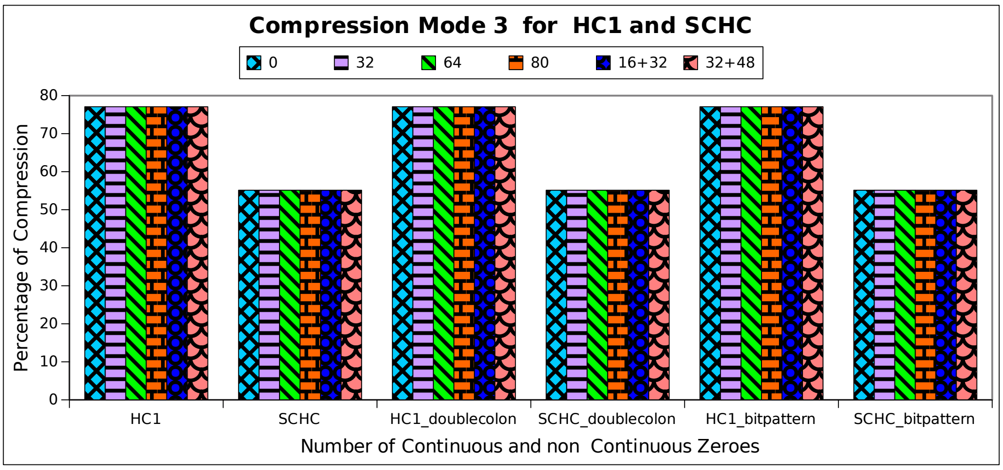


Figure 4.14: Comparison of HC1 and SCHC Mode 3 Compression Rate

compressed with HC1 header compression. The address compression is performed over HC1 compression and results are compared as shown in figures 4.11 to 4.14. In figure 4.11 , the results are shown for compression rate for Mode 0, where both addresses are specified in the header completely. The double colon as well as bit pattern based compression techniques provides better compression compared to HC1. The improvement depends on the number of continuous zeroes in the address. If X is the number of continuous zeroes and if the packet contains only the base IPv6 header, then compression rate is the percentage of X/N bits where N is the number of bits in the IPv6 Header. In Mode 0, Both the Double colon and Bit pattern based compression technique provides the same percentage of compression when contiguous zeroes are present only once in address, without any other numbers in between them. However, the Bit pattern compression provides better compression when contiguous zeroes are mentioned in separate hextents of address.

In figures 4.12 and 4.13 the results are shown for compression rate for Mode 1 and Mode 2, where 64 bit address is specified in the header (IID for Mode 1 and Prefix for Mode 2). The double colon as well as bit pattern based compression techniques provides better compression compared to HC1. The improvement depends on the number of continuous zeroes in the address. If X is the number of continuous zeroes and if the packet contains only the base IPv6 header, then compression rate is the percentage of X/N bits where N is the number of bits in the IPv6 Header. In Mode 1 and 2, Both the Double colon and Bit pattern based compression technique provides the same percentage of compression when contiguous zeroes are present only once in address, without any other numbers in between them. However, the Bit pattern compression provides better compression when contiguous zeroes are mentioned in separate hextents of address.

In figure 4.14 the results are shown for compression rate for Mode 3, where the complete 128 bit address is elided. Since no address is specified in the packet, the compression rate is the same for all three techniques. The results show that the compression rate of Double colon varies from 10% to 40% more compared to traditional HC1 compression and Bit pattern based compression techniques provide better compression compared to double colon technique when the continuous zero bytes are spread over the IPv6 address.

Figures 4.11 to 4.14 shows the percentage of compression achieved for an IPv6 frame with 30 bytes of data in the context of SCHC, SCHC with Double Colon compression and SCHC with Bit Pattern compression for different number of contiguous zeros in the IPv6 addresses for different communication modes (Mode 0 to 3). While the performance of SCHC is identical to SCHC with double colon or bit pattern based compression when there are no contiguous zeros in the address, the use of double colon or bit pattern compression with SCHC gives better compression results when the number of contiguous zeros increase in the addresses in case of Mode 0, 1 and 2. In case of Mode 3, since the IPv6 addresses are always elided in the compressed frame, the performance across all three schemes are identical.

The Table 4.11 tell about maximum data in a single frame. An experiment is run to transfer an image of size 1KB from the sensor node to the root node of the network with different number of contiguous zeros in the IPv6 source address of the sensor and root nodes. The experiment counts the number of 802.15.4 frames required to be transmitted from the sensor node to transfer the image successfully to the root node. In the first set of runs, the total number of frames sent is counted when using the default IPHC header compression technique against all the different source address schemes. In the next run, the total number of frames sent is counted when using the double colon compression method on top of the IPHC compression. In the last run, the total number of frames sent is counted when using the bit pattern compression method on top of the IPHC compression. The Table 4.12 shows the total number of frames sent in each case. It is clear from the table that the number of frames required to send the same image reduces when the number of contiguous zeros increase when compared to the default IPHC compression.

```
0000  61 dc 51 cd ab 07 00 00  00 00 00 0c c1 0e 00 00
0010  00 00 00 0c c1 7c d5 00  3f c3 0c 00 00 00 00 00
0020  07 c3 0c 00 00 00 00 00  01 e1 06 63 04 40 00 05
0030  13 f0 22 3d 16 2e 16 1c  31 30 39 ae
```

Figure 4.15: Compression without Bit Pattern Technique

```
0000  61 dc 51 cd ab 07 00 00  00 00 00 0c c1 0e 00 00
0010  00 00 00 0c c1 7c d5 00  3f 90 c3 0c 00 07 90 c3
0020  0c 00 01 e1 06 63 04 40  00 05 13 f0 22 3d 16 2e
0030  16 1c 31 30 6d dd
```

Figure 4.16: Compression with Bit Pattern Technique

In this example, the last fragment of a sensor data (2 bytes) captured by node with IP address fe80::c30c:0:0:7 is encoded in a 6LoWPAN encapsulated UDP frame and transported to node with IP address fe80::c30c:0:0:1. In the first case as shown in Figure 4.15, the packet is compressed using the existing

Table 4.11: Maximum data in a single frame: HC1: Stateless Header Compression, DC: Double Colon Compression, BC: Bit Pattern Compression

#Continuous #zeroes	HC1-M0 (Bytes)	HC1-M1 (Bytes)	HC1-M2 (Bytes)	HC1-M3 (Bytes)
0	64	80	80	96
32	64	80	80	96
64	64	80	80	96
80	64	80	80	96
16+32	64	80	80	96
32+48	64	80	80	96
#Continuous #zeroes	HC1-DC-M0 (Bytes)	HC1-DC-M1 (Bytes)	HC1-DC-M2 (Bytes)	HC1-DC-M3 (Bytes)
0	64	80	80	96
32	70	86	86	96
64	78	94	94	96
80	82	94	94	96
16+32	70	86	86	96
32+48	74	90	90	96
#Continuous #zeroes	HC1-BC-M0 (Bytes)	HC1-BC-M1 (Bytes)	HC1-BC-M2 (Bytes)	HC1-BC-M3 (Bytes)
0	64	80	80	96
32	70	86	86	96
64	78	94	94	96
80	82	94	94	96
16+32	74	90	90	96
32+48	82	90	90	96

IPHC compression scheme. Mode 1 compression is used for compressing both the addresses (SAM=0x1 and DAM=0x01). The compressed source and destination addresses encoded in the packet are c30c:0:0:7 and c30c:0:0:1 respectively. The packet size on the wire in this case is 60 bytes.

In the second case as shown in the Figure 4.16, the packet is compressed using the IPHC compression scheme with mode 1 compression similar to the previous case. But in addition, the compressed IP addresses are further compressed using the bit pattern compression scheme. The IPHC compressed source address c30c:0:0:7 is further compressed as c30c:7 and the destination address c30c:0:0:1 as c30c:1. A one byte metadata 0x90 (10010000b) is associated with each address to indicate the octets that are compressed. A total of 6 bytes of data is additionally compressed using this scheme. The packet size on the wire in this case is 54 bytes.

Based on analysis of proposed double colon address compression and Bit pat-

Table 4.12: Number of frames required to send 1KB of data: HC1: Stateless Header Compression, DC: Double Colon Compression, BC: Bit Pattern Compression

#Continuous #zeroes	HC1-M0 (Bytes)	HC1-M1 (Bytes)	HC1-M2 (Bytes)	HC1-M3 (Bytes)
0	16	13	13	11
32	16	13	13	11
64	16	13	13	11
80	16	13	13	11
16+32	16	13	13	11
32+48	16	13	13	11
#Continuous #zeroes	HC1-DC-M0 (Bytes)	HC1-DC-M1 (Bytes)	HC1-DC-M2 (Bytes)	HC1-DC-M3 (Bytes)
0	16	13	13	11
32	15	12	12	11
64	13	11	11	11
80	12	11	11	11
16+32	15	12	12	11
32+48	14	11	11	11
#Continuous #zeroes	HC1-BC-M0 (Bytes)	HC1-BC-M1 (Bytes)	HC1-BC-M2 (Bytes)	HC1-BC-M3 (Bytes)
0	16	13	13	11
32	15	12	12	11
64	13	11	11	11
80	12	11	11	11
16+32	14	11	11	11
32+48	12	11	11	11

tern address compression for HC1 and SCHC as shown in table 4.10 and the percentage of compression for HC1 and for SCHC as shown in figures 4.11 to 4.14. following points can be depicted.

1. The HC1 and SCHC header compression techniques significantly reduces IPv6 header size (45% (Mode 0) to 98% (Mode 3). However the Implementation of SCHC is rule based and it provides 2.5% reduction of header compared to HC1.

2. The HC1 and SCHC header compression provides further compression of address bits based on proposed double colon and bit pattern compression techniques by 17% to 37%. Bit pattern compression is advantageous when the contiguous zeroes are spread over the address.

4.5 Summary

Many times the IPv6 address contains leading zeros which can be compressed similar to double colon representation of the address. The proposed double colon address compression technique and bit pattern based address compression techniques, compresses the leading zeroes when they are in consecutive locations. However, the bit pattern based compression technique provides better compression rate, when the leading zeroes are not contiguous.

The proposed techniques are incorporated with respect to HC1 of IPHC in 6LoWPAN and SCHC for IPv6. The RuleID for SCHC IPv6 Compression for proposed methodology is designed. The comparative analysis shows that SCHC is better than HC1 and the proposed address compression techniques provide further compression of address bits with respect to HC1 and SCHC. With the hybrid model, the average size of the packet is reduced by providing 10% to 40% higher compression. Thus, it is possible to achieve better compression by potentially extending the IPHC and SCHC compression standard to support the bit pattern compression as one of the compression modes. The future work can be considered to analyse the proposed address compression technique with respect to larger data packets, image data transmissions and networks with substantial CRC errors.

While the proposed compression techniques do add computational overhead as the system must parse the IPv6 header to identify data that can be compressed and must be decompressed, the reduction in communication overhead more than compensates computation overhead. In wireless networks, the communication cost is much higher than computation cost due to higher packet loss ratio and need for re-transmissions. Additionally, the computation cost is further reduced with bitwise operations required by the compression techniques supported natively in hardware.

Chapter 5

Ranking based RPL (R-RPL) for Multipoint-to-Point Multimodal Data Communication in IoT Network

The applications of IoT may contain sensor nodes which sense the environment with only scalar data type sensors or it can also include multimedia sensors such as camera, audio recorder etc. The data transmission to sink or gateway may be periodic or event based. The nodes in the networks with resource constraint need energy efficient strategy to increase the life time of the network. Handling heterogeneous multimodal data in the network with in-network processing is very essential.

Most of the RPL applications concentrate on low data rates for scalar sensor data. Recent analysis and improvement depend on multimedia-based assistance and utilization. This kind of application has different requirements in terms of bandwidth, latency, storage, and so on. Fast growth in the connected devices to the Internet during the last decade and sudden demand for multimedia traffic has given rise to the emergence of the Multimedia Internet of Things (M-IoT).

In Nauman *et al.* (2020) M-IoT smart objects are usually resource-constrained, in terms of energy, memory storage, and processing power. To make the devices smaller, cost-effective, and energy-efficient, sensors are usually designed to be battery operated or solar powered with only a few kilobytes of memory, and limited processing power in megahertz.

The traditional multimedia application involves the data transmission of point-

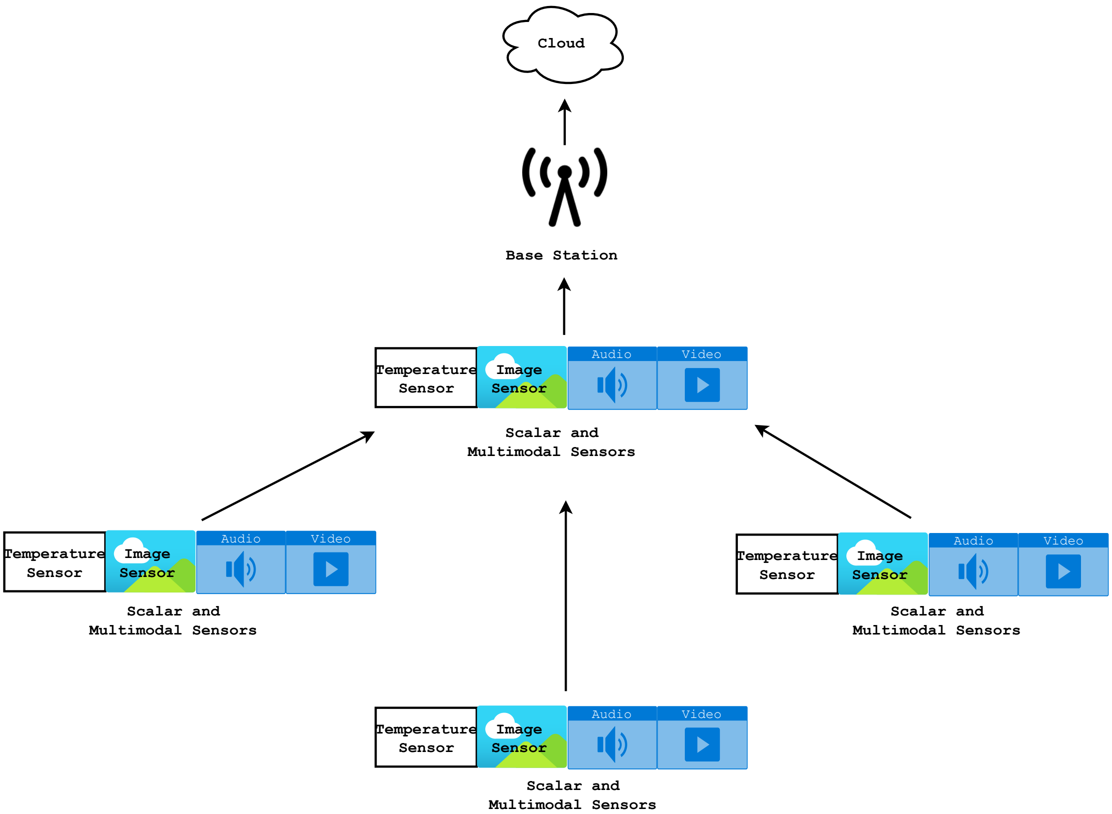


Figure 5.1: M-IoT Architecture

to-point, point-to-multipoint, or multipoint-to-point. On the contrary, M-IoT applications require immense data transmission during multipoint-to-point communication (e.g., the surveillance system of the entire smart city) The architecture of the M-IoT is shown in Figure 5.1. The sensor nodes which are capable of sensing environment through scalar data and multimedia data are considered in physical layer. The nodes can prefer IEEE 802.11 or IEEE 802.15.4 standard along with IPv6 standard for routing and communication network and data link layer based on types of applications. IEEE 802.11 can be used for communication for the applications such as Home automation, Indoor environment etc where the resources are available. For applications such as smart agriculture, disaster management etc IEEE 802.15.4 can be used as nodes are battery operated. Edge nodes are sensor nodes which collect sensor data. Fog nodes are intermediate nodes which performs the partial processing of data, or processing data and performing decision making during critical situations. The Cloud layer collects all sensor data for further data analysis. The architecture of M-IoT phases challenge in each layer.

Dynamic network, heterogeneous data, higher throughput, QoS, and delay sensitivity over such resource-constrained M-IoT smart objects escalates the challenges for M-IoT. Multimedia data i.e., audio, image, and video is set of unstructured features. Transmission of such bulky and unstructured data over bandwidth and computationally scarce network requires efficient and intelligent network topology. The addition of multimedia data acquisition and communication requires revision and amplification of the traditional IoT system, which we refer to as M-IoT. The revision of IoT for multimedia communication requires efficient feature extraction, event processing, encoding/decoding, energy-aware computation, lightweight and priority-based routing, QoS and QoE maintaining performance metrics, effective channel access, and fair-MAC protocols.

The major aspect in Multimedia IoT is handling data rate. The data rate varies based on application, event or resource constraints. As a result, in-network processing techniques for data aggregation, data transmission and data dissemination is required. Handling data transmission in resource constraint network where IEEE 802.15.4 is used for communication, with 6LoWPAN adaptation layer and RPL as routing protocol is great challenge when multimodal sensor nodes are considered. This work addresses this challenge and proposes the following techniques.

1. Proposed a Ranking based scheduling technique for RPL to handle heterogeneous data rate called R-RPL.

2. Proposed a suitable Objective Function for Multimedia IoT called DEE-OF.

The proposed Objective Function DEE-OF considers data rate, energy and ETX as parameters for parent selection and routing. The nodes estimates the rank based on proposed Objective Function, and performs scheduling of data traffic based on obtained rank for each flow in the network. The simulation results shows that the proposed R-RPL performs better compared to RPL for high data rate applications.

5.1 Related Work

In M-IoT, some of the major challenges are with respect to selection of Objective Function, performing load balancing in routing protocol and considering energy efficiency for increasing network lifetime. Hence, the literature survey is carried out with respect to these challenging issues.

In the paper Kettouche *et al.* (2019) describes that the Internet of Things systems can not successfully realise the notion of ubiquitous connectivity of everything if they are not capable to truly include multimedia things. Author has investigated the feasibility of video streaming using RPL (Routing Protocol for Low Power and Lossy Networks) by focusing on the impact of radio duty cycling on the quality of received video and the energy footprint of the network. To do so, author adopted a low complexity compression technique and use Cooja simulator to carry out experiments. There is a use of quality of service (QoS) as well as quality of experience (QoE) metrics to evaluate the quality of the received video. Mainly show that RPL along with ContikiMAC, the Contiki default radio duty cycling do not allow to handle real time video transmission in the context of constrained networks. However low rates up to 35 frames per minute are still possible with an acceptable quality.

In the paper Solapure and Kenchannavar (2020) mentioned the proposed Objective Functions design using various routing metrics used to enhance the performance of the IoT applications. Default OFs such as MRHOF and ETX will not fulfill the need for smart applications. For this purpose, the author has combined three metrics ETX, Content, and Energy, single and combination with each other to enhance and improve the design of the objective function of RPL for IoT applications. This technique will eliminate the cumulative effect of the short-listen problem of the default trickle timer. Short-listen problem arise when running Trickle in asynchronous networks. The short-listen problem may turn down the suppression mechanism of Trickle resulting in significant redundant transmissions and, thus limiting the algorithm scalability. Energy combined with Content (EC) and aggregation with Enhanced timer (EC_En_Timer) design gives better result for Packet Delivery Ratio (PDR) and Latency Delay (LD) as compared to default OF design. Residual Energy (RE) combined with ETX (EE) and conjunction with Enhanced timer (EE_En_Timer) design works well for energy consumption. Overhead is very less in RE and ETX design. Conversion time is reduced by almost 50% in an En_Timer design. Higher PDR and low delay values of EC and EC_En_Timer design encourages its use in health monitoring application where reliability is essential. Low energy consumption results of RE, EE, and EE_En_Timer designs are comfortable for forest monitoring applications, as energy is a crucial aspect. This comparative result outcome will help to fulfill the IoT application requirements. Overload of control messages along with triggering function need to be analyzed further to find its role in IoT applications.

In the paper Lamaazi and Benamar (2017) suggested that OF can operate according to a set of metrics and constraints used in a single or combined way. The use of a single metric in the OF can improve routing performances while degrades others. To overcome these barriers, the author introduces a new approach to enhance the RPL routing protocol. The proposed OF-EC (objective function-based combined metric using the fuzzy logic method), a new objective function that considers both link and node metrics, namely ETX (expected transmission count), HC (hop count), and EC (energy consumption) based on fuzzy logic concepts. The results show that the new OF-EC in comparison to the OF-based ETX and OF-based energy consumption only and OF_FUZZY allows improving RPL performances in terms of PDR and overhead. Also, this novel metric allows equalizing the energy consumption of nodes throughout the network. OF_FUZZY provided low packet delivery ratio compared to the other OFs. Since Fuzzy methods are heavy on network, simple energy efficient techniques are required.

In paper Bouzebiba and Lehsaini (2020) proposed an enhanced version of RPL for M-IoT called free bandwidth (FreeBW)-RPL in which the sensed data is essentially provided by multimedia devices. FreeBW-RPL protocol proposes a new objective function called FreeBW that takes the FreeBW calculation in the network layer. The setting of QoS routing challenges as the amount of the bandwidth while selecting the routing path to measure the maximum FreeBW to deliver better performance of the multimedia applications. Simulations have been conducted over the COOJA simulator. The results shown in (Bouzebiba and Lehsaini, 2020) outperforms the basic ones in terms of end-to-end delay, throughput, packet delivery ratio, and energy consumption and provides better performance than other protocols. Further work on FreeBWOF in heterogeneous networks and multimodal sensor is required to cover wide range of applications.

The following are the research gaps related to literature survey.

1. Most of the works concentrated on one or two metric to define objective function. Further study on identifying various Objective Function is essential with respect to Multimodal sensor data.

2. In Load Balancing, various works have been achieved with respect to improving network lifetime, energy efficiency, maximizing the packet delivery ratio and different load balancing techniques. The energy efficient load balancing is based on various Objective Functions and types of sensor data.

3. In Energy Efficiency, literature shows the work with respect to improve network lifetime as well as routing reliability. Further work on energy efficiency with respect to multimodal sensor data is essential.

5.2 Proposed Weighted Rank based Routing (R-RPL) for Multipoint-to-Point Communication

Many research papers shows the performance of RPL with respect to scalar sensor data. The future IoT requires the multi modal data transmission as the resource constraint devices can also be connected with low and medium resolution cameras and audio devices along with sensors like temperature, humidity sensors. In such applications, RPL needs certain improvement to adopt for heterogeneous sensor data transmissions. In this work, we propose a Rank based RPL for the same.

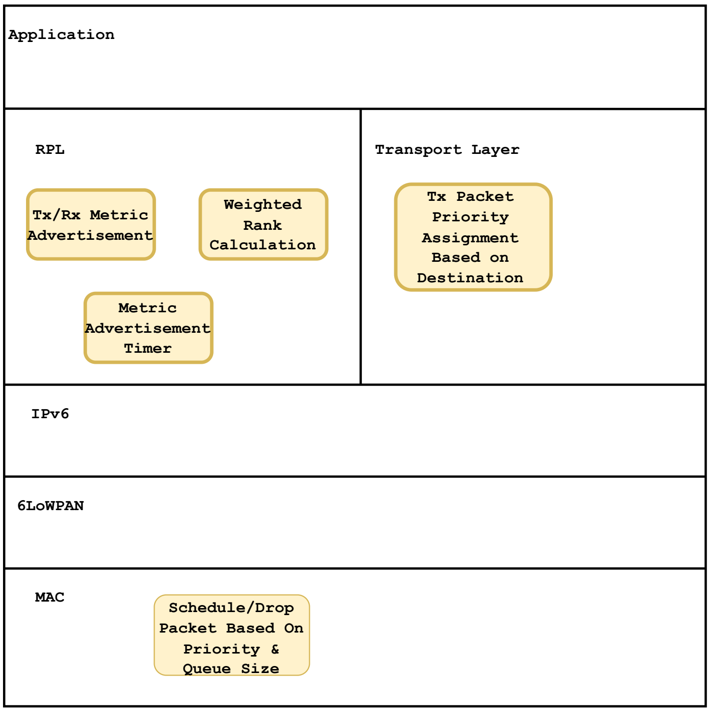


Figure 5.2: Block diagram Representing the Flow of Weighted Rank.

The Figure 5.2 gives brief about the working process of weighted rank at different layers of the network stack. In RPL, DIOs are enhanced to add a new sub-option field to advertise metrics to the neighbors. These metrics are fetched as part of a periodic timer. In addition, ranks are calculated for neighbors based on the received metrics. In the transport layer, priority of the packet is determined based on rank assigned to the destination of the packet. At the MAC layer, packets are either scheduled or dropped based on the packet buffer size and the priority of the inbound packet. A detailed description of each is covered in the subsequent sections. For experimental purpose three metrics have been considered

- Energy, data rate and ETX. These three metrics play a vital role in context of improving the packet deliver ratio and the total network lifetime in a network with multimodal sensors.

5.2.1 Weighted Rank Calculation for Neighbor Nodes

In a typical low power lossy network, a given node that is part of the DODAG has one or more neighbors. The neighbors may send or receive packets via the node based on the routing entries. In Contiki, at any given point, a node can have an outstanding connection with up to 2 neighbors. i.e., it can queue packets for up to 2 different destinations before it starts dropping packets for others. All the neighbors are treated equally. Packets coming from different sources are treated the same. While this works reasonably well in a less congested network, in a more congested network, packets from sources with lower energy could get dropped in favor of a higher energy node.

The system has a finite number of buffers available for outstanding packets to be transmitted. If the number of outstanding packets to be transmitted goes beyond the number of buffers, packets will be dropped. This situation is common when the rate of packets to be transmitted is higher than the link can support at the time (ex: radio busy). These drops could lead to re-transmissions from a lower energy node causing it to use more of its energy and in turn decreasing the lifetime of the node and potentially the entire network.

Similarly, fragmented packets from a higher throughput node (ex: nodes transmitting multimedia data) can be dropped in favor of a low priority packet from a sensor node and thus increasing jitter. To tackle this, we propose a technique where each neighbor is assigned a rank based on the various metrics that govern the network quality and lifetime and use the ranks associated with neighbors to determine priority for packets sourced from each of these neighbors. The process of Rank based priority selection consists of following phases: Metric advertisement and weighted rank calculation.

5.2.1.1 Metric Advertisement

The rank of each node must be decided on various metrics. As a result, to rank neighbors based on metrics, initially the neighbors must be able to share the metric values associated with various aspects. For example, to decide on parent selection at later stages, a neighbor must be able to communicate the details of remaining energy with its peer nodes. This process is called "Metric Advertisement".

To share the metric information, DIO message is considered and proposed certain changes for original DIO message format as shown in Figure 5.3. A new sub-option field is added and all other fields of DIO message is considered as represented in Figure 5.3. An RPL node will include this sub-option in all its DIO messages. Since it is part of a DIO message, all the neighbors in the range of the node receive this information.

