



**JIMMA UNIVERSITY**  
**JIMMA INSTITUTE OF TECHNOLOGY**  
**FACULTY OF COMPUTING**  
**AND INFORMATICS.**

Modified reactive route discovery algorithm for constrained machine to  
machine communication in low power and lossy networks

By

Daniel Teklu

This Research Study is Submitted to faculty of computing and informatics, Institute of  
Technology, Jimma University, as a Partial Fulfillment for The Award Degree of Master Science

In

Computer Networking.

Advisor: Million Meshesha (PhD)

Co-Advisor: Mr. Samuel Sisay

February, 2021

## Approval sheet

This thesis titled “**Modified reactive route discovery algorithm for constrained machine to machine communication in low power and lossy networks**” has been read and approved as meeting the requirement of department of computing as a partial fulfillment for the award degree of master science in computer networking, institute of technology, Jimma University, Ethiopia.

### Advisor

**Name: - Million Meshesha (PhD)**

**Signature: million**

**Date: - Jan 30, 2021**

### Co-Advisor

**Name: - Samuel Sisay (MSc)**

**Signature: - \_\_\_\_\_**

**Date: - \_\_\_\_\_**

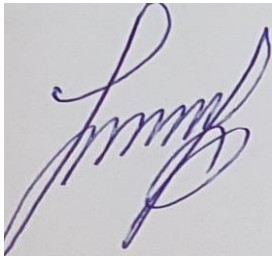
## Declaration

I, the under signed, verify that this thesis study titled as “**Modified reactive route discovery algorithm for constrained machine to machine communication in low power and lossy networks**” is my original study, and has not been conferred by any other person for grant of a degree in current or any other university.

**Daniel Teklu:** \_\_\_\_\_

### External Examiner

**Name:** - \_\_\_\_\_



**Signature:** - \_\_\_\_\_

**Date:** - \_\_\_\_\_

### Internal Examiner

**Name:** \_\_\_\_\_

**Signature:** - \_\_\_\_\_

**Date:** - \_\_\_\_\_

### Chairperson

**Name:** \_\_\_\_\_

**Signature:** - \_\_\_\_\_

**Date:** - \_\_\_\_\_

## Acknowledgment

First and for most, I would like to thank the **Almighty God** for blessing me with all the time I need to do this thesis in the midst of the pandemic (Covid-19) while the world was in shock.

I would like to extend my profound gratitude to **Million Meshesha (PhD)**, for his unwavering support and dedication in providing me with feedbacks and comments on this thesis. It was an honor having him as a principal advisor and for lighting the way.

I would like to pay tribute to **Mr. Samuel Sisay** (Co-advisor) for providing me with fruitful comments.

I would like to honor **Girum Ketema (PhD)**, **Mr. Kebebew Abebu** and **Mr. Getamessay Haile** for the lifesaving remarks and comments on the beginning of the research work.

At last, but not least, I wish to express my deep affection and appreciation to my families and friends who were by my side along the journey.

## Abstract

RPL builds a DODAG to enable routing for a source-destination pair in a network in order to allow point-to-point data transmission in LLNs. The source node sends its message to the root node, and the root helps route messages between the source and the destination. The root node is responsible in routing and preserving the route.

When using RPL in point-to-point communication, low power and lossy networks are subjected to extreme energy depletion due to the routing algorithms that operate within the nodes and the energy used when nodes communicate. Because network performance is highly dependent on the energy available in the network nodes, energy reservation mechanisms for longer periods of time should be introduced.

Therefore, the purpose of this study is to develop a modified routing mechanism that reduces the waste of energy and to increase the packets delivered between the restricted low-power and lossy network nodes described in RPL (RFC 6550) for machine-to-machine communication in routing data packets.

This thesis follows Design Science Research (DSR), which is seen as a research practice that develops new or invents, creates inventive objects to fix problems or enhance the accomplishment of those new innovative artifacts, rather than describing or attempting to make sense of the current reality from it. It produces and assesses IT objects that are meant to address certain organizational challenges identified.

The suggested solution presented satisfactory results in the grid case, where the network was sparse and the number of adjacent nodes was stable, demonstrating its scalability and achieving a PDR of between 75 percent and 80 percent. In comparison, with the increase in the number of nodes, the P2P-RPL solution reduced its efficiency. The justification for this action was the dependence on a set root node to deliver the messages.