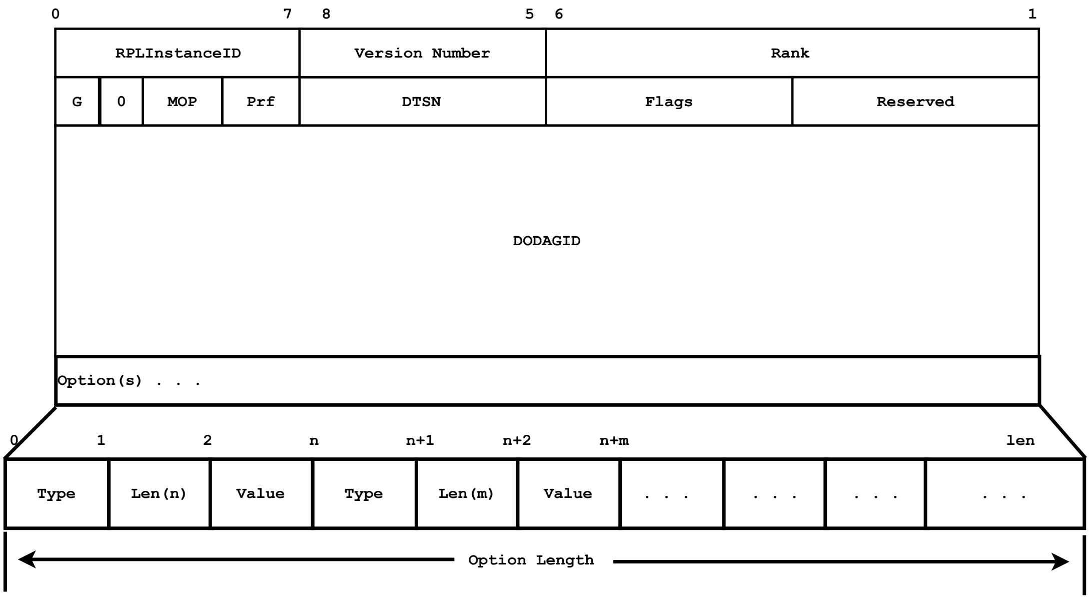


Figure 5.3: DIO - Message format followed by Sub-option - Metric Advertisement Message Format

Each metric is defined as a TLV (Type, Length, and Value). Type identifies the metric, the length indicates the size of the value associated with the metric and the value is the data associated with the metric. For example, in our work, we define 3 metrics as shown in Table 5.1.

Table 5.1: Metrics

Metric	**Type**	**Length**
Energy	1	1
Data-Rate	2	2
ETX	3	2

1. Energy - Indicates the percentage of energy left in the node
2. Data-Rate - Indicates the rate (in pps) at which the node is sending data (self generated + routed)

3. ETX - Indicates the quality of the link between the node and the neighbor.

5.2.1.2 Weighted Rank Calculation

An RPL node in the network receives DIOs periodically from all the neighbors in its range. The node will parse the DIO and look for the Metric Advertisement sub-option. When it finds the sub-option, it stores the data associated with all the metrics shared in the sub-option in its cache. This cache is updated every time a new DIO is received from the neighbor. This sequence is shown in Figure 5.4.

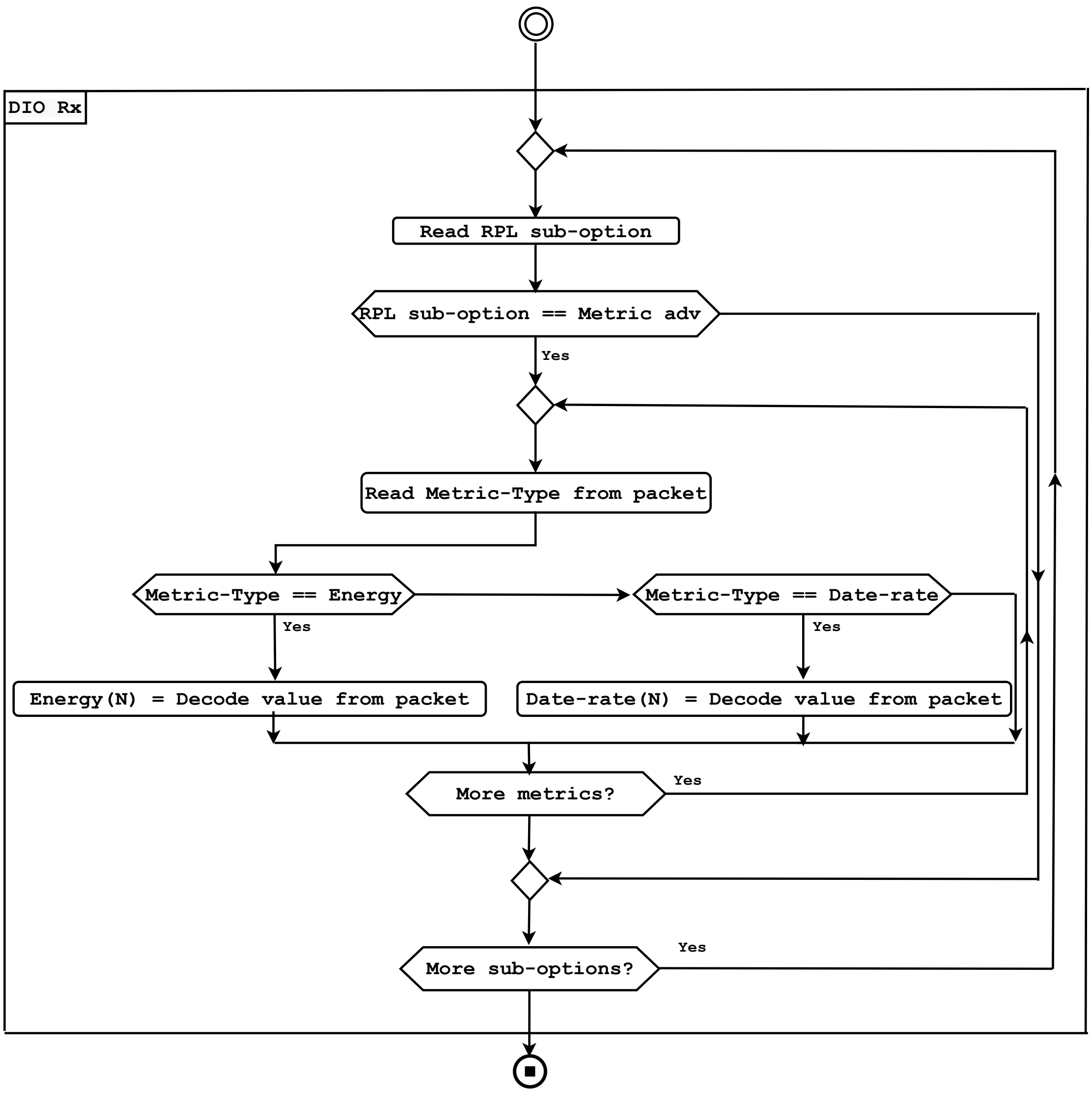


Figure 5.4: DIO - Rx

Algorithm 2 RunMetricAdvertisementTimer

Input: Neighbor Table
Output: $W_{Rank}(Max)$

Energy(Max) = Data-Rate(Max) = ETX(Max) = 0
for each neighbor N in the neighbor table **do**
  if Energy(N) > Energy(Max) **then**
    Energy(Max) = Energy(N)
  end if
  if Data-Rate(N) > Data-Rate(Max) **then**
    Data-Rate(Max) = Data-Rate(N)
  end if
  ETX(N) = Calculate ETX for neighbor
  if ETX(N) > ETX(Max) **then**
    ETX(Max) = ETX(N)
  end if
end for
$W_{Rank}(Max) = 0$
for each neighbor N in the neighbor table **do**
  R_{Energy} = Rank based on Energy(N)
  $R_{Data-Rate}$ = Rank based on Data-Rate(N)
  R_{ETX} = Rank based on ETX(N)
  $W_{Rank}(N) = (W_{Energy} * R_{Energy}) + (W_{Data-Rate} * R_{Data-Rate}) + (W_{ETX} * R_{ETX})$
  if $W_{Rank}(N) > W_{Rank}(Max)$ **then**
    $W_{Rank}(Max) = W_{Rank}$(N)
  end if
end for

The node runs a fixed interval timer to walk the list of all the current neighbors assigning rank to each based on the metrics advertised. This fixed interval timer is termed 'Metric Advertisement Timer' and set at 3 seconds in the proposed work. Thus, the ranks associated with each neighbor is refreshed every 3 seconds. The node then runs through all the it's current neighbors periodically, we call it "Metric Advertisement Timer" and assigns ranks for each of the neighbor based on the values of the metrics advertised. In the proposed work, the periodicity is set to 3 seconds. The algorithm 2 explains the details of the Metric Advertisement Timer and the complexity is O(n).

When the node transmits a DIO, it includes the details of the metrics to be advertised to it's neighbors. This sequence is shown in Figure 5.5.

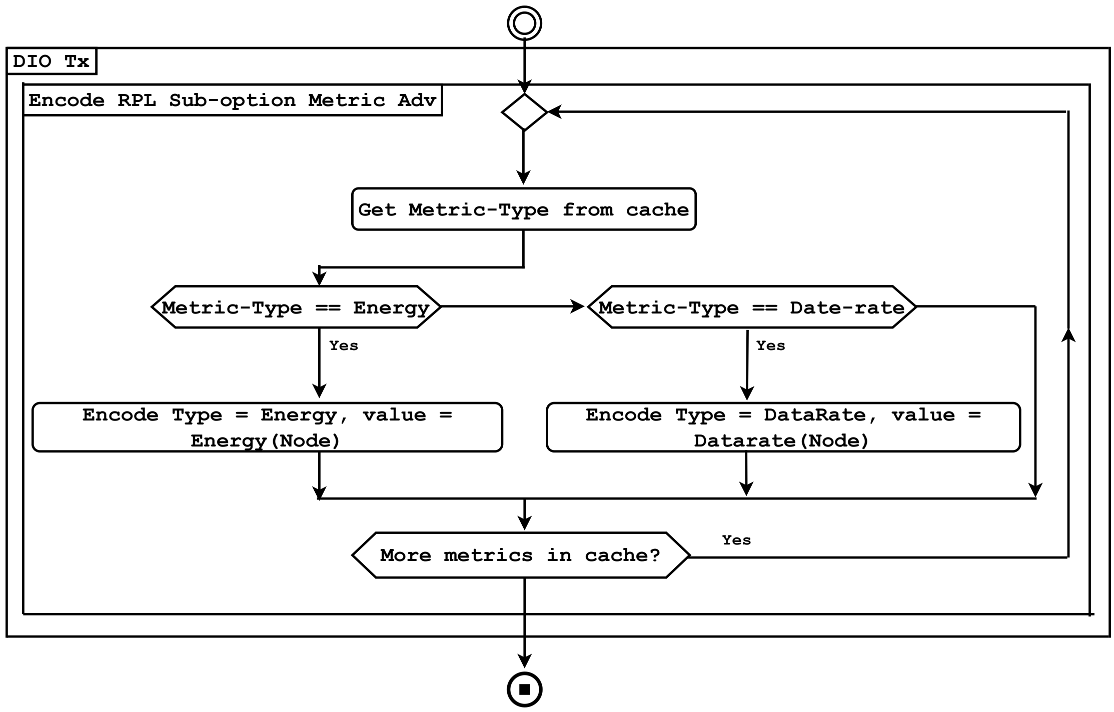


Figure 5.5: DIO - Tx

5.2.1.3 Ranking Method for Child Nodes

The Ranking method is popular because it is relatively simple to implement, and it only requires knowing the marginal proportions for each variable used in weighting. This method has been chosen to sort the child nodes based on energy, data rate, and ETX. The characteristics of the parameters considered are as follows:

1. Lower the energy value the node must get a higher rank.
2. A higher data rate must get a higher rank.
3. Lower ETX must get a higher rank.

From the above characteristics, higher Rank number gets higher priority. The rank based on each metric is calculated separately and finally priority is assigned based on combined metric rank calculation. We propose the rank calculation based on energy as shown in equation 5.1 and 5.2. The goal of this formula is to ensure the node with the lowest energy in the group is assigned the highest rank. Thus a higher priority would be assigned to a node with lower energy with the intent to reduce the need for re-transmissions from such a node in turn preserving the energy.

$$Minimize\ R_{Energy} = [10 - N_{Energy} * 10/MAX\_ENERGY] \tag{5.1}$$

$$N_{Energy} = \frac{(TotalBatteryEnergy - EnergyConsumed) * 100}{TotalbatteryEnergy} \quad (5.2)$$

We propose the rank calculation based on data rate as shown in equation 5.3. A node with the highest data rate in the group is assigned the highest rank. A higher rank ensures the likelihood of packet drops from nodes generating higher volume of data is lower since these packets are generally from audio/video services that would have strict latency and jitter requirements.

$$Maximize\ R_{DataRate} = [N_{DataRate} * 10/MAX\_DATA\_RATE] \quad (5.3)$$

Similarly, We propose the rank calculation based on ETX as shown in equation 5.4. A link with lower ETX implies less congestion on the link and thus lower chances of packet drops. Thus the nodes that have lower ETX on the link are assigned higher ranks to improve packet delivery ratio.

$$Minimize\ R_{ETX} = [10 - ETX * 10/MAX\_ETX] \quad (5.4)$$

The combined weighted Rank determined for child nodes is considered as shown in equation 5.5.

$$WeightedRank = W_1 * R_{Energy} + W_2 * R_{Datarate} + W_3 * R_{ETX} \quad (5.5)$$

where $W_1 + W_2 + W_3 = 1$

In each parent node the priority of child node is assigned based on weighted Rank.

5.2.1.4 Rank based on Energy

For calculating rank based on energy, the battery capacity of the mote is necessary to consider. For simulation purposes, a Zolertia Z1 mote with a 2xAA battery has been used. Based on the capacity of the Z1 battery, the battery capacity of each node is calculated. Based on the value of estimated energy, assigning of rank has been performed.

5.2.1.5 Rank based on Data Rate

The data rate is a term to indicate the transmission speed, or the number of packets per second transferred. The leaf nodes of the topology have been given different data rates, to check the packet drop of the node. The leaf node with less data rate is considered with x packet/sec and leaf nodes with a high data rate have y packet/sec. Based on the Ranking method, the Rank data rate is calculated.

5.2.1.6 Rank based on ETX

ETX optimize or constrain a routing metric on the paths. Since ETX is linked specifically, it is not advertised as part of a DIO message since a DIO can be a multicast message destined to all the neighbors in the node's radio range. Instead, the rank based on ETX is calculated as part of the metric advertisement timer. When the timer expires, the ETX for each link is fetched and the rank is assigned based on that.

5.2.2 Weighted Rank Calculation Example

In Figure 5.6 example depicts at a high level, the different stages in how a WR is calculated for a node. Node 5 receives DIOs from all it's neighboring nodes 9, 13 and 2. Each DIO contains the E percentage and the DR of that node. Node 9 reports a E level of 90% and DR of 1pps. Node 13 reports it's E level as 75% and DR as 5pps. And node 2 advertises it's E as 60% and DR as 8pps. Node 5 stores this information in it's neighbour cache for further processing. At the end of the metric advertisement timer interval, node 5 walks it's list of neighbors and assigns ranks for individual metric equation 5.1 and equation 5.3 for each of it's neighbor. During this process, it also calculates the ETX of the link for each neighbor and assigns a rank for it as well using equation 5.4. Once the individual metric ranks are calculated for each neighbor, node 5 then calculates the WR for each equation 5.5. Node 5 stores the calculated WR against the neighbor in it's cache for future use. Node 2 is assigned a WR of 5. While node 9 and 13 are assigned WR 2 and 4 respectively.

5.2.3 Priority based Packet Forwarding using Weighted Rank

Here weighted rank is assigned to each neighbor in the range and use this for determining the priority of the packets being transmitted over a given link. The first step is to determine the priority of the packet at the transport layer based on the source and destination addresses.

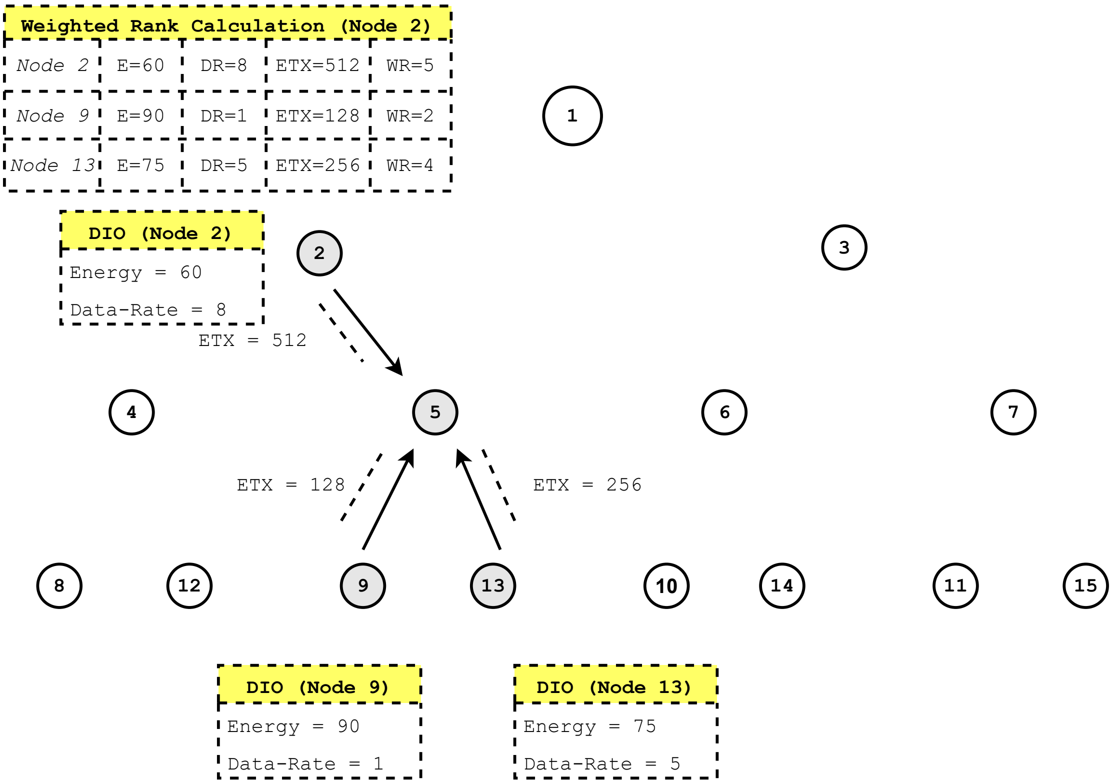


Figure 5.6: Weighted Rank Calculation

5.2.3.1 Transport Layer

The node first determines if the packet being forwarded is destined to the root of the DODAG as in Figure 5.7. If the packet is destined to the root, the priority for the packet is assigned based on the previous hop for the packet. i.e., assign the priority based on the weighted rank associated with the node from which the packet was received. If the packet is self-generated (generated on this node), assign an arbitrary priority to it. In the proposed work, it is assigned with the highest priority in the priority range. Once the priority is determined, the priority is pushed in the metadata of the packet and forwarded to the MAC layer.

5.2.3.2 MAC Layer

When the packet reaches the MAC layer as shown in Figure 5.8 , the priority of the packet is looked up from the metadata. At the MAC layer, the neighbor queue for the current destination is looked up and the packet is queued for transmission if -

1. The neighbor queue exists and both the neighbor queue and the packet queue is not full.

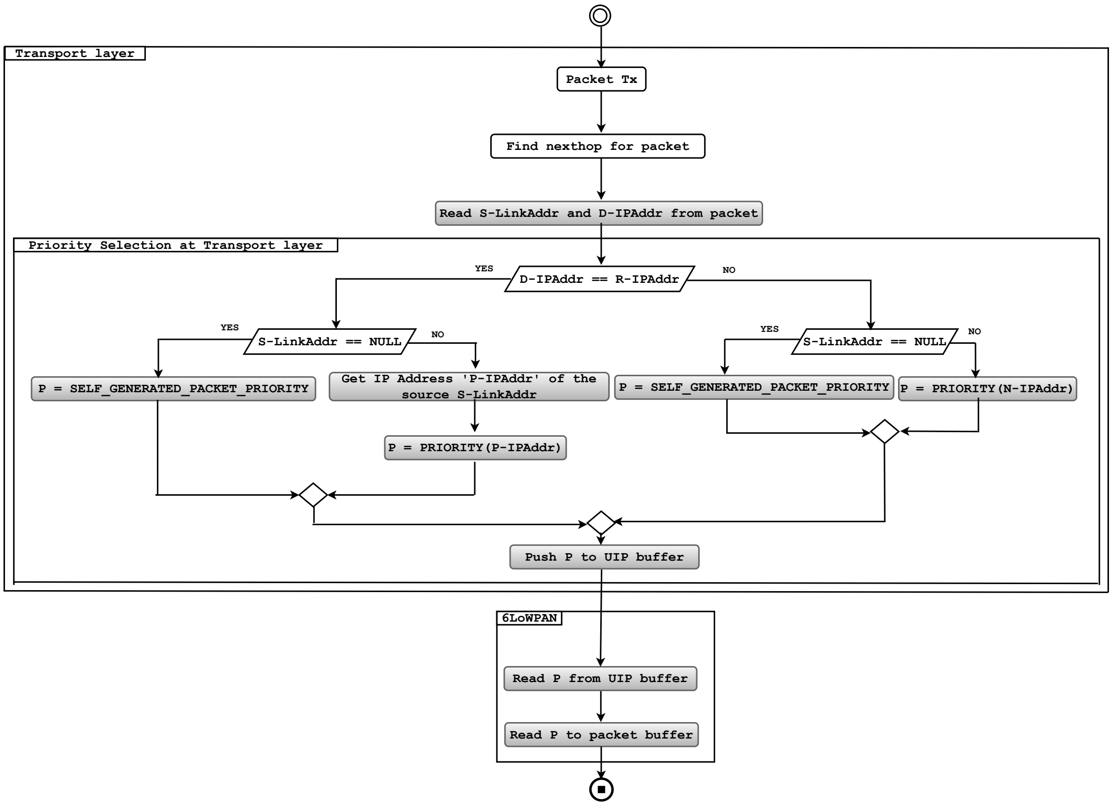


Figure 5.7: Data-Plane Packet Prioritization With RPL Metric Advertisement

2. The neighbor queue does not exist and the current number of neighbor queues is less than the limit and the packet queue is not full.

In all other cases, the packet is dropped.

In this work, additional checks are performed based on the priority of the packet before determining if the packet must be dropped.

1. If the neighbor queue exists but is full, find a packet with a priority less than the priority of the current packet. If a packet is found, drop the packet and queue the current packet for transmission. If not, drop the current packet.

2. If the neighbor queue does not exist and the current number of neighbor queues is at the limit, find the highest priority associated with a packet in each of the neighbor queues. Find the lowest priority amongst all the highest priorities of each queue. If the priority is lower than the priority of the current packet, delete the neighbor dropping all the packets in its queue. Create the neighbor queue for the current destination and queue the current

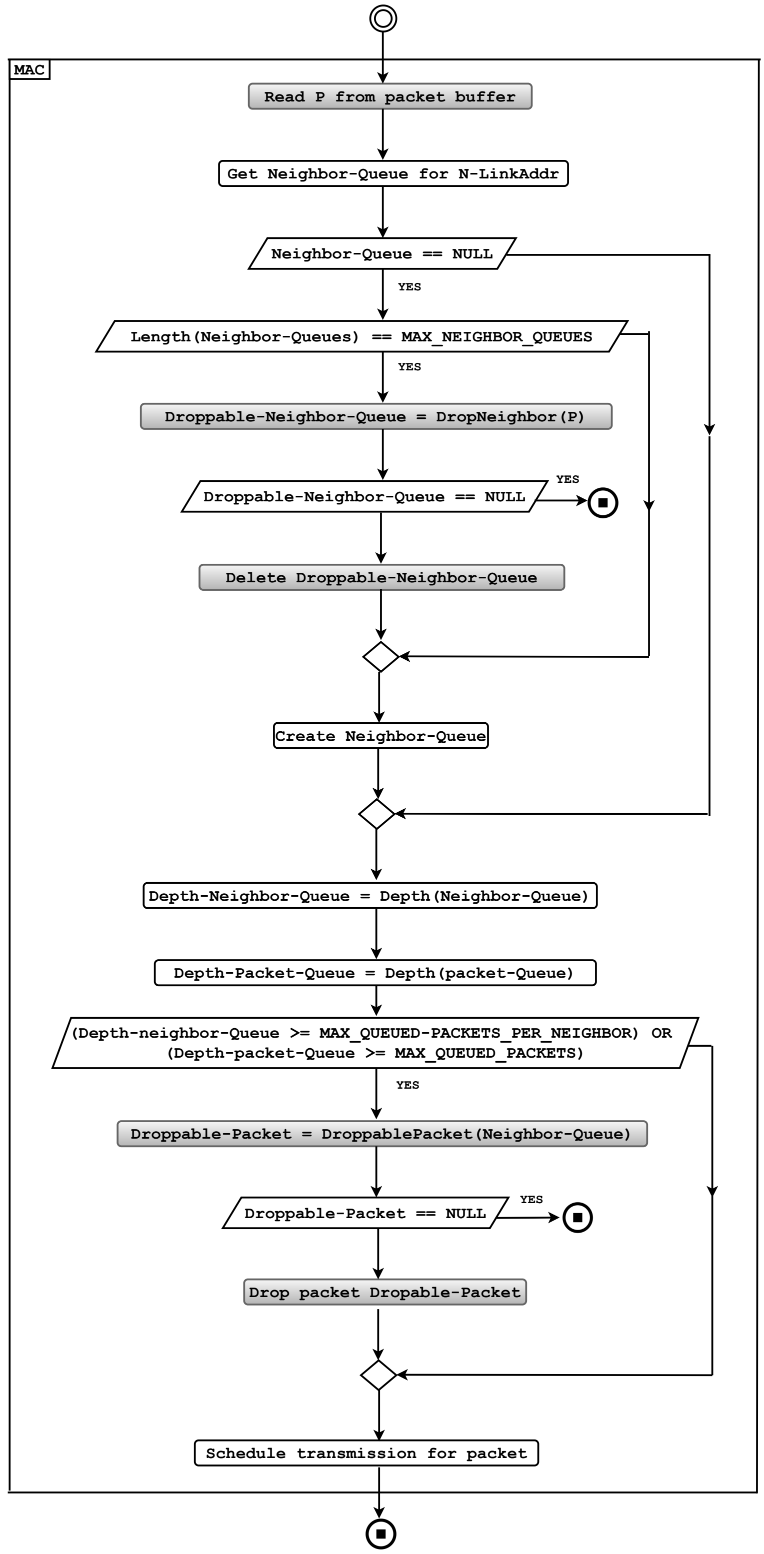


Figure 5.8: Data-Plane Packet Prioritization with RPL Metric Advertisement - MAC Layer

packet for transmission. If the priority is equal to or greater than the current packet, drop the current packet.

This aids in reducing the chances of higher priority packets from being dropped in favor of lower priority packets.

5.2.3.3 Packet Priority

Determining the priority of packet is calculated based on equation 5.6

$$Priority = \frac{W_R * 10}{W_R(MAX)} \tag{5.6}$$

5.2.4 Priority based on Weighted Calculation

In example Figure 5.9, Node 9 and Node 13 are trying to send packets to Node 1, the root of the DAG. The first hop of the packets in both cases is Node 5 the parent for both nodes 9 and 13. Node 5 already has WRs calculated for nodes 9 and 13 using the metrics they have advertised in their DIOs. When packet P1 from Node 9 arrives at Node 5, Node 5 sees the packet is to the root and uses the WR of the previous hop (Node 9) to determine the priority for this packet. Based on the WR of Node 9, a priority of 4 is assigned to packet P1. While P1 is still in the queue for transmission, packet P2 from Node 13 arrives at Node 5. Like in case of packet P1, Node 5 determines the priority for this packet as 8 based on the WR assigned to Node 13.

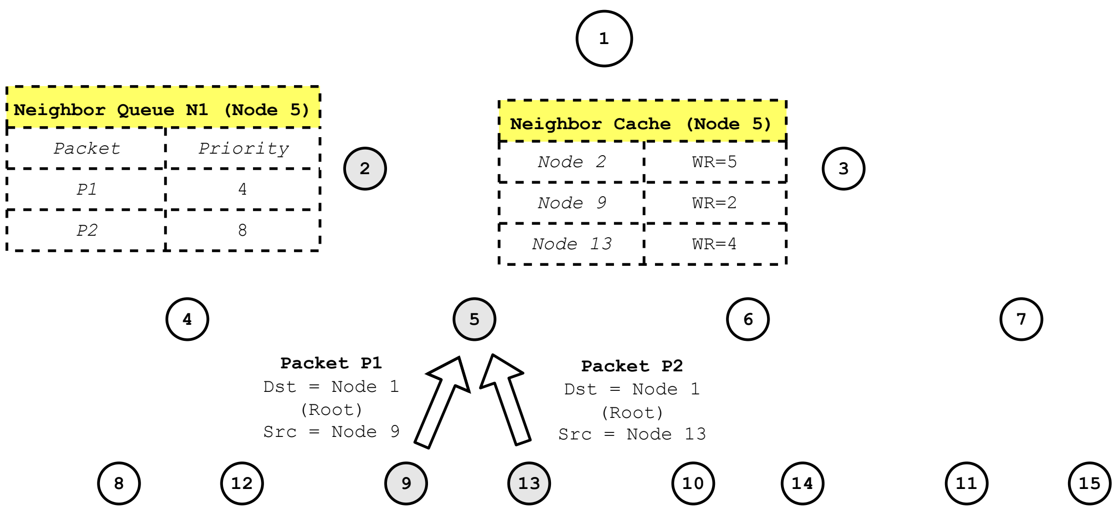


Figure 5.9: Priority based on Weighted Rank

Due to the radio channel being busy, 4 packets are already queued up to be sent towards the root of the packet and there are no more buffer space available to queue anymore packets in Figure 5.10. Meanwhile another packet P5 from Node 13 arrives at Node 5 destined to Node 1. Based on the weighted rank of Node 13 a priority of 8 is assigned to packet P5. Since there is no more buffer space available to queue packet P5, Node 5 checks for any lower priority from the back of the queue that can be dropped in favor of this packet. It finds packet P4 with priority 4 and drops it to free up the packet buffer to queue packet P5.

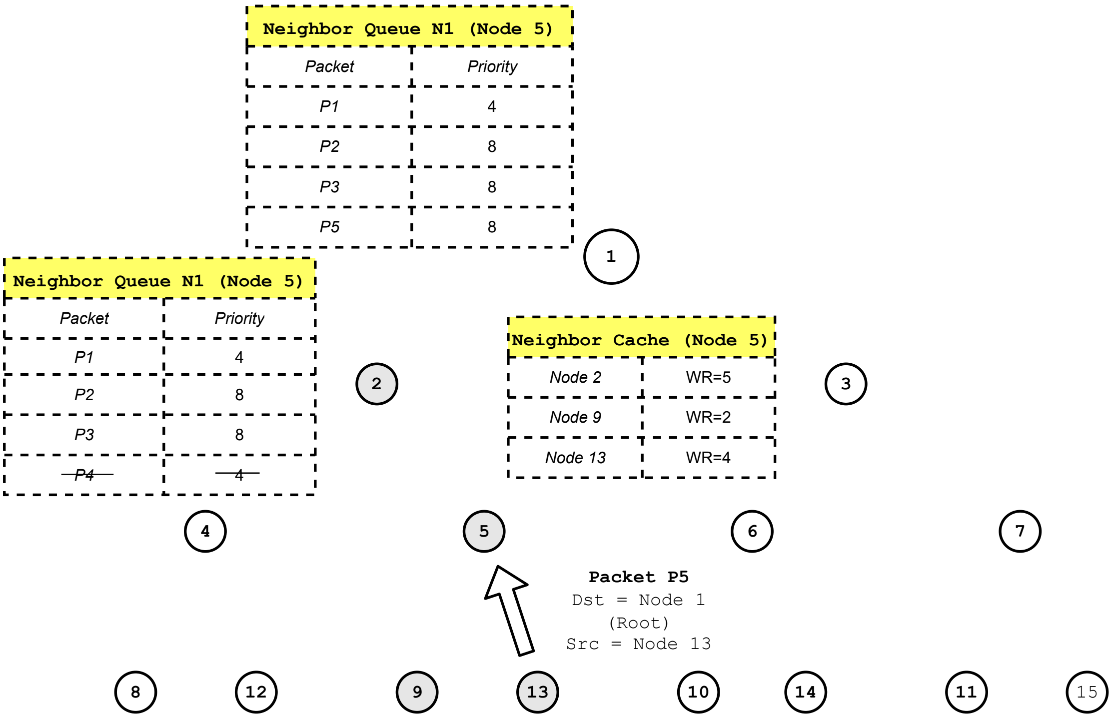


Figure 5.10: Priority based on Weighted Rank

5.3 Results and Discussions

The experiment included 2 types of Z1 motes. Type 1 with a total energy of 100000mJ and data rate of 1pps and Type 2 with a total energy of 180000mJ and data rate of 5pps. Different weights has been considered for different metrics. The weights used in the experiment are $W_{Energy} = 5$, $W_{Datarate} = 3$ and $W_{ETX} = 2$. The proposed technique has considered three performance metrics and compared the result with RPL. Figure 5.11 shows the test topology considered to experiment with the performance metrics. The leaf node with less data rate is considered with 1 packet/sec and leaf nodes with a high data rate have 5 packet/sec based on limitations with the simulator. Table 5.2 summarizes the simulation settings.

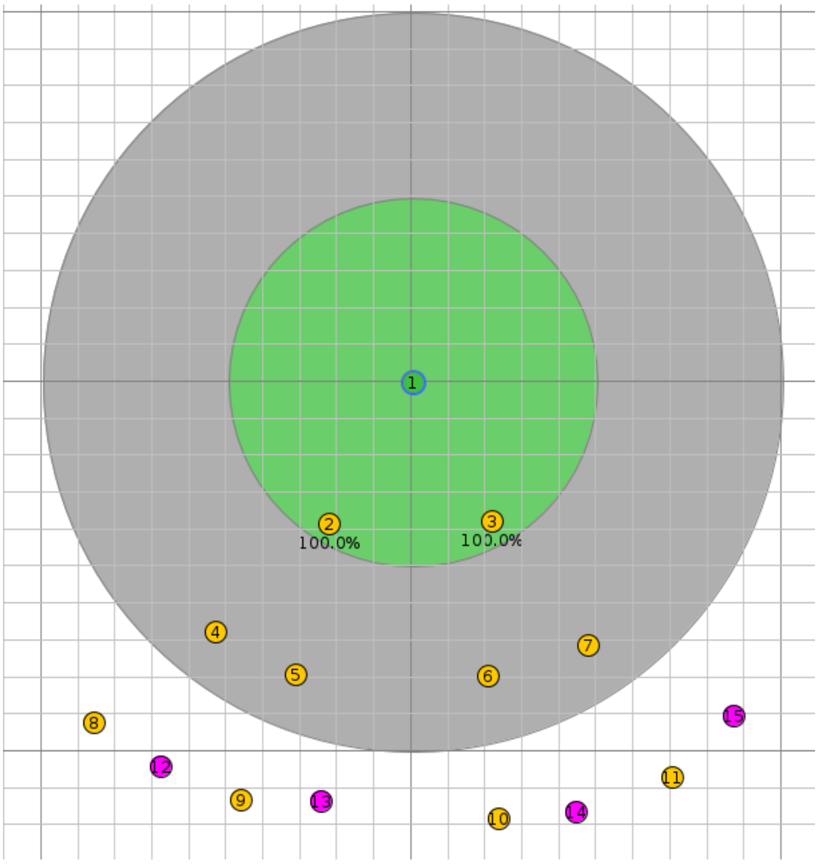


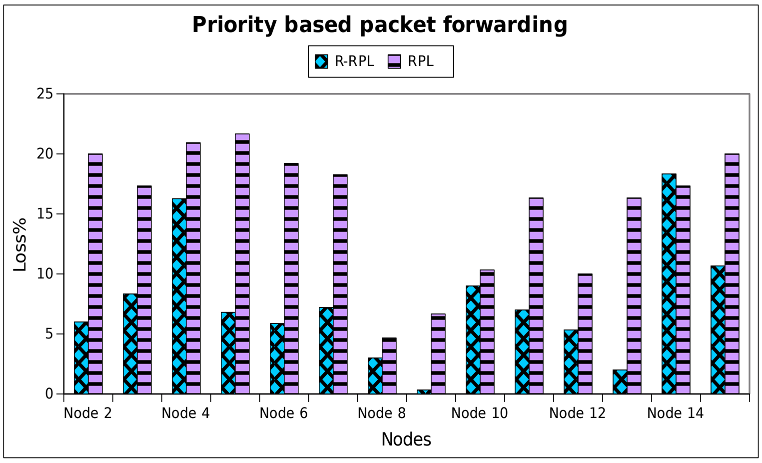
Figure 5.11: Deployment of Nodes

Table 5.2: Simulation Parameter.

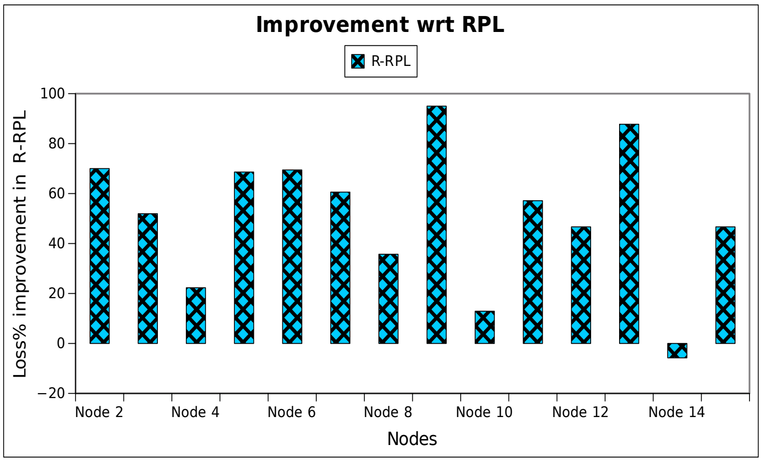
Simulation Parameter	**Values**
OS	ContikiOS-ng
Radio model	Unit disk graph model
Mote type	Z1 Mote
Network size	100 m x 100 m
Application Program	Examples/rpl-udp

1. Loss Percentage: The reliability of a communication network path is expressed by the packet loss rate. Packet loss occurs when one or more packets within a transmission are successfully sent, but fail to arrive at the destination. Packet loss can be caused by a variety of factors including network congestion, faulty network components such as hardware or drivers, or corrupted packets within the transmission.

$$Minimize\ Loss\% = \frac{(ReceivedPacket - SentPacket)}{SentPacket} * 100 \tag{5.7}$$



(a) Loss percentage



(b) Loss percentage improvement

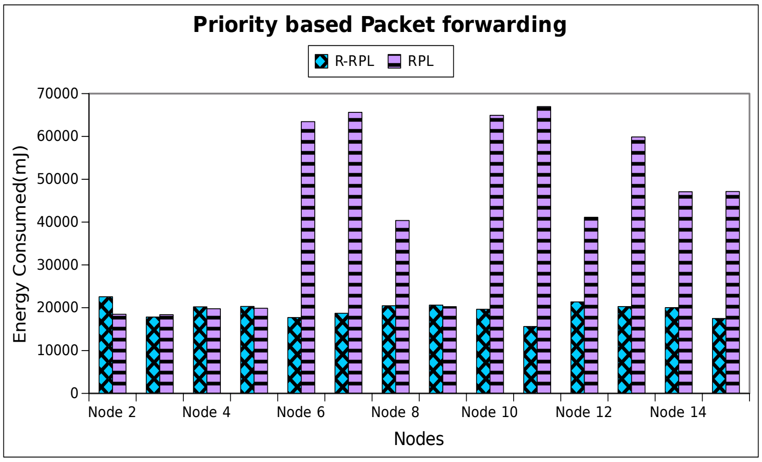
Figure 5.12: Performance Metrics of Loss% in R-RPL

From the above results, Figure 5.12a mention the comparison between RPL and R-RPL in priority based packet forwarding. Figure 5.12b says the percentage improvement of each node with respect to RPL. The node 14th provides more loss compared to RPL. But overall, PPF method gives better results than the RPL. The graph 5.12b mention the loss% improvement graph with respect to RPL, where the percentage of improvement equals 51.55%.

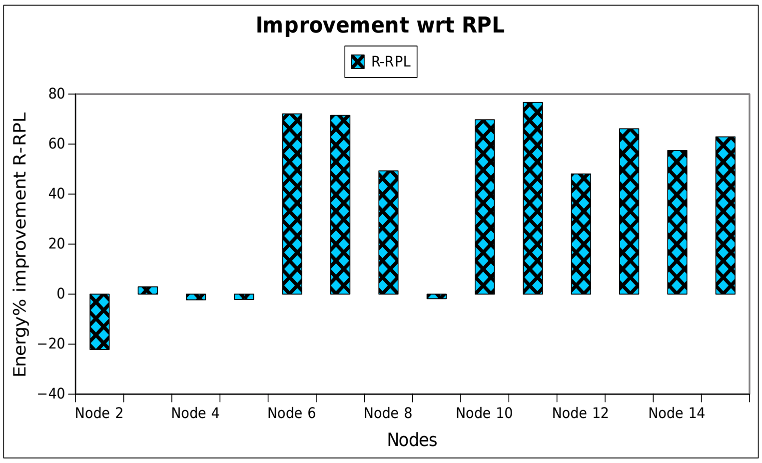
2. Energy Consumed: The calculation is carried out using a powertrace tool available in ContikiOS. It is the energy of nodes spent during the exchange of information in the network. During transmission, the energy spent by the node is called "all transmit" while in the reception it is called "all listen". In addition, other parameters are considered for energy computation which are CPU that represents the power consumption during the full power mode

and LPM representing the power consumption during the low power mode. V corresponds to the battery voltage. Rtimer represents the number of ticks per second (=32768 ticks/s).

$$
\begin{aligned}
Minimize\ Energy(mJ) = (&Transmit * 17.4mA + Listen * 18.8mA + \\
&CPU\_time * 0.33mA + LPM * 0.011mA) * \\
&3V/(32768)
\end{aligned}
\tag{5.8}
$$



(a) Energy Consumed



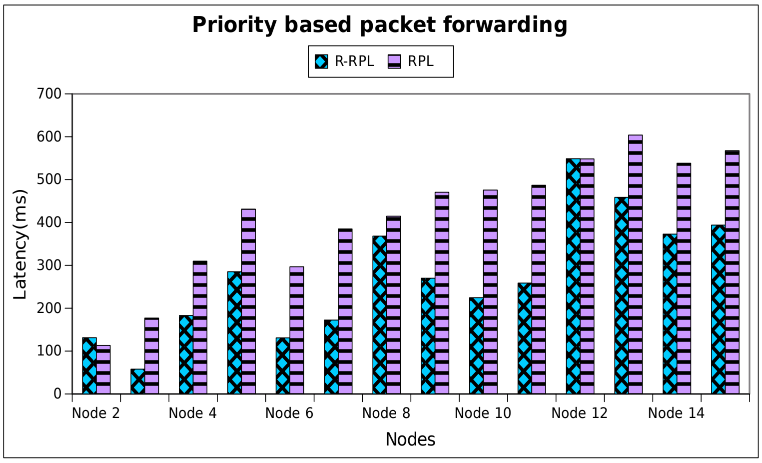
(b) Energy Consumed Improvement

Figure 5.13: Performance Metrics of Energy Consumed in R-RPL

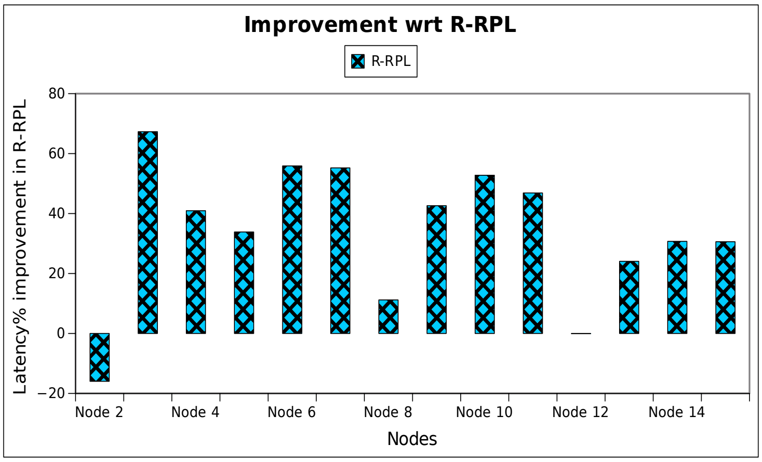
From Figure 5.13a and Figure 5.13b, percentage of energy consumed in the bottleneck node 2 is more comparatively with the RPL. The percentage improvement with respect to RPL in energy consumption is 54.02%.

3. Latency: Latency is a measure of delay. In a network, latency measures the time it takes for some data to get to its destination across the network.

$$Minimize\ Latency(ms) = (Senttime - Receivedtime) \tag{5.9}$$



(a) Latency



(b) Latency improvement

Figure 5.14: Performance Metrics of Latency in R-RPL

Figure 5.14a and Figure 5.14b mention that delay is more in node 2 when compared to other nodes. Overall result of the network says that R-RPL in priority based packet forwarding method outperforms better compared to the RPL. The graph 5.14b describes the improvement with respect to RPL, where percentage equals to 33.72.

5.3.1 Weighted Rank Based Objective Function for Parent Selection

In RPL, an objective function is responsible for determining the best parent for a given node at a given point amongst multiple potential parents. The path cost calculation for a neighbor is what drives the decision on which neighbor is chosen has the parent. Each objective function varies on how it determines the path cost that in turn driving how a parent is chosen. In addition to path cost, the objective function is also responsible for determining the rank to be assigned for a node based on the parent node selected.

In the proposed objective function, the weighted rank based model is used to determine the path cost and rank for a neighbor.Since the criteria for choosing a parent is different to prioritizing a child, the weights chosen for the metrics is different when calculating the weighted rank for a neighbor as a potential neighbor.

$$PathCost(N) = ((10 - WRank(N)) * (Min\_HopRank\_Inc/10)) + Min\_HopRank\_Inc \tag{5.10}$$

where 10 is the maximum value of weighted rank that can be associated with any neighbor.

The path cost associated with a neighbor will be lower if it has a higher weighted rank. The path cost for neighbors are distributed between Min_HopRank_Inc and (2 * Min_HopRank_Inc).
i.e., Min_HopRank_Inc $\leq PathCost(N) \leq (2 * Min\_HopRank\_Inc)$

$$Rank = MAX((Rank(N) + Min\_HopRank\_Inc), PathCost(N)) \tag{5.11}$$

The Figure 5.15 example is at a high level describes how Node 9 is determining it's parent between nodes 5 and 4. Node 9 receives DIO with the energy and data-rate metrics from nodes 4 and 5. As explained in the previous example, node 9 like 5 uses this information along with the ETX metric to calculate weighted ranks for nodes 4 and 5. Based on the metrics advertised by 4 and 5, Node 4 gets a weighted rank of 3 and Node 5 is assigned a weighted rank of 9. Node 9 then uses this information when it is calculating the path cost via Node 4 and 5 to determine the best path and hence the preferred parent. Using the weighted rank, Node 9 calculates the path cost via Node 4 as 326 and 211 via Node 5 using equation 5.10. Since the path cost via Node 5 is lower, Node 9 picks Node 5 as

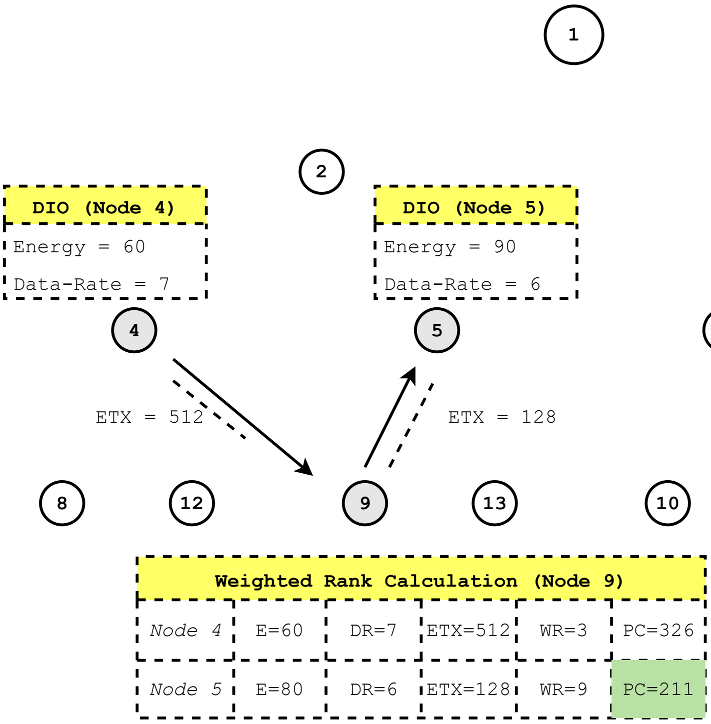


Figure 5.15: Path cost calculation

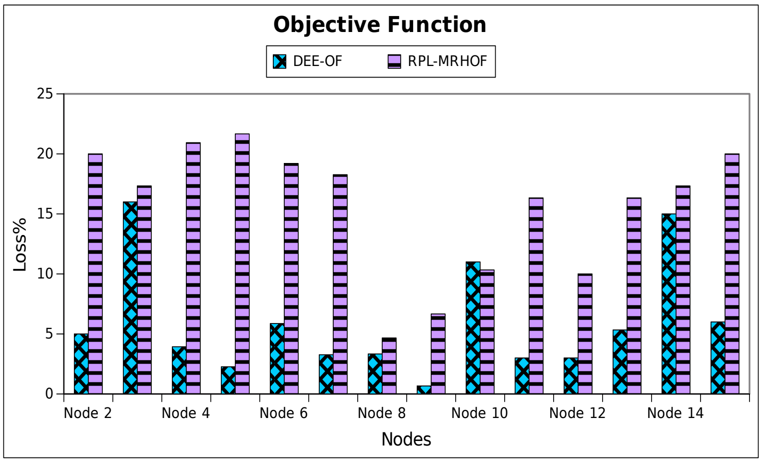
it's preferred parent.

5.3.2 Results and Discussion

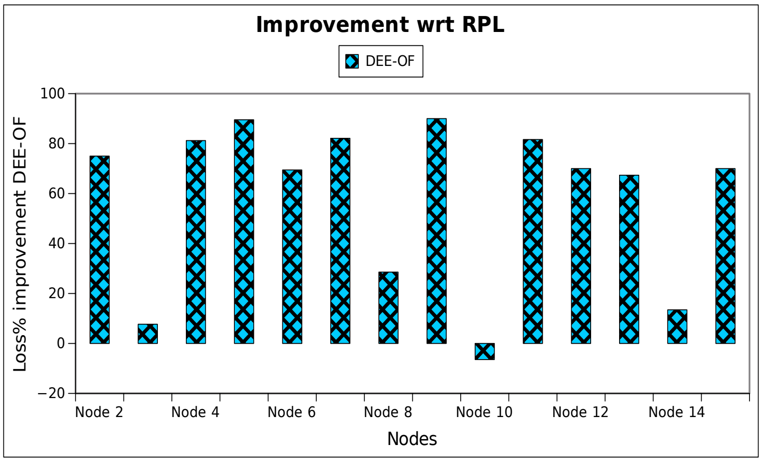
From Figure 5.16a and Figure 5.16b one particular node gives more loss, but overall results outperforms better compared to RPL. The graph 5.16b says the improvement of Loss percentage is 61.8 with respect to RPL.

Figure 5.17a and Figure 5.17b mention about energy consumption of each node in RPL and DEE-OF. Bottleneck nodes such as node 2 and node 3 consumes less energy compared to other nodes in the network. Every node gives better results from DEE-OF compared to RPL. The percentage improvement of energy consumption with respect to RPL is 55.41.

Figure 5.18a and Figure 5.18b mention the comparison and percentage improvement of latency with respect to RPL and DEE-OF. Proposed method gives more delay in the bottleneck node as compared to RPL. Considering overall network, proposed method is better compared to RPL. The graph 5.18b is the improvement graph, where the percentage equals to 26.78.