**Keywords:** Routing, IoT, Machine to Machine communication, WSN, RPL, M2M-IoT

## Contents

<b>Approval sheet</b> .....	<b>i</b>
<b>Declaration</b> .....	<b>ii</b>
<b>Acknowledgment</b> .....	<b>iii</b>
<b>Abstract</b> .....	<b>iv</b>
<b>List of Figures</b> .....	<b>viii</b>
<b>List of Tables</b> .....	<b>ix</b>
<b>Acronyms</b> .....	<b>x</b>
<b>1. CHAPTER ONE</b> .....	<b>1</b>
<b>INTRODUCTION</b> .....	<b>1</b>
1.1. Background .....	1
1.2. Statement of the Problem .....	4
1.3. Objective of the study .....	5
1.3.1. General Objective .....	5
1.3.2. Specific Objectives .....	5
1.4. Methodology of the study .....	6
1.4.1. Research Design.....	6
1.4.2. Problem identification and motivation.....	7
1.4.3. Objectives of a solution .....	7
1.4.4. Design and development.....	8
1.4.5. Demonstration.....	8
1.4.6. Evaluation .....	10
1.4.7. Communication.....	10
1.5. Scope and Limitation of the study.....	11
1.6. Significance of the study .....	12
<b>2. CHAPTER TWO</b> .....	<b>13</b>
<b>LITERATURE REVIEW</b> .....	<b>13</b>
2.1. Overview .....	13
2.2. Characteristics of RPL .....	14
2.2.1. Data traffic flow assumption.....	14
2.2.2. DODAG root requirement .....	15
2.2.3. Fragmentation .....	15

2.2.4. Link Bi-directionality.....	16
2.2.5. Loops.....	16
2.3. Application of LLNs in relation to RPL.....	17
2.4. Challenges of LLNs in relation to RPL.....	18
2.4.1. Efficient routing support for generic traffic patterns with limited memory .....	19
2.4.2. Energy-efficient route discovery under severe resource constraints .....	19
2.4.3. Reliable and energy-efficient routing in LLNs.....	20
2.4.4. Congestion detection and control.....	20
2.4.5. Mobility support.....	21
2.4.6. High throughput with a low duty cycling of lower layer.....	21
2.4.7. Workload balancing strategy for RPL .....	21
2.4.8. Security issues.....	21
2.5. Routing protocol in LLNs .....	22
2.6. Related Works .....	25
2.7. Research gap .....	28
<b>3. CHAPTER THREE .....</b>	<b>30</b>
<b>DESIGN AND DEVELOPMENT .....</b>	<b>30</b>
3.1. Overview.....	30
3.2. M2M-IoT Route Discovery .....	31
3.3. Metric Evaluation.....	35
3.4. M2M-IoT Algorithms .....	38
3.5. Smart Route request Enhancement .....	42
3.6. Route Cache for M2M-IoT .....	42
3.7. Lost Error Code for M2M-IoT.....	45
<b>4. CHAPTER FOUR.....</b>	<b>47</b>
<b>DEMONSTRATION .....</b>	<b>47</b>
4.1. Simulation and Result .....	47
4.2. Contiki OS Files system.....	47
4.3. M2M-IoT Observations.....	48
4.4. Module .....	49
4.5. Descriptions of the simulation.....	49
4.5.1. Scenarios .....	50
4.5.2. Platforms .....	51
4.6. Demonstration and Evaluation.....	53

4.6.1. M2M-IoT module installation.....	53
4.7. Evaluation.....	54
4.7.1. Testing procedure.....	54
4.7.2. Packet Delivery Ratio .....	55
4.7.3. Average Energy Spent per Delivered Data Bit.....	57
4.8. Discussion of result .....	58
<b>5. CHAPTER FIVE .....</b>	<b>60</b>
<b>CONCLUSION AND FEATURE WORK.....</b>	<b>60</b>
5.1. Conclusion .....	60
5.2. Contribution of the study .....	60
5.3. Future work .....	60
<b>6. References .....</b>	<b>62</b>



## List of Figures

FIGURE 1.1: DODAG CONSTRUCTION [6] .....	3
FIGURE 1.2:DESIGN SCIENCE RESEARCH PROCESS (DSRP) MODEL [15].....	7
FIGURE 1.3:THE COOJA INTERFACE.....	10
FIGURE 2.1: ARCHITECTURE OF RPL ROUTING SUPPORT FOR SMART METER SYSTEM [55] .....	18
FIGURE 3.1: RREQ MESSAGE PROCESSING [53] .....	32
FIGURE 3.2: RREP MESSAGE PROCESSING [54].....	33
FIGURE 3.3: COMMON MESSAGE PROCESSING [55] .....	34
FIGURE 3.4: EVALUATION METRIC [60].....	36
FIGURE 3.5: M2M-IOT PROTOCOL ALGORITHM .....	38
FIGURE 3.6: M2M-IOT ROUTE DISCOVERY PROCESS [66] .....	44
FIGURE 4.1: CONTIKI FILESYSTEM HIERARCHY [99] .....	47
FIGURE 4.2: TRANSMITTING AND INTERFERENCE RANGES IN COOJA SIMULATION SCENARIO ...	51
FIGURE 4.3: PACKET DELIVERY RATIO FOR GRID DEPLOYMENT OF NODES .....	56
FIGURE 4.4: PACKET DELIVERY RATIO FOR RANDOM DENSE DEPLOYMENT OF NODES .....	56
FIGURE 4.5: AVERAGE ENERGY FOR GRID SPARCE DEPLOYMENT.....	57
FIGURE 4.6: AVERAGE ENERGY FOR RANDOM DENSE DEPLOYMENT OF NODES.....	58