(a) Loss percentage

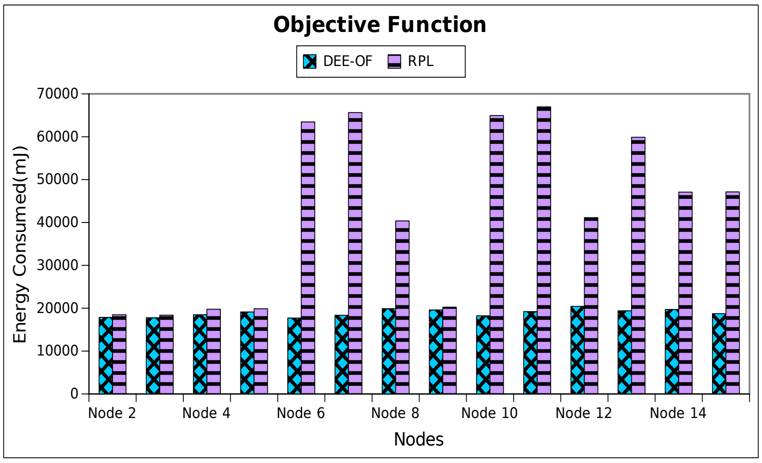


(b) Loss percentage improvement

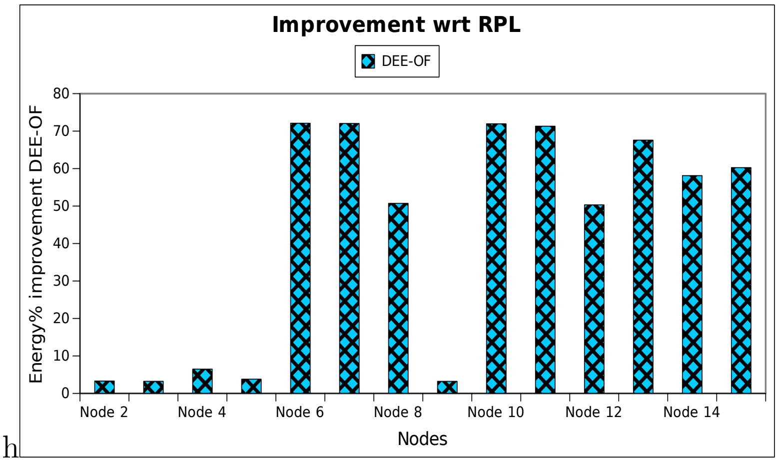
Figure 5.16: Performance Metrics of Loss% in DEE-OF

5.3.2.1 Image Transmission Time with R-RPL running Objective Function DEE-OF

For the same Figure 5.11, the following graph Figure 5.19a shows the time taken to transfer an image of size 100KB from the multimodal sensor nodes to the root. The total time taken by DEE-OF to transfer the 100KB data is approximately 400 seconds when compared to plain RPL which takes about 750 seconds. Figure 5.19b shows the percentage improvement with respect to the total time taken for each node to transmit the image. The average percentage of improvement with respect to RPL is 24.46.



(a) Energy Consumed



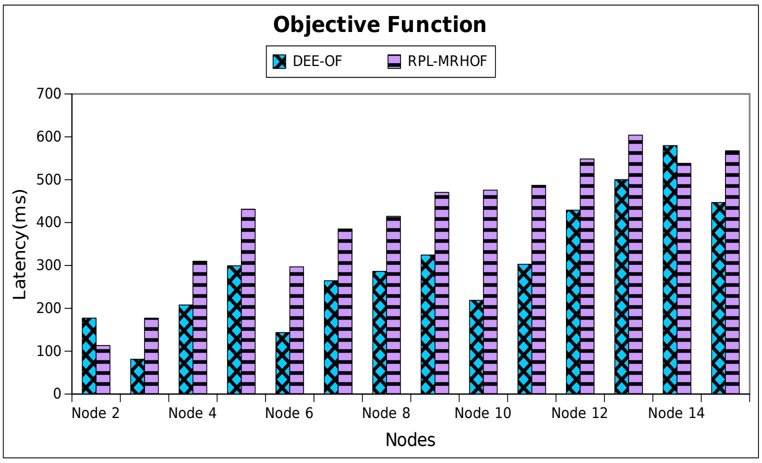
h

(b) Energy Consumed improvement

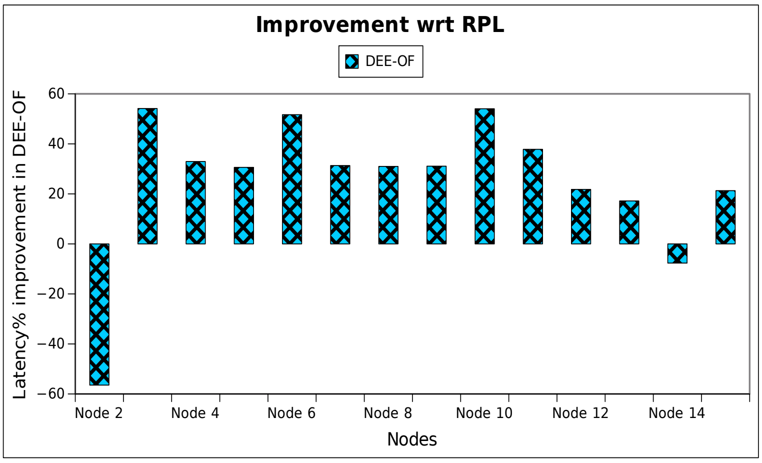
Figure 5.17: Performance Metrics of Energy consumed in DEE-OF

5.3.2.2 Bursty Data

Data bursts are high bandwidth transmission over a short period of time. With multimodal sensors, data bursts during transmission are an expected phenomena. An experiment was run to compare the performance of R-RPL w.r.t RPL when a sudden burst of 3x the normal data rate (15pps vs 5pps) is sent at random intervals for short periods of time during the transmission of an image. Figure 5.20a shows the image transmission with bursty data compared with RPL. In Figure 5.20b mention that the percentage improvement with respect to RPL is 68.60.

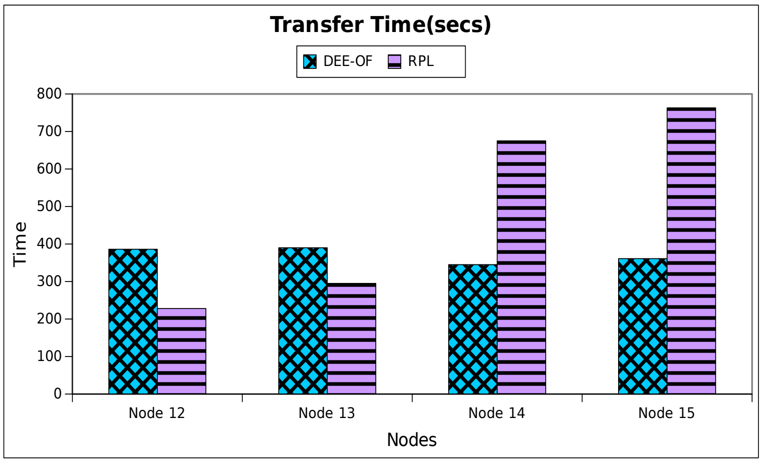


(a) Latency

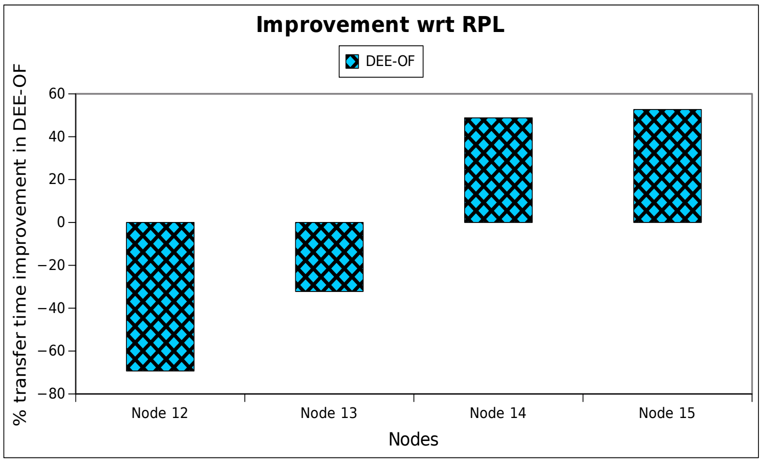


(b) Latency improvement

Figure 5.18: Performance Metrics of Latency in DEE-OF

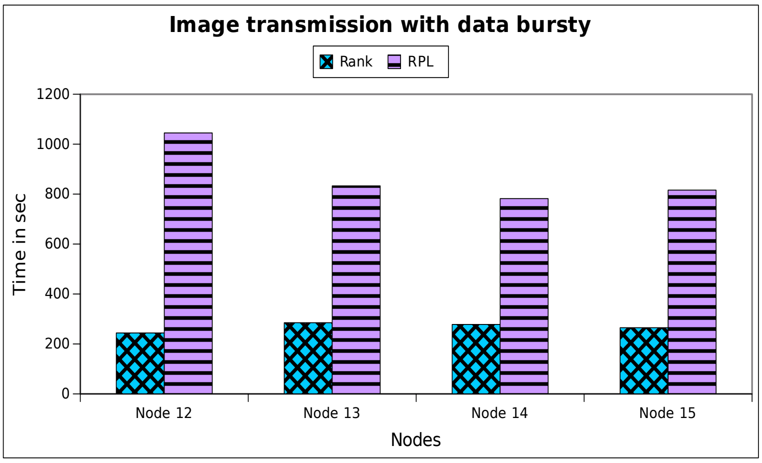


(a) Transfer Time

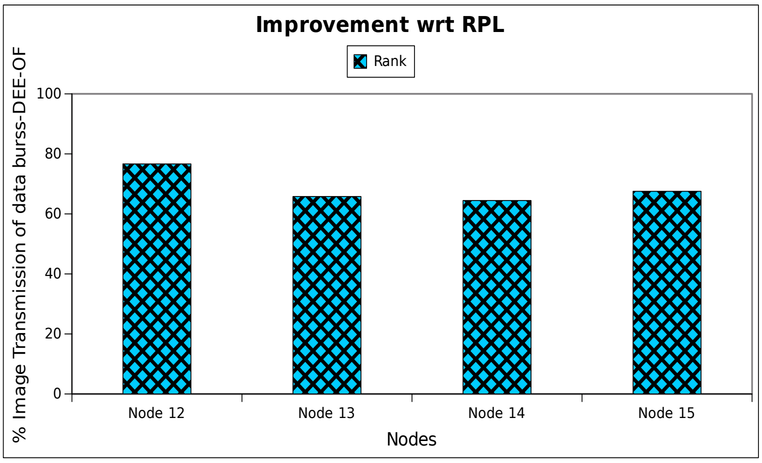


(b) Transfer time improvement

Figure 5.19: Performance of Image Transmission Time



(a) Image Transmission



(b) Image Transmission improvement

Figure 5.20: Performance of Image Transmission with Data Burst

5.4 Summary

In a low power lossy network running RPL, packets being forwarded are not prioritized. In case of congestion, packets are dropped without any consideration to the type of the packet. Based on the network type, it can lead to lower network lifetime or higher drops and re-transmissions. The proposed technique is used where the neighbors are ranked based on various network metrics and packets are prioritized based on these ranks increasing the quality and lifetime of the network.

Chapter 6

Multicast Group Management based RPL for Point-to-Multipoint Multimodal Data Communication

An IoT network comprises of heterogeneous set of IoT nodes. Each of these nodes houses one or more sensors. With the advancement in semiconductor technology, a variety of low-end devices are becoming part of the Internet. The scale of such devices is huge and to help (Kharrufa *et al.*, 2019) connect them to the Internet is challenge. In order to leverage the Internet protocol (IP) which is the backbone of the Internet to connect such devices, IETF developed the IPv6 low-power wireless personal area networks (6LoWPAN) which is used as an adaptation layer on top of the IP stack. This adaptation layer enables the use of new routing protocols that can connect the low-end devices to the Internet. The design paradigms of conventional routing protocols does not fit well in the world of Internet of Things (IoT).

RPL is an IPv6 based routing protocol designed specifically for Low-Power and Lossy Networks. RPL is designed with the goal to connect millions of resource-scarce devices. It uses a Destination Oriented Directed Acyclic Graph (DODAG) topology and enable nodes in the network to communicate while storing minimal routing state information.

The low-end devices (Verma, 2015) are embedded with multiple sensors and gather a variety of data through these sensors. The devices don't have a lot of memory or compute to store and process these information. Additionally, they don't have a big energy store to keep the sensors turned on all the time. A remote node controls the state of the sensors on each node. It also periodically collects the sensor data from all the nodes for storage and processing.

The remote node uses multicast frames to control or query multiple nodes at the same time. Multicast allows a single source to communicate with a set of destinations using reduced number of network resources. The frames are destined to a multicast address based on the sensor being controlled or queried. The multicast address used for a sensor may not be static. Also, multiple sensors can be controlled or queried with the same multicast address.

1. The node responds back to the query if the query is for a sensor it supports.

2. The node forwards the query further down the network.

While this workflow does work, it suffers from 2 major drawbacks.

1. Each node must be statically configured with all the multicast addresses that can be used for queries. This increases the size of the multicast address table required on the node and the size of the multicast routing table on the upstream nodes.

2. The queries can land on parts of the network that don't support any of the sensors that it is intended for wasting the network bandwidth and in turn energy.

Address compression and sensor grouping scheme is proposed to optimise the routing table and query dissemination.

6.1 Related Work

In the paper Oikonomou *et al.* (2013) discusses the various challenges of adopting multicast in IPv6 networks with resource constrained devices. Trickle Multicast (TM), the multicast protocol for low power and lossy networks, is a step in the right direction to address some of the challenges in adopting multicast in such networks. TM uses flooding governed by the trickle algorithm. Trickle is a technique wherein the frequency of periodic information exchange between neighbor nodes decreases exponentially when they share the same status. This saves energy and improves the bandwidth efficiency. When a change is discovered, the trickle timer is reset to a minimum interval to ensure the change is propagated to all the neighbors within milliseconds and they can converge to the same status. Each node in the network broadcasts the multicast packets to all of its neighbors. A sequence number is associated with every packet as an extension option inside the IPv6 header to ensure there are no duplicate multicast packets in the network. It's merits include it can fit alongside any routing protocol without any modifications, it guarantees a higher packet delivery ratio with no duplicates, While TM has its merits, it also has certain shortcomings which include lack of scalability due to maintenance of per packet state information, low in performance due to delays in forwarding a frame to ensure there are no duplicates, lack of topology maintenance that results in the packets to be flooded in the entire network irrespective of if it's needed or not, susceptibility to out of order packets.

The the paper Oikonomou and Phillips (2012) introduces stateless multicast RPL forwarding algorithm (SMRF), that is designed to overcome the shortcoming of the current multicast solutions for low power lossy networks. Nodes in a RPL network exchange topology information to build a Destination Oriented Directed Acyclic Graph (DODAG) and SMRF leverages this property of RPL for efficient multicast forwarding. When the storing mode of operation is used in RPL, nodes join a multicast group advertising it's address in the outgoing DAO messages upward in the tree. The nodes that receive this message make an entry for this multicast address in their routing table. The node then advertises this address in it's own DAO messages and also forwards any frames destined to this multicast address downward in the tree.

This suffers from two drawbacks - there is no way to stop a node from accepting the same datagram more than once, the node needs to transmit the same multicast frame multiple times, once for every node that is participating in this multicast address group. SMRF overcomes both these drawbacks by - accepting multicast frames on a node only if received from it's preferred parent, forward the multicast frame further only if there is an entry for that specific address in it's multicast routing table.

The performance of TM and SMRF is compared for several metrics including packet delivery ratio, end-to-end delay, out-of-order datagram delivery ratio and energy consumption. Four different topologies, one line and three tree topologies are used for comparisons. The results show SMRF in exchange for an occasional slight reliability drop is both faster and more energy efficient.

The the paper Abdel Fadeel and El Sayed (2015) introduces Enhanced Stateless Multicast RPL Forwarding (ESMRF), which is an improvement over the existing SMRF scheme. SMRF suffers from a drawback. The multicast traffic can only flow downwards in the RPL tree. In other words, while the source of the multicast stream can be anywhere in the network, it can only stream that data downwards in the RPL tree. Nodes that are sitting above the multicast source node also registered to the same multicast address drop the stream since it isn't received from their preferred parent. ESMRF eliminates this limitation and allows the multicast traffic to traverse both upward and downward a RPL tree. While ESMRF reuses the same acceptance and forwarding model of SMRF, it adds multicast-on-behalf features at the RPL DODAG root.

For a node to send a multicast data frame, the packet is encapsulated inside an Internet Control Message Protocol version 6 (ICMPv6) header and redirected to the root of the tree. The root of the tree then decapsulates the ICMPv6 header and forwards the multicast frame down in the network. SMRF and ESMRF share similar characteristics. But with ESMRF, the multicast source can be any node in the RPL tree and not just the root node. The drawback of ESMRF is that all of the multicast traffic in the network is routed through the root node of the RPL tree.

In the paper Hwang *et al.* (2020) mention multicast in RPL focus on routing issues and still many challenges has been left out. To create a multicast tree for effective routing author proposed a wireless shortest path heuristic (W-SPH) mechanism. The paper talks about increasing the reliability of the multicast, thus introducing proactive multicast forwarding with RPL (PMFR). Also compared the proposed results with MPL and ESMRF and achieved higher PDR and reduction in the energy consumption.

The following are the research gaps of different multicast protocols.

1. The size of the multicast address table and multicast routing table increases.

2. Packets are forwarded to nodes that are not interested in it.

6.2 Multicast Address Groups for Sensors

Each node can have multiple type of sensors like temperature, humidity etc. If the publish subscribe mode is used for accessing data from different types of sensors, multicast address will help for grouping the sensors. In network a query must be forwarded to the nodes which has those sensors whose data is requested in the query.

A query is generally destined to one or more sensors. A multicast group address is reserved in the network for a group of sensors. When the base station queries any of the sensor in this sensor group, it should direct the query to the reserved multicast address.

For example, consider an IoT network with 3 types of nodes - Cameras, Smart-Lights and Thermometers in Table 6.1. The following table lists the various sensors each of these 3 devices supports.

Table 6.1: Sensors Supported on Devices

IoT Devices	**Sensors**					
	Battery	**LED**	**Button**	**Image**	**Light**	**Temperature**
Camera	Y	Y	N	Y	N	N
Smart-Light	Y	Y	Y	N	Y	N
Thermometer	Y	Y	Y	N	N	Y

Since all 3 devices has battery and LED sensors and 2 of the 3 have a button sensor, these 3 sensors can be grouped and assigned a multicast group address. Each of image, light and temperature sensor can be assigned an individual multicast group address.

This scheme allows for multicast group addresses to be shared between sensors reducing the scale requirement of the multicast address and routing tables while still providing isolation between different sensors when needed.

Sub-sections 6.2.1 to 6.2.6 describe the various aspects of the solution proposed in this work. It includes

1. A new RPL sub-option to advertise sensor groups in the network is introduced.

2. Grouping sensors to multicast addresses and group advertisement.

3. Nodes joining and leaving groups based on the sensors associated with a group.

4. Multicast route lifetime management.

5. Multicast address compression to reduce the size of the DIO when advertising multicast groups.

6. Examples of different grouping schemes.

6.2.1 Multicast Sensor Group Advertisement

A sensor group (Hawbani *et al.*, 2013) is a set of sensors that share the same multicast group address. Each sensor is assigned an integer value. A bitmap is used to represent a group of sensors where the bit associated with a sensor is set if the sensor is part of the group. While there is no restriction on how sensors can be grouped, the general thumb rule is to group sensors that are part of a particular node type. Two sensors that are not common to a node type are generally not grouped together. This ensures queries to sensors are not broadcasted to parts of the network that don't have a node supporting such a sensor.

In RPL, a DIO message as shown in Figure 6.1 can be used to distribute this information to the entire network. A DIO message can carry several different sub-options. Each sub-option is meant to carry specific information. To share the various multicast sensor groups, a new RPL sub-option is introduced as shown in Figure 6.1. Each multicast address is followed by a bitmap of sensors that are mapped to that multicast address. The size of the RPL sub-option will be based on the number of sensor groups in the network.

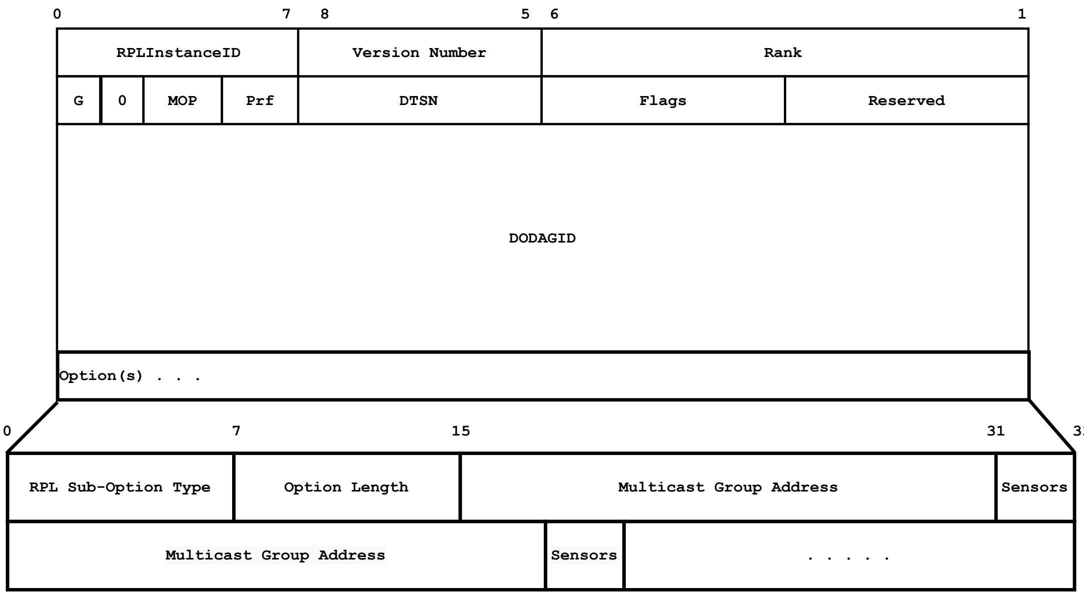


Figure 6.1: DIO - Message Format (Winter, 2012) followed by DIO - New RPL Sub Option

The payload of the sub-option is a set of 'N' multicast group address + sensors associated with the address.

6.2.1.1 Multicast Group Address and Sensors

The IPv6 multicast address that will be used as the destination address in the query packets. The address could be compressed to save space. The details on the compression scheme is described in Section 6.3.4.

The sensors is a bitmap representing all the sensors that will be queried using this mutlicast group address. The following table lists a sample on the bits assigned for each sensor in Table 6.2.

Table 6.2: Bit map

Sensors	Bit
Battery	1
LED	2
Button	3
Image	4
Light	5
Temperature	6

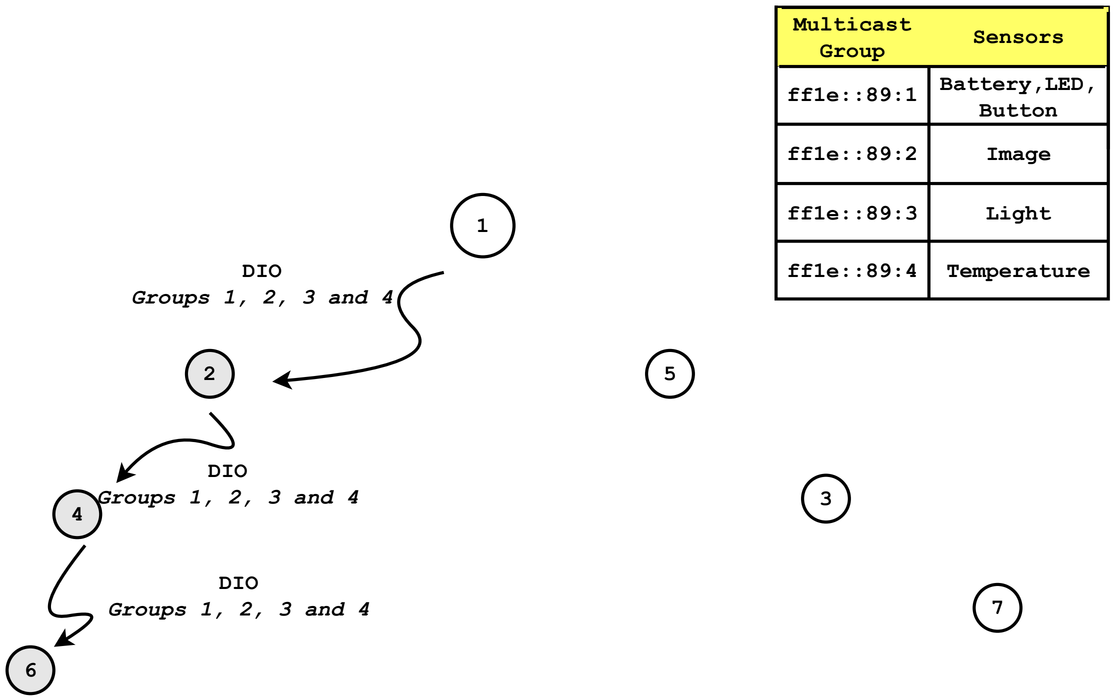


Figure 6.2: Multicast Group Advertisement

The root of the RPL network will advertise all the different groups via this sub-option. Each node in the DAG further propagates this information to the other nodes in the network ensuring the entire network is aware of the various multicast group addresses available and the sensors attached to each as shown in Figure 6.2.

6.2.2 Multicast Sensor Group Join and Leave

When a node receives a DIO with this information for the first time, it looks for group addresses it should register to or 'join' to receive queries based on the sensors it supports. To join a group, the existing RPL mechanism in storing mode is used where the node sends a DAO message to it's parent as shown in Figure 6.3.

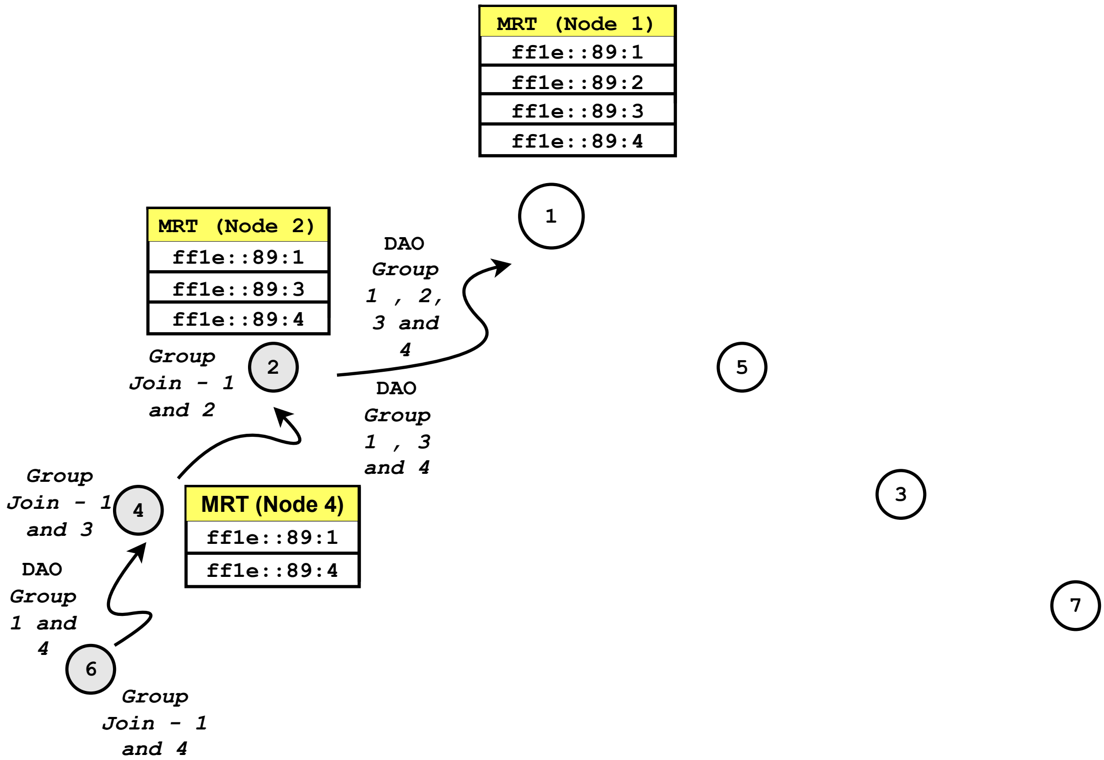


Figure 6.3: Multicast Sensor Group Join

When a node joins a group, it sends a DAO message to it's parent to indicate it's interest in the given group address using the RPL Target and Transit Information sub-options. When the parent receives the DAO, it adds the multicast group address in it's multicast routing table. This enables the parent to forward any packets destined to that multicast group address to it's child.

On receiving a DIO without a multicast group that the node has currently joined as shown in Figure 6.4, it 'leaves' the group by sending a DAO to the parent with the RPL Target set to the multicast address it wants to leave and the lifetime set to 0 in the Transit Information sub-option. On receiving the DAO, the parent removes the multicast group address from it's multicast routing table as shown in Figure 6.5.

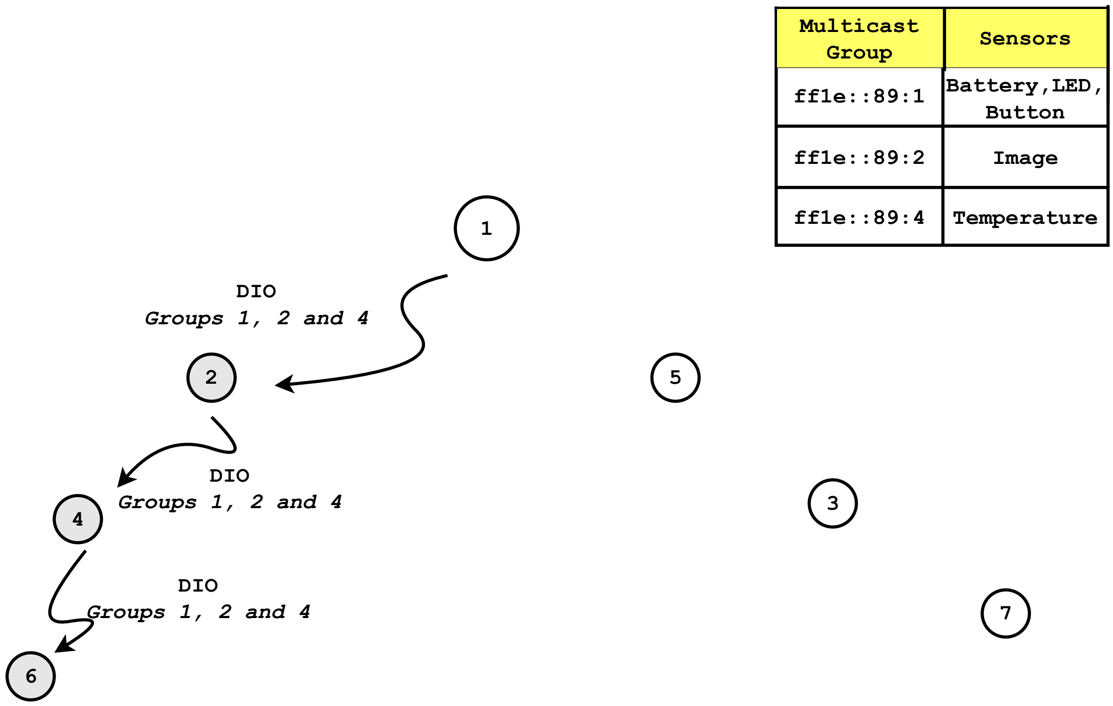


Figure 6.4: Multicast Sensor Group Update

Algorithm 3 Route Refresh Timer Expire

Input: Multicast Address Table
Output: DAO Packets

Mcast-Addr-Record = HEAD(Mcast−Addr−Table)
while $Mcast - Addr - Record! = NULL$ **do**
  Mcast-Group-Addr = Mcast-Addr-Record.Group-Addr
  DAO.RPL−Target.Prefix = Mcast-Group-Addr
  DAO.Lifetime = Default-Mcast-Route-Lifetime
  Send(DAO)
end while

6.2.3 Multicast Route Refresh

All the multicast routes added in the upstream path when a node joins a multicast group have a lifetime. If a DAO with the same address and a new lifetime is not received before the end of the current lifetime, the routes are purged on the node.

To ensure the routes are not purged, a periodic timer is run on a node that has joined at least one multicast group. At the end of every cycle of this timer, DAOs for each multicast address present in the multicast address table of the node are sent to the parent with a refreshed lifetime. The parent updates the lifetime multicast route for each of these addresses with the new value.

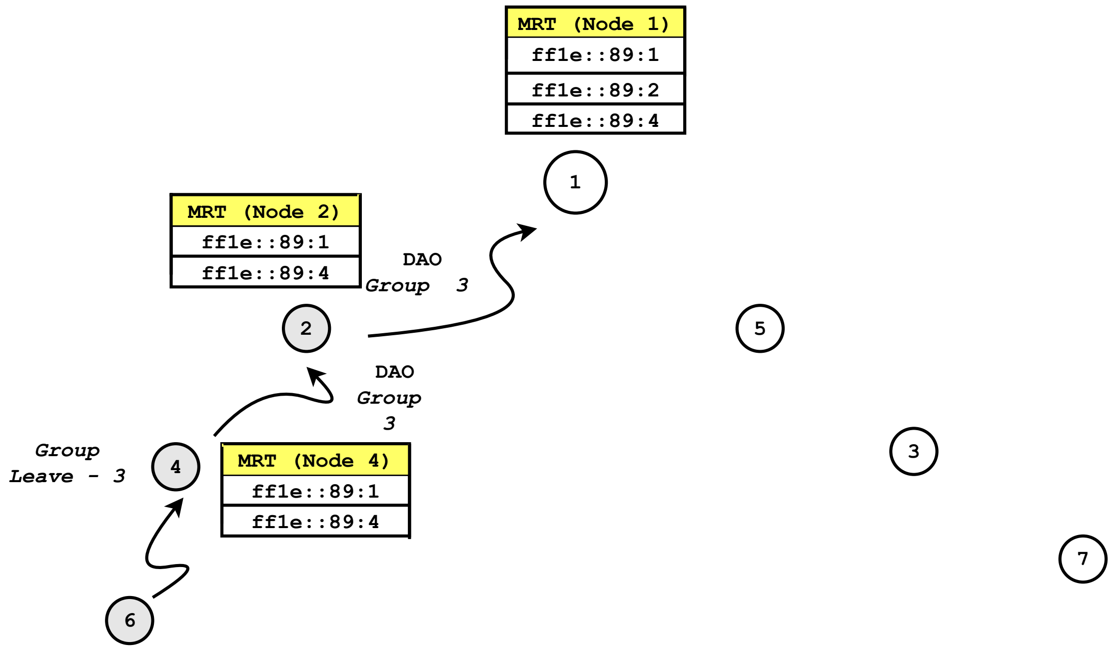


Figure 6.5: Multicast Sensor Group Leave

By default, a lifetime of 180 seconds is assigned to each route. The periodic timer runs every 120 seconds to ensure a DAO is sent before the previous lifetime expires. Algorithm 3 mention about route refresh timer expire and the complexity is O(n).

6.2.4 Proposed Multicast Address Compression

The IPv6 address is 16 bytes long. Encoding a few of these addresses in the Group Advertisement message can cause the DIO message to grow rather large. To workaround this, the IPv6 addresses are compressed when possible.

Most of the IPv6 addresses have one or more consecutive bytes as 0. In this compression scheme as shown in Figure 6.6, if there are consecutive bytes of 0s in the addresses, they are omitted and not encoded in the message. Instead, a one byte metadata is prefixed with the address to indicate the compression details. The format of the metadata is described below.

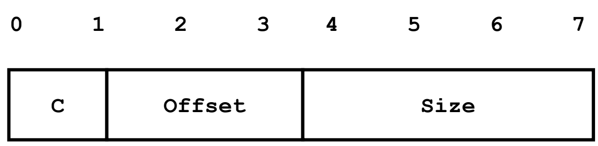


Figure 6.6: IPv6 Address Compression

1. C - Indicates if the IPv6 address following this header is actually compressed. A value of 1 indicates the addresses is compressed. 0 indicates the address is not compressed.

2. Offset - The byte in the IPv6 address where the compression starts.

3. Size - The number of consecutive bytes that is compressed.

Using a compression scheme significantly reduces the size of the DIO messages when advertising group addresses. Example of address compression in Figure 6.7 with this technique is as follows.

Multicast Address: ff1e:0000:0000:0000:0000:0000:0089:0001

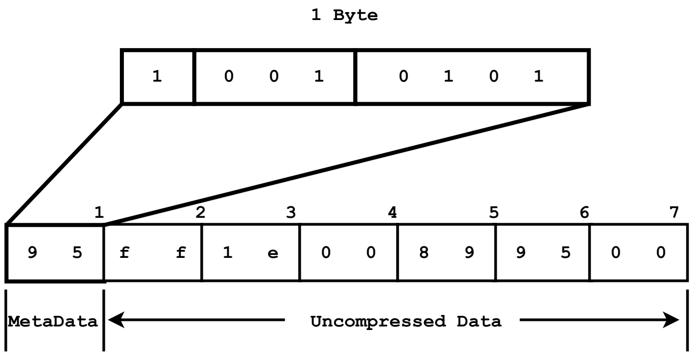


Figure 6.7: Metadata followed by Encoded data (Metadata + Uncompressed data)

6.2.5 New RPL Sub-Option Payload with Different Grouping and Compression Schemes.

The efficiency of this technique is primarily governed by how the different sensors are grouped based on the use case. Addition of a group increases the size of the DIO frame as the group must be encoded in the packet and communicated to the entire network. Define too many groups and the size of the DIO frame gets very large increasing the network overhead in control messages. Group sensors into a single group and the capability to drops frames from making it to parts of networks that is not needed is lost. Thus it is important to pick the strategy for total number of groups and mapping the sensors to those groups. The examples below explore different grouping strategies and their impact on the control overhead introduced.

1. 6 Group Address, 6 Sensors - No compression

Table 6.3: Multicast Group Address to Sensor Mapping

Group	Multicast Address	Sensors
G1	FF1E::89:1	Battery
G2	FF1E::89:2	LED
G3	FF1E::89:3	Button
G4	FF1E::89:4	Image
G5	FF1E::89:5	Light
G6	FF1E::89:6	Temperature

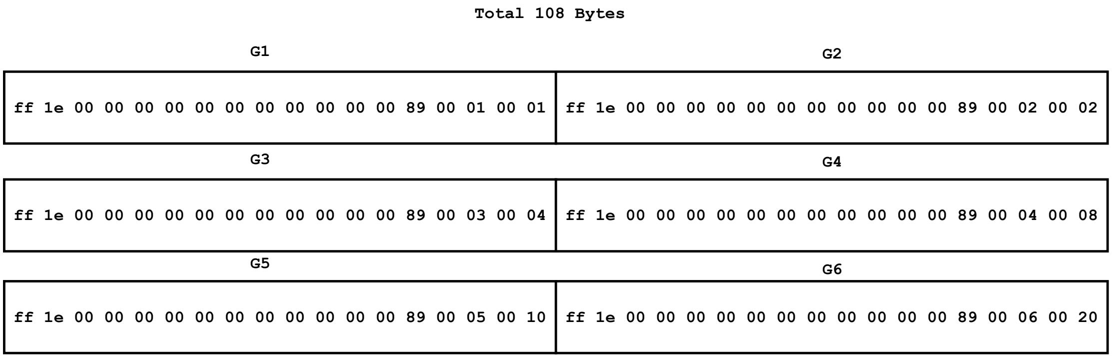


Figure 6.8: Encoded Data

In this scheme as shown in Table 6.3, each of the 6 sensors is assigned its own group address and the IPv6 multicast group addresses are not compressed. Encoding each group information requires a total of 18 bytes, 16 bytes for the IPv6 multicast address associated with the group and 2 bytes for the indicating the sensors mapped to the group. Thus a total of 108 bytes (6 groups * 18 bytes per group) is required to share the group information in a DIO as shown in Figure 6.8.

2. 6 Group Address, 6 Sensors - With compression

Table 6.4: Multicast Group Address to Sensor Mapping

Group	Multicast Address	Sensors
G1	FF1E::89:1	Battery
G2	FF1E::89:2	LED
G3	FF1E::89:3	Button
G4	FF1E::89:4	Image
G5	FF1E::89:5	Light
G6	FF1E::89:6	Temperature

Total - 54 Bytes

G1	G2	G3
95 ff 1e 00 89 00 01 00 01	95 ff 1e 00 89 00 02 00 02	95 ff 1e 00 89 00 03 00 04
G4	**G5**	**G6**
95 ff 1e 00 89 00 04 00 08	95 ff 1e 00 89 00 05 00 10	95 ff 1e 00 89 00 06 00 20

Figure 6.9: Encoded Data

In this scheme as shown in Table 6.4, each of the 6 sensors is assigned its own group address but the IPv6 multicast group addresses are compressed. With the multicast addresses used in the example, encoding each group information requires a total of 9 bytes, 6 bytes for the compressed IPv6 multicast address associated with the group, 1 byte for the compression metadata and 2 bytes for the indicating the sensors mapped to the group. Thus a total of 54 bytes (6 groups * 9 bytes per group) is required to share the group information in a DIO as shown in Figure 6.9.

3. 4 Group Address, 6 Sensors - With compression

Table 6.5: Multicast Group Address to Sensor Mapping

Group	Multicast Address	Sensors
G1	FF1E::89:1	Battery, LED, Button
G2	FF1E::89:2	Image
G3	FF1E::89:3	Light
G4	FF1E::89:4	Temperature

Total - 36 Bytes

G1	G2	G3	G4
95 ff 1e 00 89 00 01 00 07	95 ff 1e 00 89 00 02 00 10	95 ff 1e 00 89 00 03 00 20	95 ff 1e 00 89 00 03 00 08

Figure 6.10: Encoded Data

In this scheme as shown in Table 6.5, 3 of the sensors share the same group address and the other 3 are assigned their own group address. Thus a total of 4 group addresses is used for the same 6 sensors and the IPv6 multicast group address is compressed. With the multicast addresses used in the example, encoding each group information requires a total of 9 bytes, 6 bytes for the compressed IPv6 multicast address associated with the group, 1 byte for the compression metadata and 2 bytes for the indicating the sensors mapped to the group. Thus a total of 36 bytes (4 groups * 9 bytes per group) is required to share the group information in a DIO as shown in Figure 6.10.

From the 3 examples, it is obvious that using an address compression saves a lot of space in the DIO message when advertising the same group information. In addition, sharing the groups between sensors also reduces the number of multicast groups to advertise which in turn reduces the total size of the DIO when advertising the group information.

6.3 Results and Discussion

To compare the performance of group based technique with non-group based, two different topology is used. The first topology, Figure 6.11 uses 7 nodes. Node 1 acting as the base station. Node 2 and 3 acting as cameras. Node 4 and 5 acting as thermometers and Node 6 and 7 acting as light nodes. The second topology, Figure 6.12 uses 15 nodes. Node 1 acting as the base station. Node 2 to Node 6 acting as cameras. Node 7 to Node 11 acting as light nodes and Node 12 to Node 15 acting as thermometers.

Each of these nodes have the sensors as described in Table 6.5.

The multicast address groups to sensors are mapped as follows.

The base station sends a query every 5 seconds to all the scalar sensors. In addition to the scalar sensors, it also sends 2 blocks of the image query to the image sensor. The entire image query is transferred in 32 blocks. In the group based experiment, the base station advertises the multicast group addresses associated with each sensor and the nodes register to only those addresses that it or a downward node to which it is the parent is interested. In the non-group based experiment, the base station does not advertise any groups and each of the devices registers to all the multicast groups statically.

6.3.1 Experiment Conducted using Cooja

Cooja is an open-source, java-based simulator available in Contiki Operating System, it is been known as a very suitable tool for IoT network development. Simulations are conducted in the cooja simulator by using Contiki OS. The proposed

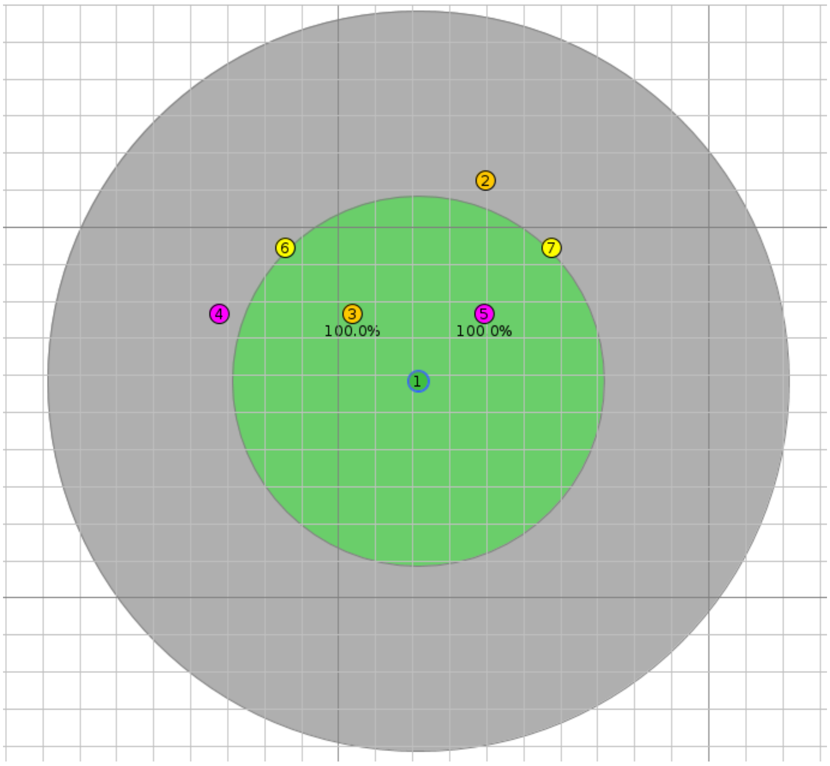


Figure 6.11: Two Level - Topology

model is evaluated in comparison with the existing RPL protocol. Also considered Z1 mote for the experiment. Table 6.6 mention the simulation parameter.

Table 6.6: Simulation Parameter

Simulation Parameter	Values
OS	ContikiOS 3.1
Radio model	Unit disk graph model
Mote type	Z1 Mote
Mode of operation	Storing mode
Network size	100 m x 100 m
Application Program	examples/er-rest-example
Simulation time	17mins

6.3.1.1 Tree Topology with Depth 2

Figure 6.13a and Figure 6.13b show the number of queries successfully delivered to each node in both the group based and non group based techniques in the two level topology.

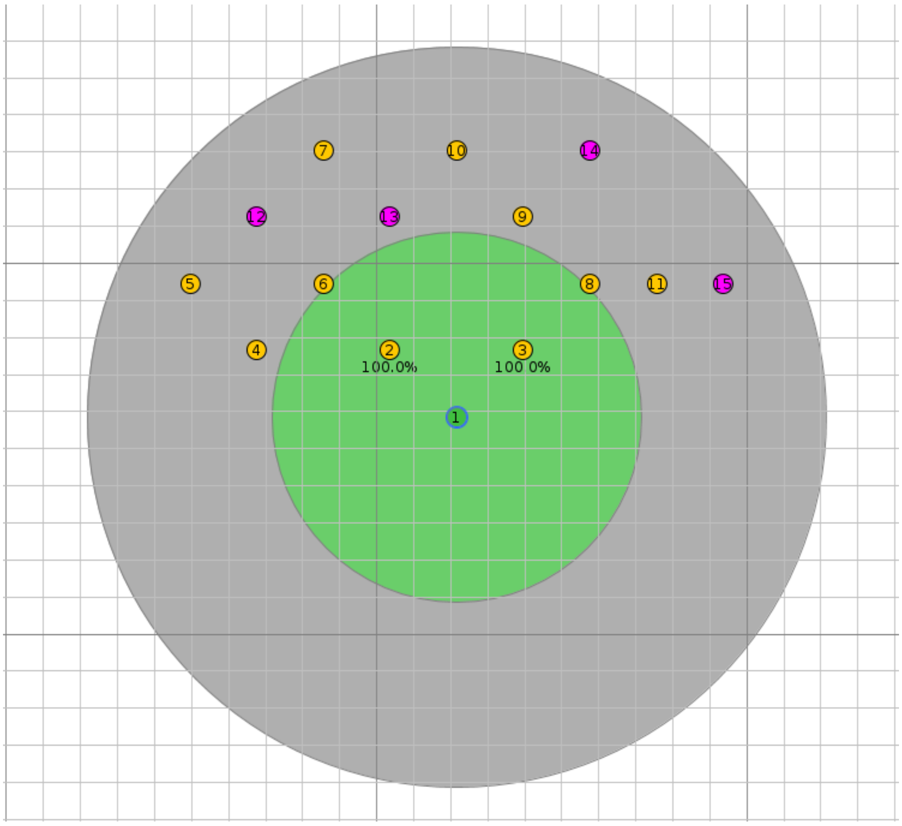


Figure 6.12: Three level - Topology

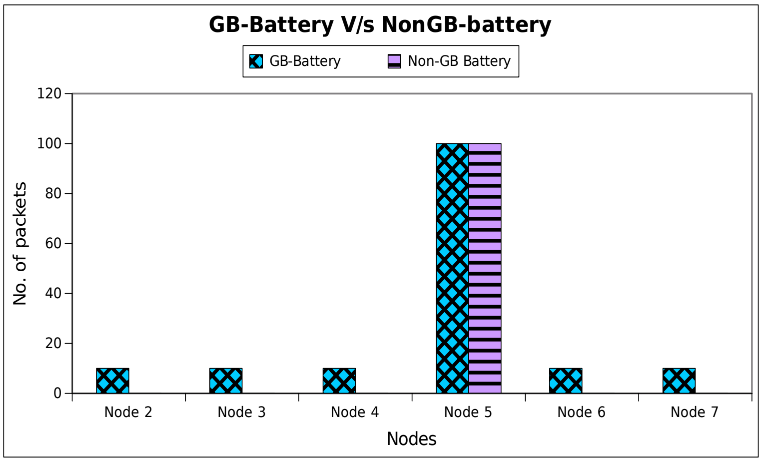
Table 6.7 shows the percentage of improvement in the packet delivery ratio for group based technique over non group based technique.

Table 6.7: PDR Improvement with respect to RPL

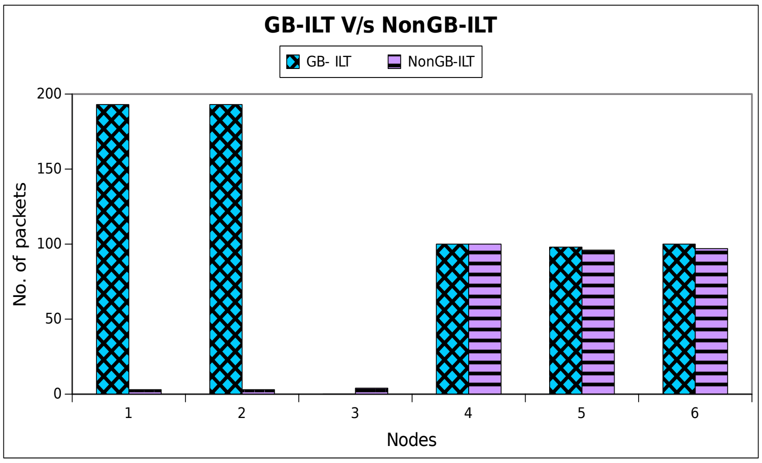
Sensors	Improvements %
Battery	83.33
Image	98.44
Light	0
Temperature	2.52

6.3.1.2 Packet Transmission - Tree Topology with Depth 2

The base station sends one query to each sensor every 10 seconds. A total of 100 queries are sent to each sensor in the simulation. Comparison has been made between NonGroup-based and Group-based group registration for packet transmission of packet is shown in Figure 6.14a. Percentage improvement in Figure 6.14b with respect to NonGroup-based group registration is 35.03.

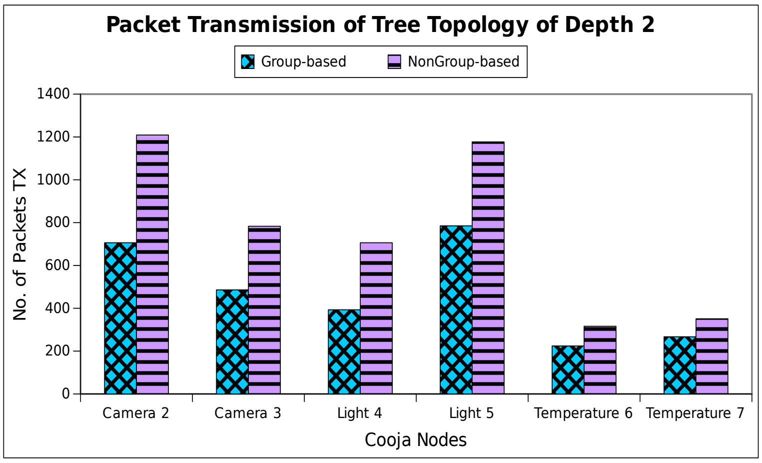


(a) Queries Delivered - Battery

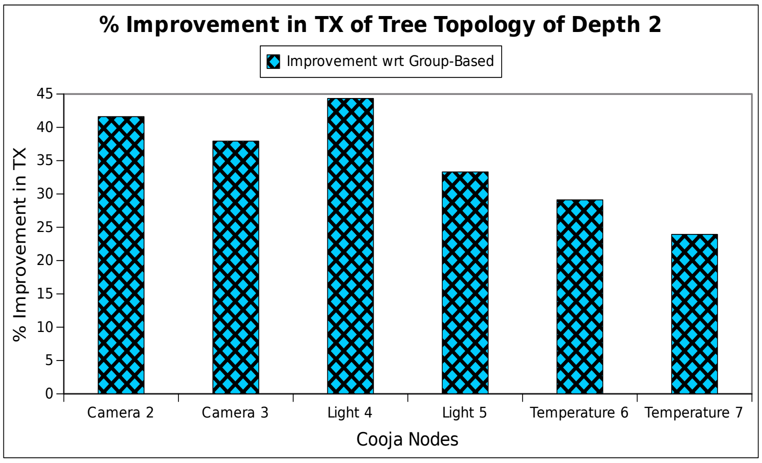


(b) Queries Delivered - ILT

Figure 6.13: Performance of Tree Topology of depth 2 - battery and Image, Temperature and Light



(a) Packet Transmission

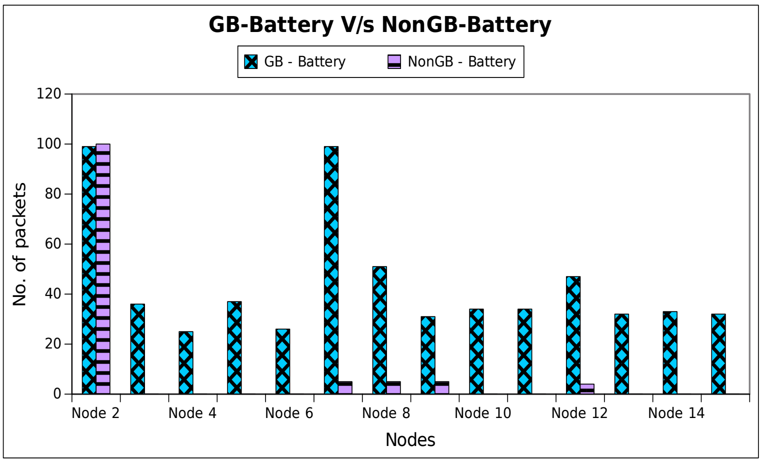


(b) Improvement

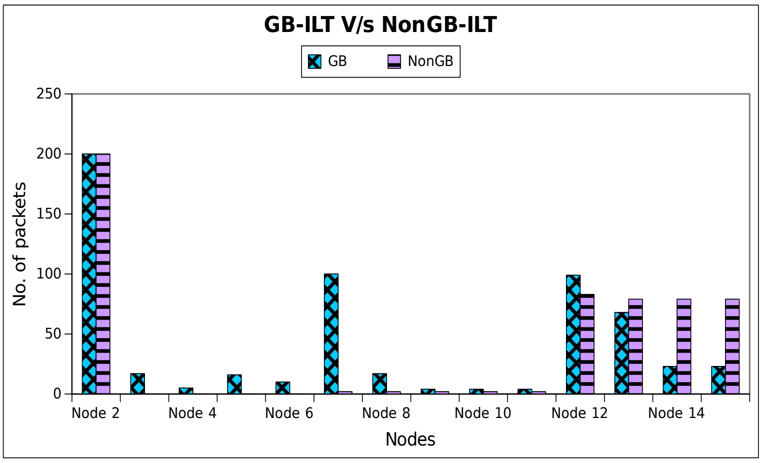
Figure 6.14: Performance of Packet Transmission

6.3.1.3 Tree Topology with Depth 3

Figure 6.15a and Figure 6.15b show the number of queries successfully delivered to each node in both the group based and non group based techniques in the three level topology.



(a) Queries Delivered - Battery



(b) Queries Delivered - ILT

Figure 6.15: Performance of Tree Topology of Depth 3 Battery and Image, Temperature and Light

Table 6.8 shows the percentage of improvement in the packet delivery ratio for group based technique over non group based technique.

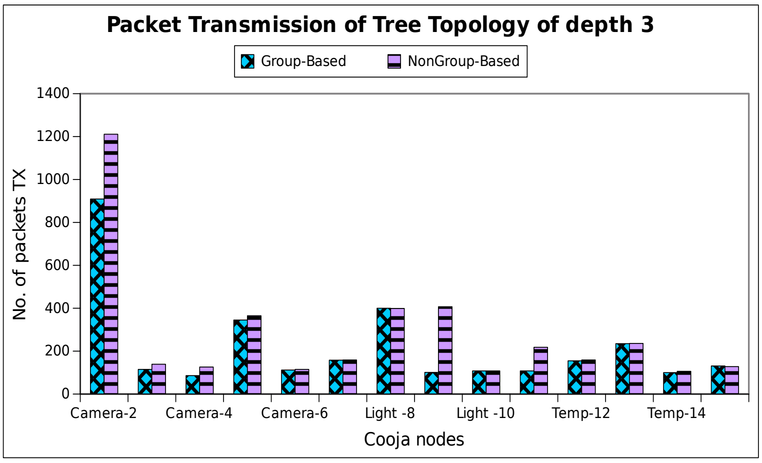
6.3.1.4 Packet Transmission - Tree Topology with Depth 3

The base station sends one query to each sensor every 10 seconds. A total of 100 queries are sent to each sensor in the simulation. Comparison has been made between NonGroup-based and Group-based group registration for packet trans-

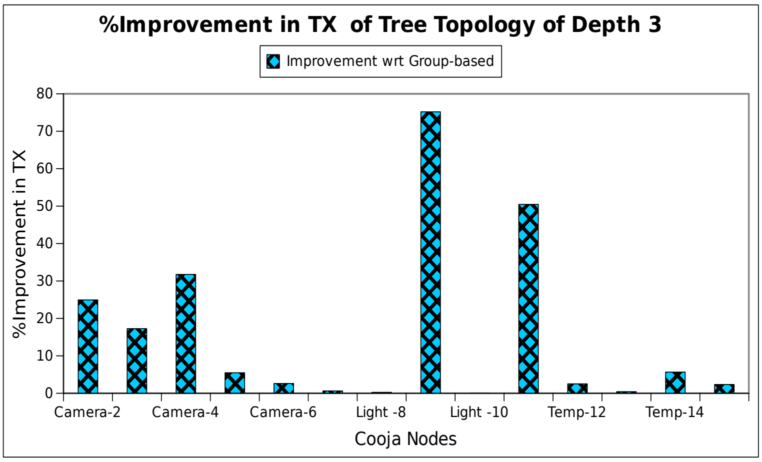
Table 6.8: Improvement % with respect to RPL

Sensors	Improvements %
Battery	89.86
Image	80
Light	67.24
Temperature	31 more packets in NonGB

mission of packet is shown in Figure 6.16a. Percentage improvement in Figure 6.16b with respect to NonGroup-based group registration is 28.18.



(a) Packet Transmission



(b) Improvement

Figure 6.16: Performance of Packet Transmission

6.4 Summary

In RPL based IoT networks, a popular workflow is for the base stations to query sensors deployed across the entire network. For efficient operations, these queries are directed to multicast addresses to ensure they get delivered to all the nodes on the network without the need of maintaining states at each node. But there isn't any good multicast group management schema today in RPL to manage the use of these multicast groups in the network. The proposed work attempts to define a simple multicast group management scheme to manage the various multicast addresses used when querying these sensors including group advertisement and registrations.

The results of the experiments on both Cooja and FiT-IoT indicate that the group based technique offers better performance in terms of packet delivery ratio which in turn reduces the energy consumed to transmit the same of amount of data extending the lifetime of the network.

Chapter 7

Performance Analysis using FiT-IoT LAB

IoT-LAB (Adjih *et al.*, 2015) is a framework with a real world IoT testbed enabling researchers around the world to validate their work in the areas of but not limited to wireless communications, sensor networks and low power routing protocols. The testbed is setup in seven different sites in the country of France. The connectivity to the nodes in the FIT-IoT testbeds required to control them is provided by a global networking backbone as shown in Figure 7.1.

Any FIT-IoT node is comprised of three components - 1. Open Nodes 2. Gateway Nodes 3. Control Nodes

FIT-IoT supports the integration of embedded software, ranging from direct access to node hardware, to operating system (OS). The open nodes can be used to run different operating systems with a certain level of software maturity given the node is capable to support it. Currently, FIT-IoT has support for five popular IoT operating systems that include Contiki, FreeRTOS, RIoT, OpenWSN and TinyOS as shown in Table 7.1 .

Table 7.1: Supported Operating System

OS	**WSN430 Node**	**M3 Node**	**A8 Node**
RIoT	✓	✓	X
OpenWSN	✓	✓	X
FreeRTOS	✓	✓	X
Contiki	✓	✓	X
TinyOS	✓	X	X
Linux	X	X	✓

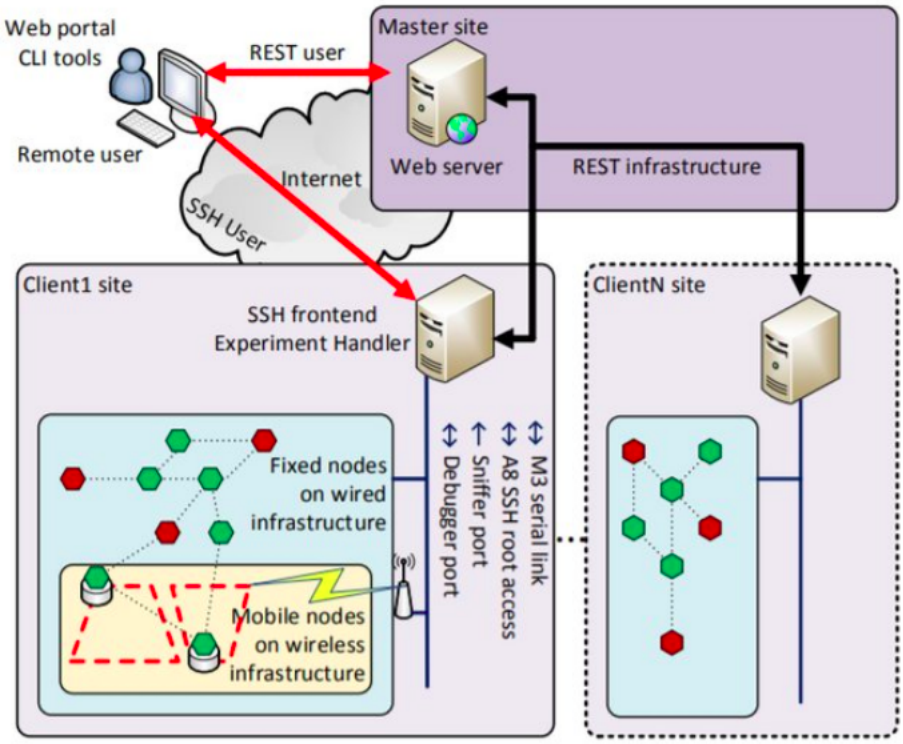


Figure 7.1: IoT-LAB Infrastructure (Adjih *et al.*, 2015)

The FIT-IoT testbed also supports three different types of nodes.

1. WSN430 - 16-bit MSP430F1611 micro-controller, a CC2420 (2.4GHz version) or CC1101 (868MHz version) radio chip, and sensors (light/temperature)

2. M3 - 32-bit ARM Cortex M3 micro-controller (STM32F103REY), an AT86RF231 IEEE802.15.4 radio chip, and sensors. This node is representative of most of today's advanced IoT nodes.

3. A8 - 32-bit ARM Cortex-A8 600 MHz mini-computer, a 32-bit ARM Cortex-M3 micro-controller, an AT86RF231 IEEE802.15.4 radio chip and sensors. This is the most powerful node in the IoT lab and representative of devices like set-top boxed and smartphones capable of running Linux or Android.

The Iot-LAB allows multiple nodes to be reserved at one or several sites and offers the following services.

1. Total access to the remote nodes. This includes allowing users to flash and install the firmware of their choice on the nodes.

2. Access to a debugger server on the node to debug the firmware on the node remotely.

3. Access to serial ports on all the nodes for real-time interaction.

4. Access to an accurate power consumption monitoring tool on all the nodes.

5. Access to a packet sniffer and analyzer on all the nodes.

6. End to end IPv6 and 6LoWPAN connectivity.

7. Tutorials and documentation on how to access and use the testbed.

The users of the lab are encouraged to share their experience of using the framework and any improvement ideas for the framework. The experiment is executed in the IoT-LAB site located in Lille, France. The ARM-Cortex based M3 nodes are selected in the testbed. The M3 node has an ARM M3-Cortex microcontroller, 64kB RAM, IEEE 802.15.4 radio AT86RF231, a rechargeable 3.7 V LiPo Battery, and several types of sensors. The coordinates used for the nodes in FiT-IoT lab is the same as used in Cooja simulation.

Around 7 nodes are utilised in level 2 topology and 15 nodes in level 3 topology. The coordinates used in FiT-IoT lab is the same used in Cooja simulation.

7.1 Running a Custom Contiki Firmware in FiT-IoT

1. Create a user account in FIT-IoT

2. Login into the IoT-LAB environment with user credentials

```
$   ssh <login>@<site>.iot-lab.info
```

3. Clone the IoT-Lab code from Github

```
$ <login>@<site>~$
```

git clone https://github.com/iot-lab/iot-lab.git
Cloning into 'iot-lab'...
...

```
$ <login>@<site>~ cd iot-lab
```

4. Setup the Contiki target

```
$ make setup-contiki
$ <login>@<site>:~/iot-lab
$ make setup-contiki
```

git clone https://github.com/iot-lab/contiki.gitparts/contiki
Cloning into parts/contiki...
...

```
$ <login>@<site>:~/iot-lab$ cd parts/contiki
```

5. Apply the patch with all the enhancements to Contiki

```
$ <login>@<site>:~/iot-lab/parts/contiki$ git apply multimodal-enhancements.patch
```

6. Go to the example program that will be used as a base for the experiment

```
$ <login>@<site>:~/iot-lab/parts/contiki
$ cd examples/iotlab/04-er-rest-example/
```

7. Make the required changes to the example program
8. Compile the Contiki images for M3 node target for different node profiles

```
$ <login>@<site>:~/iot-lab/parts/contiki/examples/iotlab/04-er-rest-example
$ make TARGET=iotlab-m3
```

9. Upload the firmwares for different node profiles to IoT-Lab via Web Portal https://www.iot-lab.info/testbed/resources/firmware
10. Setup the topology in one of the IoT-Lab sites and use the nodes with the custom fimrware and submit the experiment with the required duration.

7.2 Analysis of Proposed Multipoint-to-Point Algorithm with FiT-IoT

The experiments use 3 different types of nodes. A light node that includes a light and battery sensor. A temperature node that includes a temperature and battery sensor. And finally a camera node that includes an image and battery sensor. The experiments also include a sink node that acts as a base station. In the experiment, all the different sensor nodes push sensor data periodically to the base station. The energy and data-rate associated with each of the node type is different. This affects the weighted ranks assigned to each node and thus how the packets are prioritized and forwarded in the network. The experiments capture the total number of packets sent in the network and the time taken to complete the data transfer.

7.2.1 Tree Topology with Depth 2 - Cooja Results

In level 2 topology Figure 7.2, one root node(green), 2 light nodes(yellow), 2 camera nodes(dark yellow) and 2 temperature nodes(purple) has been used in Cooja setup. Considering the Figure 7.3, the results are better in FIT IoT nodes when compared to Cooja nodes. The results obtained are similar for R-RPL and RPL in Cooja nodes.

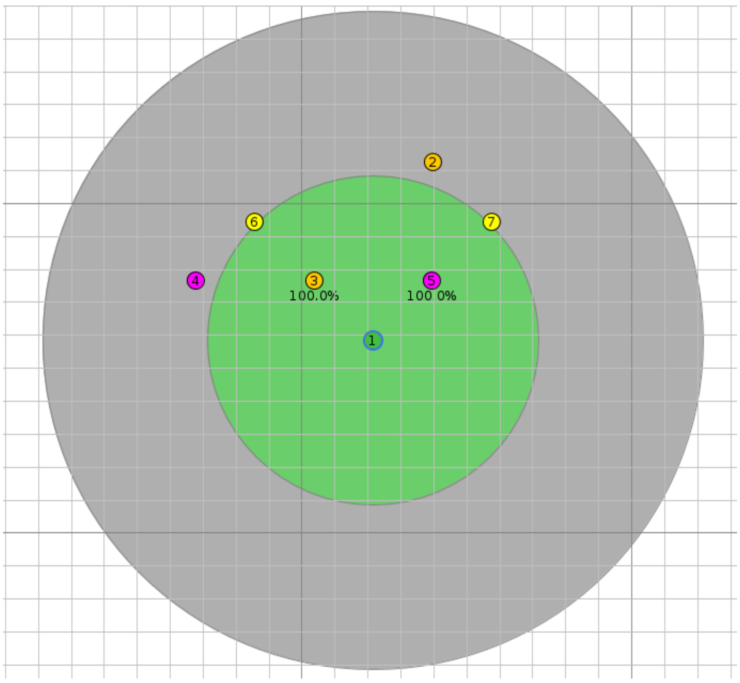


Figure 7.2: Test - Topology

7.2.2 Tree Topology with Depth 2 - FiT-IoT Lab Results

FiT-IoT nodes have been utilized for the performance of MP2P. The improvement of R-RPL with respect to RPL in Figure 7.4 is 5.39%.

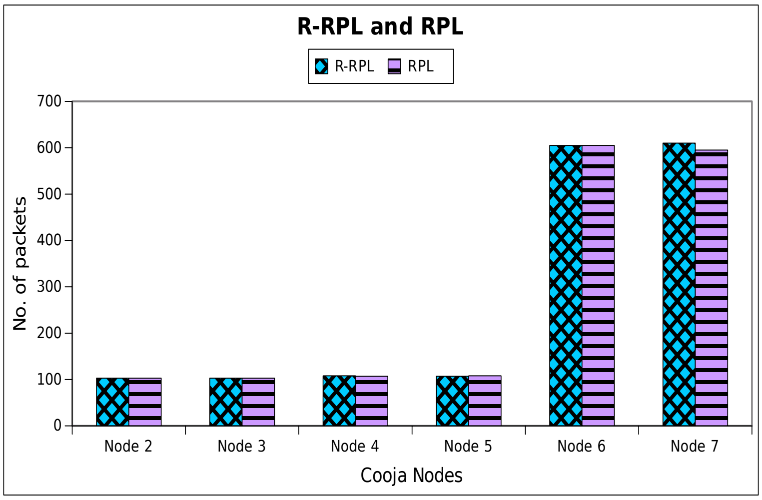


Figure 7.3: Performance of MP2P - Cooja nodes

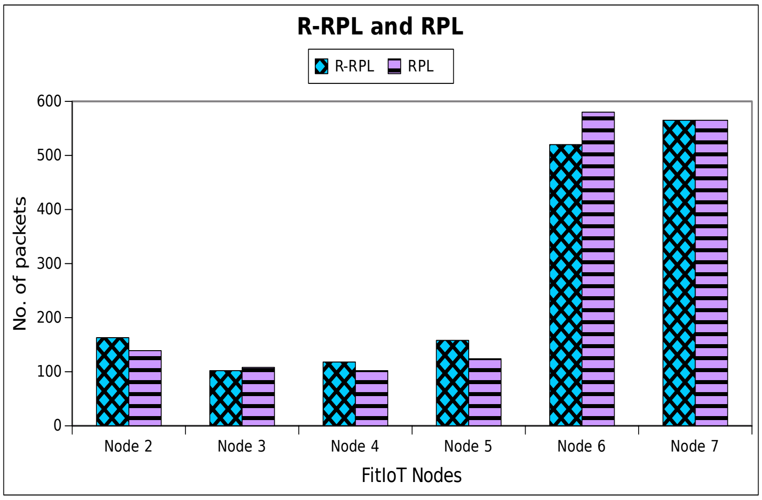


Figure 7.4: Performance of MP2P - FIT-IoT Lab Nodes

7.2.3 Tree Topology with Depth 3 - Cooja Results

In level 3 topology Figure 7.5, one root node(green), 5 light nodes(yellow), 5 camera nodes(Dark yellow) and 4 temperature nodes (purple) has been used in Cooja setup. The improvement of R-RPL with respect to plain RPL in Figure 7.6 is -12.51%. Even though RPL gives better results, time taken by the RPL is 5 times more than the proposed work as shown in Table 7.2

Table 7.2: Time Taken Comparison

Methods	Time taken
R-RPL	6 Minutes
RPL	30 Minutes

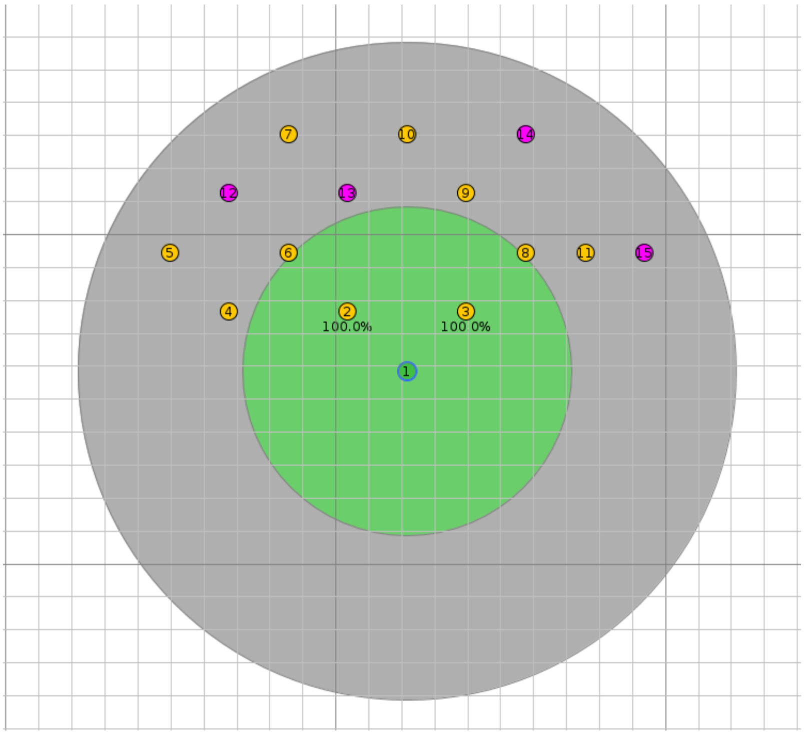


Figure 7.5: Test - Topology

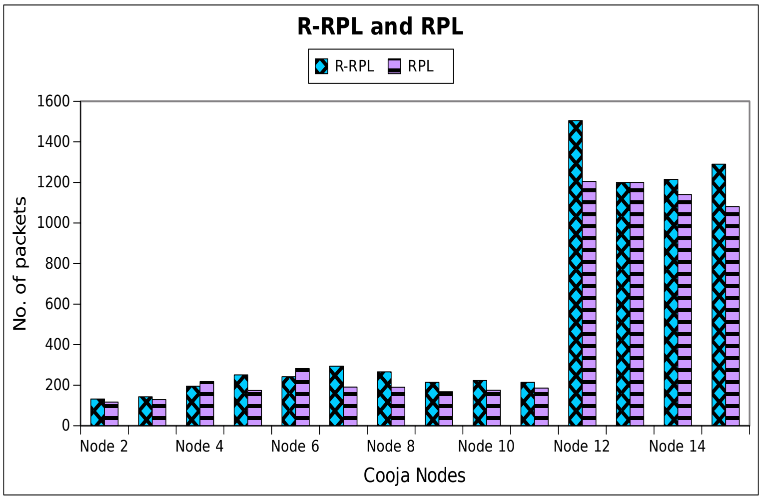


Figure 7.6: Performance of MP2P 3 Level - Cooja Nodes

7.2.4 Tree Topology with Depth 3 - FiT-IoT Lab Results

The improvement of R-RPL with respect to plain RPL in Figure 7.7 is 6.54%.

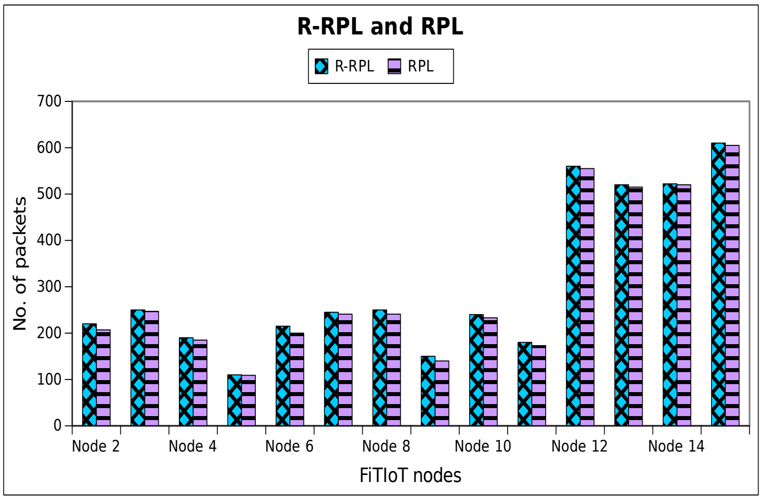


Figure 7.7: Performance of MP2P 3 Level - FiT-IoT Lab Nodes

7.3 Analysis of Proposed Point-to-Multipoint Algorithm with FiT-IoT

The experiments use 3 different types of nodes. A light node that includes a light and battery sensor. A temperature node that includes a temperature and battery sensor. And finally a camera node that includes an image and battery sensor. The experiments also include a sink node that acts as a base station. In the experiment, the base station advertises the multicast groups and then sends out multicast queries to all the different sensor nodes. Based on the grouping scheme used, the total of packets transmitted in the network vary. The experiments capture the total number of packets sent in the network to successfully send queries to all the different sensors.

7.3.1 Tree Topology with Depth 2 - Packet Transmission - Cooja Results

In Figure 7.8, shows the packet transmission using Cooja nodes. Percentage improvement in Figure 7.9 with respect to NonGroup-based group registration is 35.03%.

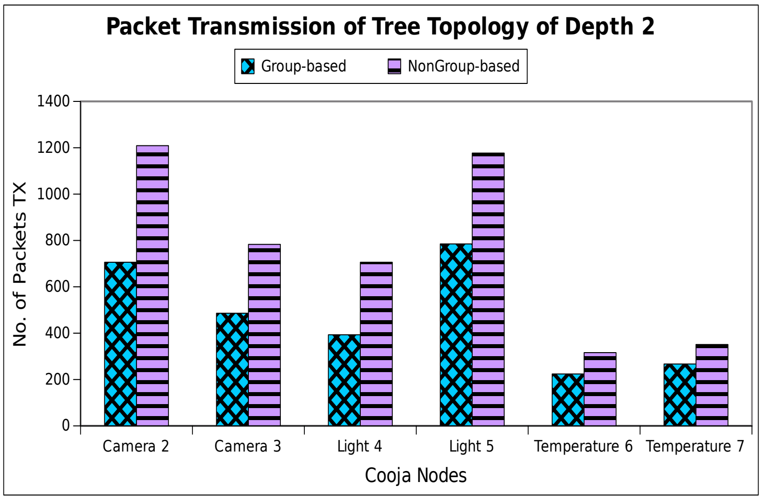


Figure 7.8: Performance of Packet Transmission

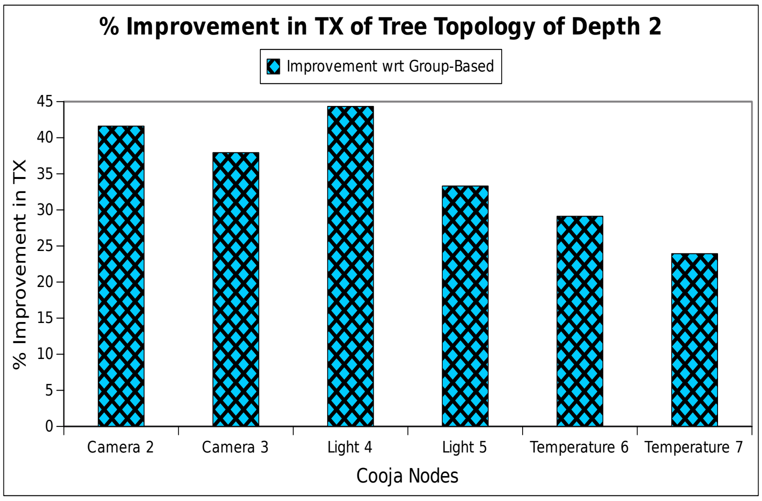


Figure 7.9: % Improvement of Packet Transmission

7.3.2 Tree Topology with Depth 2 - Packet Transmission - FiT-IoT Results

In Figure 7.10, shows the packet transmission using FiT-IoT nodes. FiT-IoT nodes provide better improvement in Transmission in Figure 7.11 with respect to Cooja nodes is 43.54%.

7.3.3 Tree Topology with Depth 2 - Cooja Results

In level 2 topology Figure 7.12, one root node(green), 2 light nodes(yellow), 2 camera nodes(dark yellow) and 2 temperature nodes(purple) has been used in Cooja setup. The performance of 2 level Cooja nodes has been shown in Figure

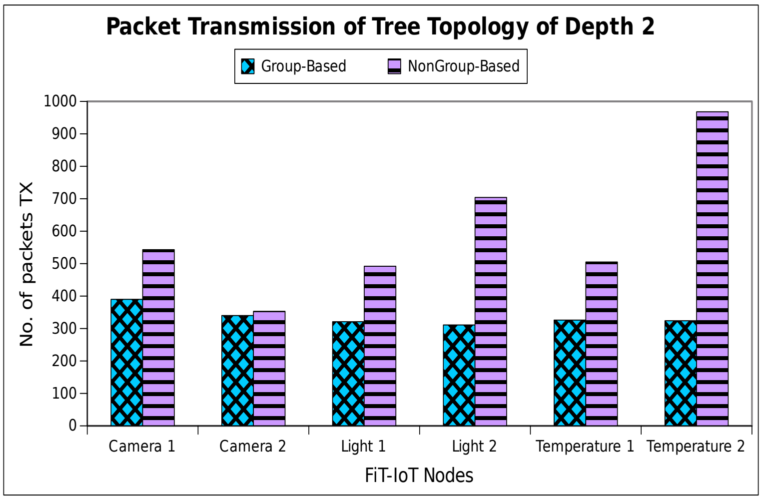


Figure 7.10: Performance of Packet Transmission

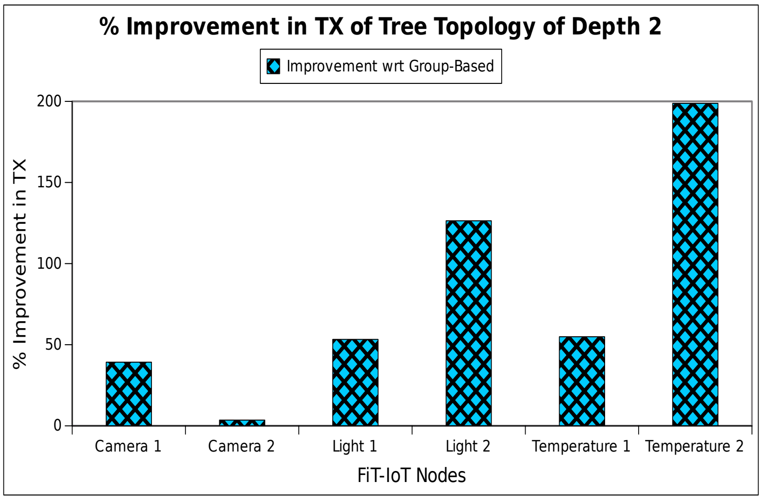


Figure 7.11: % Improvement of Packet Transmission

7.13 and Figure 7.14. The % improvement has been shown in Table 7.3.

Table 7.3: Improvement % Comparison with RPL

Sensors	**Improvements %**
Battery	83.33
Image	98.44
Light	0
Temperature	2.52

7.3.4 Tree Topology with Depth 2 - FiT-IoT Lab Results

The results from the FiT-IoT lab mention that the improvement percentage is comparatively more in the proposed group based technique when compared to

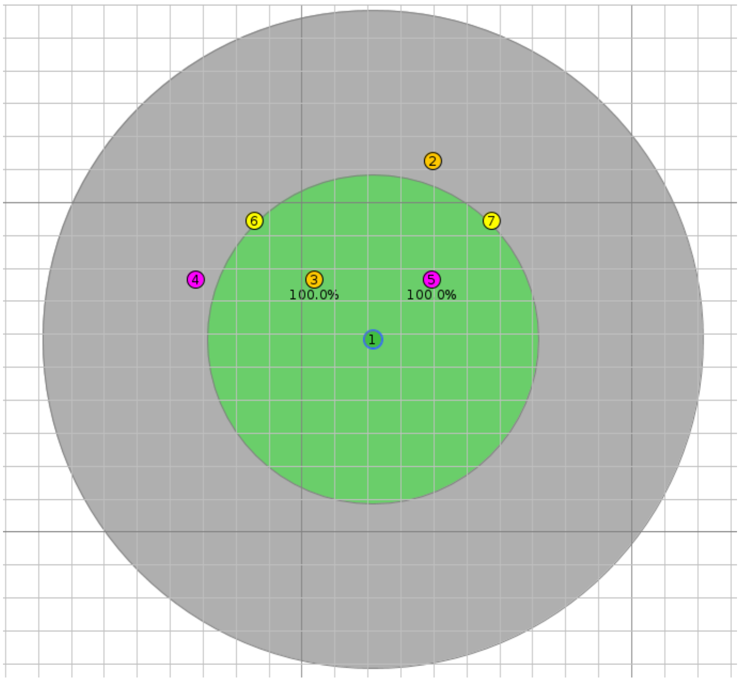


Figure 7.12: Test - Topology

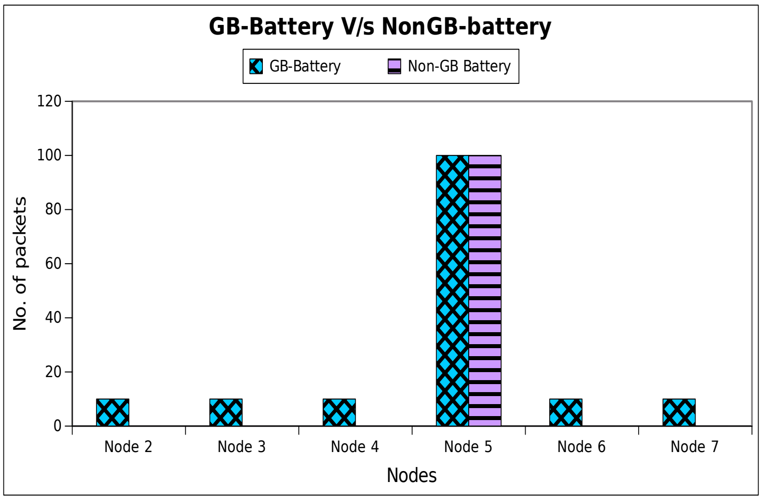


Figure 7.13: Queries Delivered - Battery

nonGroup based method as seen in Table 7.4. The graph has been depicted in Figure 7.15 and Figure 7.16.

7.3.5 Tree Topology with Depth 3 - Packet Transmission - FiT-IoT Results

In 3 level, FIT IoT nodes perform packet transmission Figure 7.17 and also verify the improvement in Figure 7.18. The percentage improvement with respect to

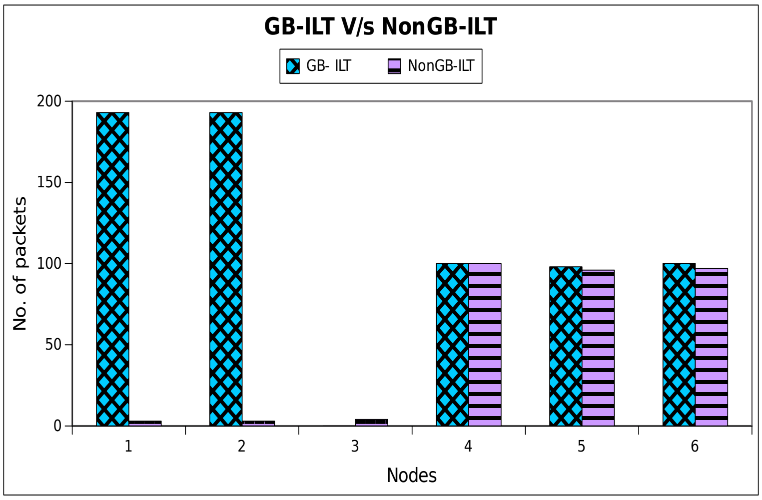


Figure 7.14: Queries Delivered - Image, Light, Temperature

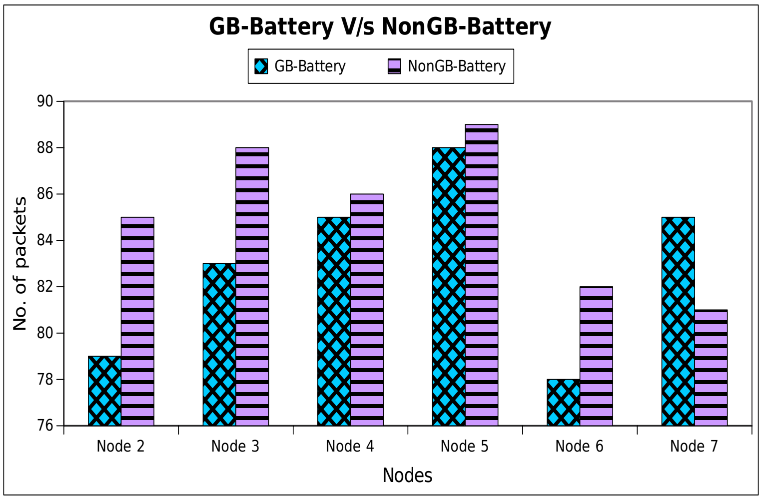


Figure 7.15: Queries Delivered - Battery

Table 7.4: Improvement % Comparison with RPL

Sensors	**Improvements %**
Battery	4.244
Image	13.457
Light	16.609
Temperature	9.544

NonGroup-based is 13.84.

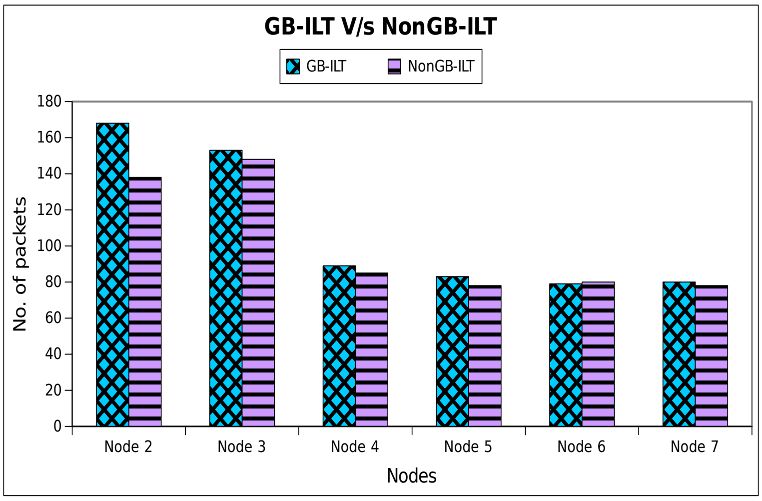


Figure 7.16: Queries Delivered - Image, Light, Temperature

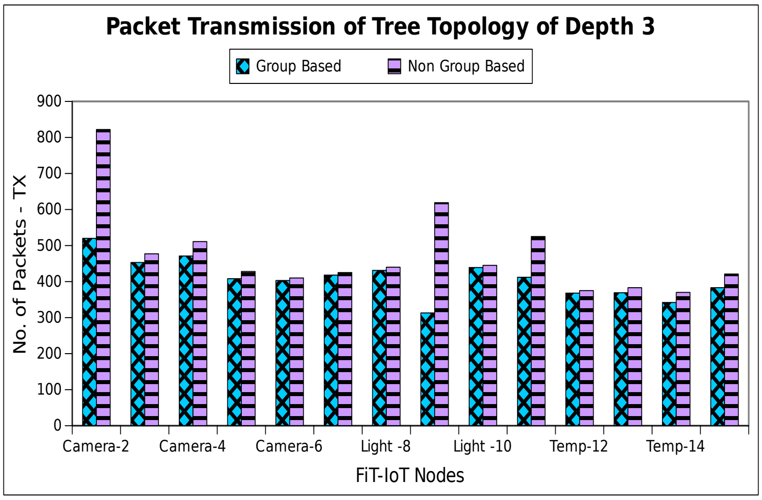


Figure 7.17: Packet Transmission of Tree Topology of Depth 3

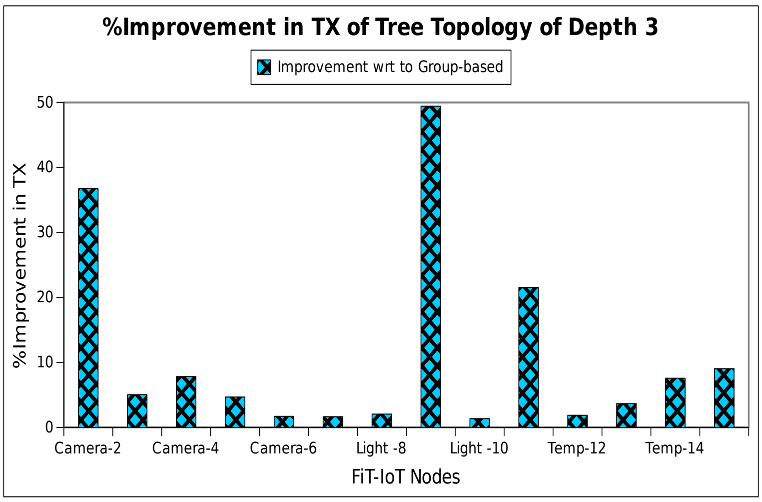


Figure 7.18: % Improvement w.r.t Group-based

7.3.6 Tree Topology with Depth 3 - Packet Transmission - Cooja Results

The base station sends one query to each sensor every 10 seconds. A total of 100 queries are sent to each sensor in the simulation. Comparison has been made between NonGroup-based and Group-based group registration for packet transmission of packet is shown in Figure 7.19. Percentage improvement in Figure 7.20 with respect to NonGroup-based group registration is 28.18.

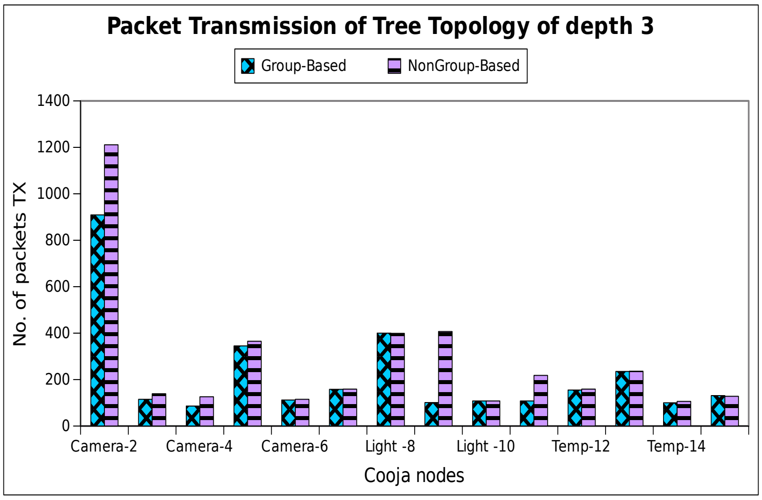


Figure 7.19: Packet Transmission of Tree Topology of Depth 3

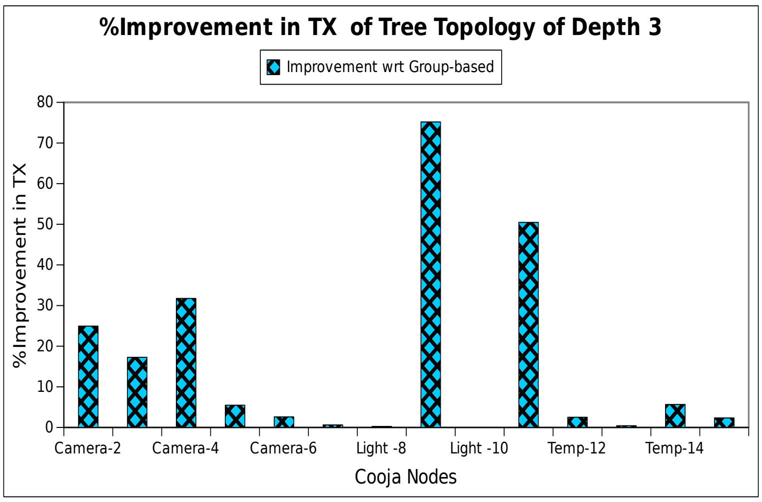


Figure 7.20: % Improvement

7.3.7 Tree Topology with Depth 3 - FiT-IoT Results

In the level 3 Figure 7.21 and Figure 7.22, FiT-IoT nodes improvement are good in Image data when compared to other scalar data.

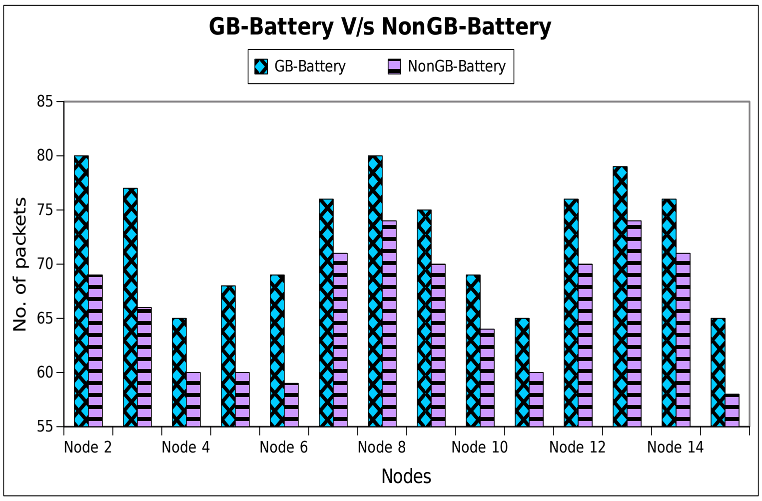


Figure 7.21: Queries Delivered - Battery

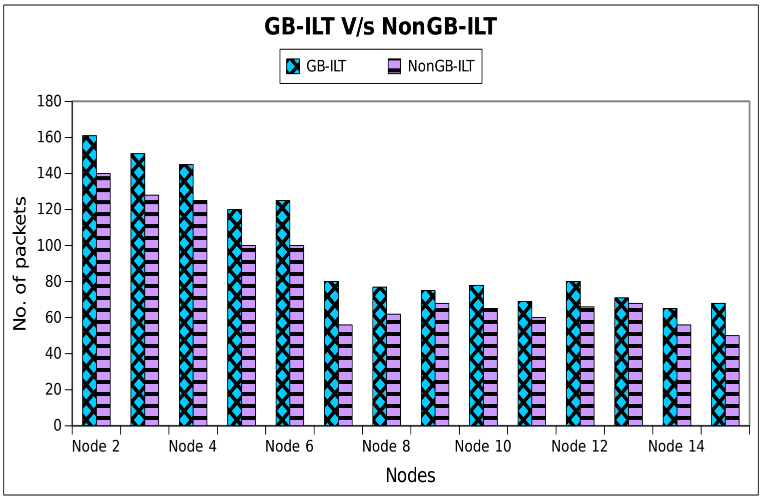


Figure 7.22: Queries Delivered - Image, Light, Temperature

Table 7.5: Improvement % Comparison with RPL

Sensors	**Improvements %**
Battery	25.84
Image	15.747
Light	17.704
Temperature	15.510

7.3.8 Tree Topology with Depth 3 - Cooja Results

In level 3 topology, Figure 7.23, one root node(green), 5 light nodes(yellow), 5 camera nodes(Dark yellow) and 4 temperature nodes (purple) has been used in Cooja setup. When looking at the graphs Figure 7.24 and Figure 7.25, Image data provides better results while comparing it with scalar data

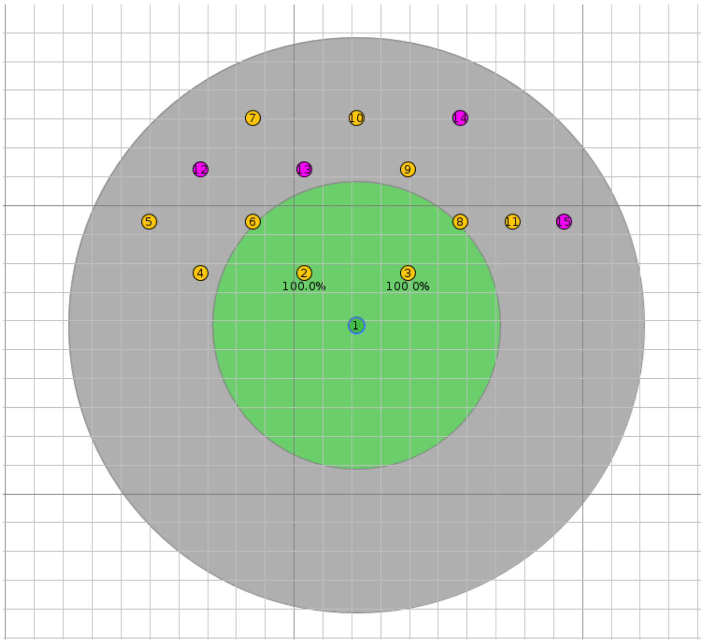


Figure 7.23: Test - Topology

Table 7.6: Improvement % Comparison with RPL

Sensors	**Improvements %**
Battery	89.86
Image	80
Light	67.24
Temperature	31 more packets in NonGB

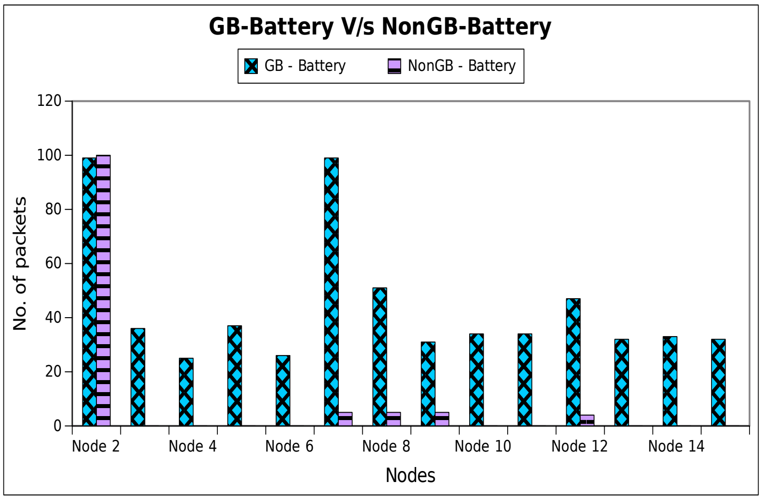


Figure 7.24: Queries Delivered - Battery

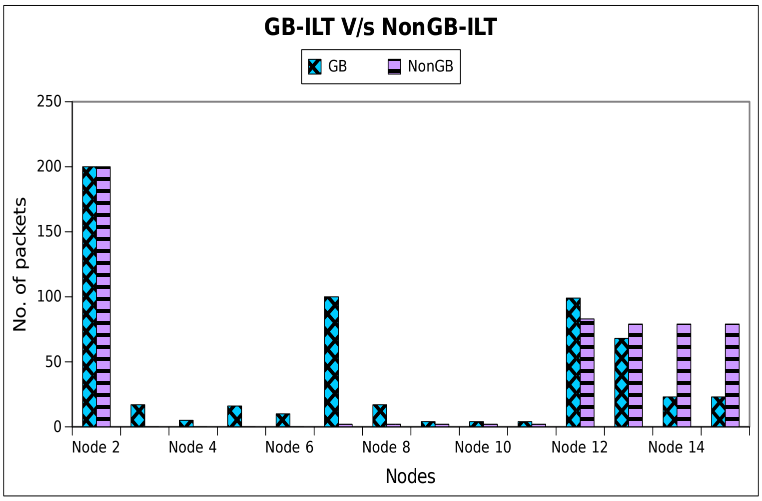


Figure 7.25: Queries Delivered - Image, Light, Temperature

7.4 Summary

The FiT-IoT testbed offers a way to validate the work in a real world deployment. Both the research proposals on point to multipoint and multipoint to point is tested on 2 different topologies (2 level tree with 7 nodes and 3 level tree with 15 nodes) and compared against the default implementation of Contiki. The results show that the proposals made fare better than the default implementation of Contiki with respect to different metrics such as PDR and Energy Consumption.

Chapter 8

Conclusions and Future Work

Internet of things (IoT) is a technology connecting millions of devices to the Internet. The devices in general are low powered with sensors monitoring the environment around them and connect to a wireless network. As Wireless Sensor Network nodes are ID based network, it is difficult to monitor their status when connected to the Internet of Things. Hence, a gateway is required to connect such a network to the Internet. In order to eliminate the need for gateways and instead remotely access and directly manage these devices, it is beneficial to have the devices support IP based connectivity. As the scale of the devices in an IoT world is very high, an IPv6 network is preferred over IPv4.

IPv6 connectivity in sensor networks mainly depend on two IETF standards: 6LoWPAN and RPL. Routing protocol in 6LoWPAN is very precise due to limited potential of the nodes and the existing routing protocols of 6LoWPAN did not satisfy the requirements of such networks. IETF came up with IPv6 routing protocol for low power lossy networks called RPL. While 6LoWPAN and RPL enable an efficient IPv6 based network for the IoT space, the design paradigms cater more for networks with scalar sensors. They do not scale when the network consists of multimodal sensors that generate a lot more data than the scalar sensors.

The thesis focuses on improving the performance of 6LoWPAN and RPL for networks running multimodal sensors. The areas of improvement include -

1. Proposed a new objective function (OF) for improving the parent selection process with focus on hop count, ETX and energy.

2. Proposed a method to further compress an IPHC compressed IPv6 address and SCHC header.

3. Proposed a priority based packet forwarding using a weighted ranking scheme.

4. Proposed a method to optimize the network performance for multicast traffic using group based addressing scheme.

All the enhancements have been compared against current RPL implementation via tests run in Cooja, a simulator and in the FiT-IoT lab which is a real world IoT test bed.

In the first objective, a new OF, HEE-OF is proposed that uses hop count, ETX and energy as metrics to determine a suitable parent for a given node. This new OF is implemented in Contiki. An experiment is run in the Cooja simulator and metrics such as packet deliver ratio (PDR), control traffic overhead, energy consumption and latency are captured. The experiment is run with OF set to the existing OFs, OF0 and MRHOF and also the proposed OF, HEE-OF. The results of the simulations indicate the proposed OF performs better than the existing OFs in all the metrics measured. Experimental results mention that the proposed HEE-OF improves PDR, reduces overhead and decreases energy consumption parameters by 4%, 6%, 3% respectively.

In the second objective, the proposed techniques are incorporated with respect to HC1 of IPHC in 6LoWPAN and SCHC for IPv6. An enhancement to the IPHC compression is proposed to further reduce the overhead of the IPv6 header in 6LoWPAN networks. The IPHC compressed IPv6 address is further compressed based on the leading zeros present in the address. This allows more application data to be transported in a single frame reducing the total number of frames required to transmit a large multimodal data such as an image. The simulation results show the compression scheme achieves anywhere between 10% to 40% better compression compared to with just with IPHC compression based on the continuous zeroes present in the IPv6 address. The future work can include more analysis on the impact of the new compression scheme with respect to larger data packets.

In the third objective, a weighted rank scheme, R-RPL is proposed where neighbors of a node are ranked based on several metrics. The metrics used in the ranking scheme include energy, data rate and ETX. The ranks assigned to the neighbors is then used to determine the priority to be assigned to the packet based on the neighbor the packet was received from. This priority is then used when queuing packets in the MAC layer. Lower priority packets are dropped in favor of higher priority packets. In addition to using the ranks to assign priorities to packets, it is also used in a new OF to determine the best parent for a node. An experiment is executed to transfer data, scalar and image from multiple different nodes to the root of the network. The proposed work is implemented in ContikiOS and executed as a simulation on Cooja as well as on a real time IoT network, FiTIoT-Lab. The analysis shows that R-RPL performs better compared to the current RPL implementation for metrics such as PDR and energy consumption. The future work can explore the impact of different weight assignment schemes for the metrics both in terms of packet prioritization and parent selection.

In the next objective, a new multicast address grouping scheme for sensors is proposed that enables nodes to join and leave multicast groups based on the sensors they support or have to relay for nodes in their RPL tree downstream. The new group advertisement message enables the root node to advertise multicast groups and the sensors attached to each group and the group join and leave messages enable a node in the network to selective join only groups which is relevant to the node. This conserves space in the multicast routing table and also stops multicast packets from being flooded to parts of the network that are not interested in those frames. The proposed work is implemented in ContikiOS and executed as a simulation on Cooja as well as on a real time IoT network, FiTIoT-Lab. The results of the simulation indicate that the proposed method outperforms the existing RPL implementation in the overall network. Experimental results show that the proposed method improves PDR in a tree topology of depth 2 and 3 by 35.03% and 28.18% respectively. The future work can focus on different grouping schemes for the various sensors and the impact of that on metrics such as PDR. Also the implementation can be enhanced to advertise the age of a multicast route instead of during periodic DAOs to refresh the routes which can in turn reduce the number of control frames in the network.

It is also important to note that all the proposed schemes work on any type of IoT node that supports IEEE 802.15.4 over MAC, 6LoWPAN adaptation layer and IPv6 in the network layer. They are not limited to any specific type of IoT nodes and hence can be deployed in a heterogeneous network with different types of IoT nodes. Also, while all the experiments considered a tree based topology with a maximum depth of 3, the effect of increase in number of nodes should not dilute the performance of the proposed schemes since all of them consider multi-hop communication as a key metric. As the number of deployed nodes increase, the number of hops in communication also increase and the proposed schemes should still perform better than existing solutions.

Publications based on Research Work

Journal Publications

1. Archana Bhat, Geetha V "*Hybrid HopCount, ETX and ENERGY Based Objective Function (HEE_OF) for Image Data Transmission over 6LoWPAN in IoT*". International Journal of Wireless and Mobile Computing(IJWMC), InderScience [Scopus] (Accepted).

2. G. V., A. Bhat and S. Thanmayee, "New Bit Pattern Based IPv6 Address Compression Techniques for 6LoWPAN Header Compression," in IEEE Access, vol. 10, pp. 80055-80070, 2022, doi: 10.1109/ACCESS.2022.3193235.

3. Archana Bhat, Geetha V "*Ranking based RPL for Multipoint-to-Point Multimodal Data Communication in IoT Network* ". Journal of Wireless personal Communications, Springer https://www.researchsquare.com/article/rs-742884/v1 (Under Review).

4. Archana Bhat, Geetha V "*Multicast Group Management based RPL for Point to Multipoint Multimodal Data Communication*". Ad Hoc Networks (Working on review comments).

Conference Publications

1. A. Bhat and V. Geetha, "Survey on routing protocols for Internet of Things," 2017 7th International Symposium on Embedded Computing and System Design (ISED), Durgapur, India, 2017, pp. 1-5, doi: 10.1109/ISED.2017.8303949.

Bibliography

Abdel Fadeel, K. Q. and K. El Sayed, Esmrf: enhanced stateless multicast rpl forwarding for ipv6-based low-power and lossy networks. *In Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*. 2015.

Accettura, N., L. A. Grieco, G. Boggia, and P. Camarda, Performance analysis of the rpl routing protocol. *In Mechatronics (ICM), 2011 IEEE International Conference on*. IEEE, 2011.

Adarsh, B., H. Shivayogappa, K. Navya, *et al.*, Automated smart sericulture system based on 6lowpan and image processing technique. *In 2016 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2016.

Adjih, C., E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele, *et al.*, Fit iot-lab: A large scale open experimental iot testbed. *In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015.

Akyildiz, I. F., T. Melodia, and K. R. Chowdhury (2007). A survey on wireless multimedia sensor networks. *Computer networks*, 51(4), 921–960.

Al-Fuqaha, A., M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.

Alvi, S. A., G. A. Shah, and W. Mahmood, Energy efficient green routing protocol for internet of multimedia things. *In 2015 IEEE tenth international conference on intelligent sensors, sensor networks and information processing (ISSNIP)*. IEEE, 2015.

Ambarkar, S. S. and N. Shekokar, Impact analysis of rpl attacks on 6lo wpan based internet of things network. *In 2021 IEEE International Conference on*

Electronics, Computing and Communication Technologies (CONECCT). IEEE, 2021.

Arunachalam, V. and N. R. Nallamothu (). Load balancing in rpl to avoid hotspot problem for improving data aggregation in iot.

Awwad, S. A., C. K. Ng, N. K. Noordin, B. M. Ali, and F. Hashim, Second and subsequent fragments headers compression scheme for ipv6 header in 6lowpan network. *In Sensing Technology (ICST), 2013 Seventh International Conference on*. IEEE, 2013.

Baccelli, E., O. Hahm, M. Gunes, M. Wahlisch, and T. C. Schmidt, Riot os: Towards an os for the internet of things. *In Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on*. IEEE, 2013.

Baccelli, E., M. Philipp, and M. Goyal, The p2p-rpl routing protocol for ipv6 sensor networks: Testbed experiments. *In Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on*. IEEE, 2011.

Betzler, A., C. Gomez, I. Demirkol, and J. Paradells (2016). Coap congestion control for the internet of things. *IEEE Communications Magazine*, 54(7), 154–160.

Bidai, Z. (2021). Rpl enhancement to support video traffic for iomt applications. *Wireless Personal Communications*, 1–28.

Bouakouk, M. R., A. Abdelli, and L. Mokdad, Odm-rpl: Optimized dual mop rpl. *In 2021 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2021.

Bouzebiba, H. and M. Lehsaini (2020). Freebw-rpl: A new rpl protocol objective function for internet of multimedia things. *Wireless Personal Communications*, 1–21.

Bruniaux, A., R.-A. Koutsiamanis, G. Z. Papadopoulos, and N. Montavont (2021). Defragmenting the 6lowpan fragmentation landscape: A performance evaluation. *Sensors*, 21(5), 1711.

Chapin, L. *et al.* (1992). Applicability statement for ospf. Technical report.

Clausen, T. and U. Herberg, Multipoint-to-point and broadcast in rpl. *In Network-Based Information Systems (NBiS), 2010 13th International Conference on*. IEEE, 2010.

Clausen, T. and P. Jacquet (2003). Rfc3626: Optimized link state routing protocol (olsr).

Dias, J., F. Ribeiro, R. Campos, M. Ricardo, L. Martins, F. Gomes, and A. Carrapatoso, Evaluation of an rpl/6lowpan/ieee 802.15. 4g solution for smart metering in an industrial environment. *In Wireless On-demand Network Systems and Services (WONS), 2016 12th Annual Conference on*. IEEE, 2016.

Djedjig, N., D. Tandjaoui, and F. Medjek, Trust-based rpl for the internet of things. *In Computers and Communication (ISCC), 2015 IEEE Symposium on*. IEEE, 2015.

Ee, G. K., C. K. Ng, N. K. Noordin, and B. M. Ali (2010). A review of 6lowpan routing protocols. *Proceedings of the Asia-Pacific Advanced Network*, 30, 71–81.

Eloudrhiri Hassani, A., A. Sahel, and A. Badri (2021). Irh-of: A new objective function for rpl routing protocol in iot applications. *Wireless Personal Communications*, 119(1), 673–689.

Estepa, R., A. Estepa, G. Madinabeitia, and E. García (2021). Rpl cross-layer scheme for ieee 802.15. 4 iot devices with adjustable transmit power. *IEEE Access*, 9, 120689–120703.

Fuller, J. D. and B. W. Ramsey, Rogue z-wave controllers: A persistent attack channel. *In Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th*. IEEE, 2015.

Garg, R. and S. Sharma, Comparative study on techniques of ipv6 header compression in 6lowpan. *In Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology-IPCT*. 2016.

Garrido, P. C., G. M. Miraz, I. L. Ruiz, and M. Á. Gómez-Nieto, A model for the development of nfc context-awareness applications on internet of things. *In Near Field Communication (NFC), 2010 Second International Workshop on*. IEEE, 2010.

Gaur, P. and M. P. Tahiliani, Operating systems for iot devices: A critical survey. *In Region 10 Symposium (TENSYMP), 2015 IEEE*. IEEE, 2015.

Gilb, J. P., *Wireless multimedia: A guide to the IEEE 802.15. 3 standard*. IEEE Standards Association, 2004.

Glissa, G., A. Rachedi, and A. Meddeb, A secure routing protocol based on rpl for internet of things. *In Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 2016.

Gnawali, O. and P. Levis (2012). The minimum rank with hysteresis objective function. Technical report.

Gomes, Y. F., D. F. Santos, H. O. Almeida, and A. Perkusich, Integrating mqtt and iso/ieee 11073 for health information sharing in the internet of things. *In Consumer Electronics (ICCE), 2015 IEEE International Conference on*. IEEE, 2015.

Gomez, C. and A. Minaburo (2022). Transmission of SCHC-compressed packets over IEEE 802.15.4 networksInternet-Draftdraft-gomez-6lo-schc-15dot4-02, Internet Engineering Task Force. URL https://datatracker.ietf.org/doc/html/draft-gomez-6lo-schc-15dot4-02. Work in Progress.

Gomez, C., A. Minaburo, L. Toutain, D. Barthel, and J. C. Zuniga (2020). Ipv6 over lpwans: Connecting low power wide area networks to the internet (of things). *IEEE Wireless Communications*, 27(1), 206–213.

Haque, K. F., A. Abdelgawad, V. P. Yanambaka, and K. Yelamarthi, An energy-efficient and reliable rpl for iot. *In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. IEEE, 2020.

Hasbollah, A. A., S. H. Ariffin, and M. I. A. Hamini, Performance analysis for 6lowpan ieee 802.15. 4 with ipv6 network. *In TENCON 2009-2009 IEEE Region 10 Conference*. IEEE, 2009.

Hawbani, A., X. Wang, and Y. Xiong (2013). Sensors grouping model for wireless sensor network. *Journal of Sensor Technology*, 2013.

Hiremath, S., G. Yang, and K. Mankodiya, Wearable internet of things: Concept, architectural components and promises for person-centered healthcare. *In Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on*. IEEE, 2014.

Hui, J. and D. Culler (2007). Stateless ipv6 header compression for globally routable packets in 6lowpan subnetworks. *Arch Rock Corporation, Internet Draft¡ draft-hui-6lowpan-hc1g-00*.

Hui, J., P. Thubert, *et al.* (2011). Compression format for ipv6 datagrams over ieee 802.15. 4-based networks.

Huiqin, W. and D. Yongqiang, An improved header compression scheme for 6lowpan networks. *In 2010 Ninth International Conference on Grid and Cloud Computing*. IEEE, 2010.

Hwang, R.-H., M.-C. Peng, C.-Y. Wu, and S. Abimannan (2020). A novel rpl-based multicast routing mechanism for wireless sensor networks. *International Journal of Ad Hoc and Ubiquitous Computing*, 33(2), 122–131.

Iova, O., P. Picco, T. Istomin, and C. Kiraly (2016). Rpl: The routing standard for the internet of things... or is it? *IEEE Communications Magazine*, 54(12), 16–22.

Iova, O., F. Theoleyre, and T. Noel (2014). Efficient energy-balancing in multipath rpl. *ALGOTEL èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*, 1–4.

Iova, O., F. Theoleyre, and T. Noel, Exploiting multiple parents in rpl to improve both the network lifetime and its stability. *In Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015.

Iova, O., F. Theoleyre, T. Watteyne, and T. Noel (2017). The love-hate relationship between ieee 802.15. 4 and rpl. *IEEE Communications Magazine*, 55(1), 188–194.

Kamgueu, P. O., E. Nataf, T. D. Ndié, and O. Festor (2013). *Energy-based routing metric for RPL*. Ph.D. thesis, INRIA.

Kechiche, I., I. Bousnina, and A. Samet, A comparative study of rpl objective functions. *In 2017 Sixth International Conference on Communications and Networking (ComNet)*. IEEE, 2017.

Kettouche, S., M. Maimour, and L. Derdouri, Qoe-based performance evaluation of video transmission using rpl in the iomt. *In 2019 7th Mediterranean Congress of Telecommunications (CMT)*. IEEE, 2019.

Kettouche, S., M. Maimour, and L. Derdouri (2021). Dm-rpl: Disjoint multipath rpl for bandwidth provision in the internet of multimedia things. *Revue de l'Information Scientifique et Technique*, 26(1), 23–35.

Khaleghnasab, R., K. Bagherifard, B. Ravaei, H. Parvin, and S. Nejatian (2020). An energy and load aware multipath routing protocol in the internet of things.

Kharrufa, H., H. Al-Kashoash, Y. Al-Nidawi, M. Q. Mosquera, and A. H. Kemp, Dynamic rpl for multi-hop routing in iot applications. *In Wireless On-demand Network Systems and Services (WONS), 2017 13th Annual Conference on*. IEEE, 2017.

Kharrufa, H., H. A. Al-Kashoash, and A. H. Kemp (2019). Rpl-based routing protocols in iot applications: a review. *IEEE Sensors Journal*, 19(15), 5952–5967.

Khelifi, N., S. Oteafy, H. Hassanein, and H. Youssef, Proactive maintenance in rpl for 6lowpan. *In Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International*. IEEE, 2015.

Kim, H.-S., H. Im, M.-S. Lee, J. Paek, and S. Bahk (2015). A measurement study of tcp over rpl in low-power and lossy networks. *Journal of Communications and Networks*, 17(6), 647–655.

Kim, H.-S., H. Kim, J. Paek, and S. Bahk (2017). Load balancing under heavy traffic in rpl routing protocol for low power and lossy networks. *IEEE Transactions on Mobile Computing*, 16(4), 964–979.

Kiraly, C., T. Istomin, O. Iova, and G. P. Picco, D-rpl: Overcoming memory limitations in rpl point-to-multipoint routing. *In Local Computer Networks (LCN), 2015 IEEE 40th Conference on*. IEEE, 2015.

Kivinen, T. and P. Kinney (2017). Ieee 802.15. 4 information element for the ietf. Technical report.

Kocakulak, M. and I. Butun, An overview of wireless sensor networks towards internet of things. *In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017.

Kumar, A. and N. Hariharan (2020). Dcrl-rpl: Dual context-based routing and load balancing in rpl for iot networks. *IET Communications*, 14(12), 1869–1882.

Kumar, S. and S. R. Lee, Android based smart home system with control via bluetooth and internet connectivity. *In Consumer Electronics (ISCE 2014), The 18th IEEE International Symposium on*. IEEE, 2014.

Kushalnagar, N., J. Hui, D. Culler, *et al.* (2007*a*). Transmission of ipv6 packets over ieee 802.15. 4 networks.

Kushalnagar, N., G. Montenegro, and C. Schumacher (2007*b*). 6lowpan: Overview. *Assumptions, Problem Statement and Goals. draft-ietf-6lowpan-problem-06, IETF (November 2006)*.

Kushalnagar, N., G. Montenegro, and C. Schumacher (2007*c*). Rfc 4919: Ipv6 over low-power wireless personal area networks (6lowpans): overview. *Assumptions, Problem Statement, and Goals*.

Lamaazi, H. and N. Benamar, Rpl enhancement using a new objective function based on combined metrics. *In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2017.

Le, Q., T. Ngo-Quynh, and T. Magedanz, Rpl-based multipath routing protocols for internet of things on wireless sensor networks. *In Advanced Technologies for Communications (ATC), 2014 International Conference on*. IEEE, 2014.

Lenders, M. S., T. C. Schmidt, and M. Wählisch (2021). Fragment forwarding in lossy networks. *IEEE Access*, 9, 143969–143987.

Li, L., G. Wen, Z. Wang, and Y. Yang (2019). Efficient and secure image communication system based on compressed sensing for iot monitoring applications. *IEEE Transactions on Multimedia*, 22(1), 82–95.

Liu, X., J. Guo, G. Bhatti, P. Orlik, and K. Parsons, Load balanced routing for low power and lossy networks. *In Wireless Communications and Networking Conference (WCNC), 2013 IEEE*. IEEE, 2013.

Lodhi, M. A., A. Rehman, M. M. Khan, and F. B. Hussain, Multiple path rpl for low power lossy networks. *In Wireless and Mobile (APWiMob), 2015 IEEE Asia Pacific Conference on*. IEEE, 2015.

Ludovici, A., A. Calveras, M. Catalan, C. Gómez, and J. Paradells, Implementation and evaluation of the enhanced header compression (iphc) for 6lowpan. *In Meeting of the European Network of Universities and Companies in Information and Communication Engineering*. Springer, 2009.

Madakam, S. and R. Ramaswamy, 100 new smart cities (india's smart vision). *In Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on*. IEEE, 2015.

Maksimović, M., V. Vujović, N. Davidović, V. Milošević, and B. Perišić (2014). Raspberry pi as internet of things hardware: performances and constraints. *design issues*, 3, 8.

Minaburo, A., L. Toutain, and R. Andreasen (2021). Static context header compression (schc) for the constrained application protocol (coap). Technical report, RFC 8824. 2021. Available online: https://www. rfc-editor. org/info/rfc8824 ....

Minaburo, A., L. Toutain, C. Gomez, D. Barthel, and J. C. Zúniga (2020). Rfc 8724 schc: Generic framework for static context header compression and fragmentation.

Montenegro, G., N. Kushalnagar, J. Hui, D. Culler, *et al.* (2007). Transmission of ipv6 packets over ieee 802.15. 4 networks. *Internet proposed standard RFC*, 4944, 130.

Moradi, S. and R. Javidan (2020). A new objective function for rpl routing protocol in iot to increase network lifetime. *International Journal of Wireless and Mobile Computing*, 19(1), 73–79.

Nam, S.-J., J. Kang, and D. Moon, Wireless packet header compression techniques for ship area sensor network (sasn). *In 2015 15th International Conference on Control, Automation and Systems (ICCAS)*. IEEE, 2015.

Nauman, A., Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim (2020). Multimedia internet of things: A comprehensive survey. *IEEE Access*, 8, 8202–8250.

Nekoogar, F. and F. Dowla, Passive rfid for iot using uwb/uhf hybrid signaling. *In Wireless Information Technology and Systems (ICWITS) and Applied Computational Electromagnetics (ACES), 2016 IEEE/ACES International Conference on*. IEEE, 2016.

Oikonomou, G. and I. Phillips, Stateless multicast forwarding with rpl in 6lowpan sensor networks. *In 2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE, 2012.

Oikonomou, G., I. Phillips, and T. Tryfonas (2013). Ipv6 multicast forwarding in rpl-based wireless sensor networks. *Wireless personal communications*, 73(3), 1089–1116.

Olsson, J. (2014). 6lowpan demystified. *Texas Instruments*, 13.

Pavković, B., F. Theoleyre, and A. Duda, Multipath opportunistic rpl routing over ieee 802.15. 4. *In Proceedings of the 14th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*. ACM, 2011.

Pekhteryev, G., Z. Sahinoglu, P. Orlik, and G. Bhatti, Image transmission over ieee 802.15. 4 and zigbee networks. *In 2005 IEEE International Symposium on Circuits and Systems*. IEEE, 2005.

Perkins, C., E. Belding-Royer, and S. Das (2003). Rfc3561: Ad hoc on-demand distance vector (aodv) routing.

Pham, C., V. Lecuire, and J.-M. Moureaux, Performances of multi-hops image transmissions on ieee 802.15. 4 wireless sensor networks for surveillance applications. *In 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2013.

Pradeska, N., W. Najib, S. S. Kusumawardani, *et al.*, Performance analysis of objective function mrhof and of0 in routing protocol rpl ipv6 over low power wireless personal area networks (6lowpan). *In 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*. IEEE, 2016.

Przygienda, T. (2002). Reserved type, length and value (tlv) codepoints in intermediate system to intermediate system. Technical report, RFC 3359, August.

Rahman, H., N. Ahmed, and I. Hussain, Comparison of data aggregation techniques in internet of things (iot). *In Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on*. IEEE, 2016.

Rakesh, B. (2021). Novel authentication and secure trust based rpl routing in mobile sink supported internet of things. *Cyber-Physical Systems*, 1–34.

Safara, F., A. Souri, T. Baker, I. Al Ridhawi, and M. Aloqaily (2020). Prinergy: A priority-based energy-efficient routing method for iot systems. *The Journal of Supercomputing*, 76(11), 8609–8626.

Saloni, S. and A. Hegde, Wifi-aware as a connectivity solution for iot pairing iot with wifi aware technology: Enabling new proximity based services. *In Internet of Things and Applications (IOTA), International Conference on*. IEEE, 2016.

Sanmartin, P. and et.al (2018). Sigma routing metric for rpl protocol. *Sensors*, 18(4), 1277.

Shacham, A., B. Monsour, R. Pereira, and M. Thomas (2001). Ip payload compression protocol (ipcomp). Technical report.

Solapure, S. S. and H. H. Kenchannavar (2020). Design and analysis of rpl objective functions using variant routing metrics for iot applications. *Wireless Networks*, 26, 4637–4656.

Somaa, F., I. El Korbi, and L. A. Saidane, Braided on demand multipath rpl in the mobility context. *In Advanced Information Networking and Applications (AINA), 2017 IEEE 31st International Conference on*. IEEE, 2017.

Sonia Kuwelkar, H. V. (2021). Design of an efficient rpl objective function for internet of things applications. *(IJACSA) International Journal of Advanced Computer Science and Applications 2021*, 12(6), 228–235.

Soro, A., J. Lacan, E. Chaput, C. Donny, and C. Baudoin, Evaluation of a generic unidirectional header compression protocol. *In 2007 International Workshop on Satellite and Space Communications*. IEEE, 2007.

Soukayna, R. B. and E. Abdellatif, Comparison between objective functions standards and of-ehe for rpl routing protocol. *In Proceedings of the 4th International Conference on Big Data and Internet of Things*. 2019.

Sousa, N. and et.al, Eraof: A new rpl protocol objective function for internet of things applications. *In 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*. IEEE, 2017.

Taghizadeh, S., H. Elbiaze, and H. Bobarshad (2020). Em-rpl: Enhanced rpl for multigateway internet-of-things environments. *IEEE Internet of Things Journal*, 8(10), 8474–8487.

Tanaka, Y., P. Minet, and T. Watteyne (2019). 6lowpan fragment forwarding. *IEEE Communications Standards Magazine*, 3(1), 35–39.

Thubert, P. (2012). Objective function zero for the routing protocol for low-power and lossy networks (rpl). Technical report.

Tripathi, J. and J. De Oliveira, Quantifying load imbalance: A practical implementation for data collection in low power lossy networks. *In Information Sciences and Systems (CISS), 2013 47th Annual Conference on*. IEEE, 2013.

Tripathi, J., J. De Oliveira, and J. Vasseur (2012). Performance evaluation of the routing protocol for low-power and lossy networks (rpl). Technical report.

Tripathi, J., J. C. de Oliveira, and J.-P. Vasseur, A performance evaluation study of rpl: Routing protocol for low power and lossy networks. *In Information Sciences and Systems (CISS), 2010 44th Annual Conference on*. IEEE, 2010.

Verma, K. (2015). Multicast routing protocols for wireless sensor networks: a comparative study. *Int. J. Comput. Sci*, 2015, 1041–1054.

Wang, Z. M., W. Li, and H. L. Dong, Analysis of energy consumption and topology of routing protocol for low-power and lossy networks. *In Journal of Physics: Conference Series*volume1087. IOP Publishing, 2018.

Watteyne, T., F. Chraim, N. Sarmicanic, C. Jian, and K. S. Pister (2010). Video transmission over a standards-based wireless multi-hop sensor network. *E-LETTER*.

Winter, T. (2012). Rpl: Ipv6 routing protocol for low-power and lossy networks.

Xiao, W., J. Liu, N. Jiang, and H. Shi, An optimization of the object function for routing protocol of low-power and lossy networks. *In Systems and Informatics (ICSAI), 2014 2nd International Conference on*. IEEE, 2014.

Xie, H., G. Zhang, D. Su, P. Wang, and F. Zeng, Performance evaluation of rpl routing protocol in 6lowpan. *In Software Engineering and Service Science (ICSESS), 2014 5th IEEE International Conference on*. IEEE, 2014.

Yang, S., Y. Xu, and Q. He, Ontology based service discovery method for internet of things. *In Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, 2011.

Yashiro, T., S. Kobayashi, N. Koshizuka, and K. Sakamura (2013). An internet of things (iot) architecture for embedded appliances, 314–319.

Yassein, M. B., W. Mardini, and A. Khalil, Smart homes automation using z-wave protocol. *In Engineering & MIS (ICEMIS), International Conference on*. IEEE, 2016.

Yi, J., T. Clausen, and Y. Igarashi, Evaluation of routing protocol for low power and lossy networks: Loadng and rpl. *In Wireless Sensor (ICWISE), 2013 IEEE Conference on*. IEEE, 2013.

Zhao, C. W., J. Jegatheesan, and S. C. Loon (2015). Exploring iot application using raspberry pi. *International Journal of Computer Networks and Applications*, 2(1), 27–34.

Zhao, M., I. W.-H. Ho, and P. H. J. Chong (2016). An energy-efficient region-based rpl routing protocol for low-power and lossy networks. *IEEE Internet of Things Journal*, 3(6), 1319–1333.

Bio-data

Name:	Archana Bhat
Address:	Research Scholar Department of Information Technology, NITK Surathkal Mangaluru, Karnataka India - 575025
Email:	archanabhat1990@gmail.com
Mobile No:	+91 9902885719
Qualification:	Ph.D. in Information Technology, NITK Surathkal, Mangaluru, D.K, Karnataka M.Tech. in Computer Science & Engineering, St. Joseph Engineering College, Vamanjoor, Mangaluru, D.K, Karnataka B.E. in Information Science & Engineering, P A College of Engineering, Nadupadav, D.K, Karnataka