## List of Tables

TABLE 2-1: RELATED WORKS SUMMARY .....	29
TABLE 3-1: IDENTIFYING VALID RREQ AND RREP MESSAGES .....	39
TABLE 3-2: RREQ PROCESSING ALGORITHM .....	40
TABLE 3-3:RREP PROCESSING ALGORITHM.....	41
TABLE 3-4: RERR PROCESSING ALGORITHM .....	41
TABLE 3-5:RREP-ACK PROCESSING ALGORITHM .....	42
TABLE 4-1: COOJA SIMULATION PARAMETERS .....	51
TABLE 4-2:CONTIKI PARAMETERS IN SIMULATED SENSOR NODES .....	52
TABLE 4-3: M2M-IOT PARAMETERS IN SIMULATED SENSOR NODES .....	53

## Acronyms

**3GPP:** 3<sup>rd</sup> Generation Partnership Project

**6LoWPAN:** IPv6 Over Low power Wireless Personal Area Network.

**AES:** Average Energy Spent

**AMI:** Advanced metering infrastructure

**AODV:** Ad hoc On demand Distance Vector

**BFD:** Bidirectional Forwarding Detection

**BSNs:** Body Sensor Networks

**BVR:** Beacon Vector Routing

**CoAP:** Constrained Application Protocol

**CTP:** Collection Tree Protocol

**CSMA-CA:** Carrier Sense Multiple Access-Collision Avoidance

**DAG:** Directed Acyclic Graph

**DAO:** DODAG Advertisement Object

**DIO:** DODAG Information Object

**DIS:** DODAG Information Solicitation

**DODAG:** Destination Oriented-DAG

**DSR:** Dynamic Source Routing protocol

**DSR:** Design Science Research

**DSRP:** Design science research process

**ER-RPL:** Energy Efficient Region based RPL

**ETX:** Expected Transmissions

**GEO-RANK:** Geographic Rank

**GOAFR:** Greedy Other Adaptive Face Routing

**GPS:** Global Positioning System

**HVAC:** Heating, Ventilation and Air Conditioning systems

**IEEE:** Institute of Electrical and Electronics Engineering

**IETF:** Internet Engineering Task Force

**IoT:** Internet of Things

**LBR:** LLN Border Router

**LEACH:** Low Energy Adaptive Clustering Hierarchy routing protocol

**LLN:** Low Power and Lossy networks

**LOADng:** Lightweight On-demand Ad-hoc Distance-vector Routing Protocol-Next Generation

**M2M-IoT:** Machine to Machine communication in Internet of Things

**M2P-RPL:** Multipoint to Point-RPL

**MRO:** Message Request Object

**MTU:** Maximum Transfer Unit

**NUD:** Neighbor Unreachability Detection

**OF:** Objective Function

**OLSR:** Optimized Link State Routing Protocol

**OSPF:** Open Shortest Path First

**P2M-RPL:** Point to Multipoint-RPL

**P2P-RPL:** Point to Point-RPL

**PDR:** Packet Delivery Ratio

**RAM:** Random-Access Memory

**RCMI:** Route Cache for M2M-IoT

**RFID:** Radio Frequency Identification

**RFO:** Region Formation Object

**RREP:** Route Reply

**RREP\_ACK:** Route Reply Acknowledgment

**RREQ:** Route Request

**RFC:** Request for Comment

**ROLL:** Routing Over Low power and Lossy networks (Working group)

**RPL:** IPv6 Routing Protocol for Low power and lossy networks

**SEQ-NUM:** Sequence Numbers

**UDGM:** Unit Disk Graph Model

**WPANs:** Wireless Personal Area Networks

**WSN:** Wireless Sensor Networks

# CHAPTER ONE

## INTRODUCTION

### 1.1. Background

Sensor networking is a core component of the future Internet of Things (IoTs), a major component of the billions of communicating machines that will eventually be incorporated into the global IP network, including products that range from actuators to home appliances, from smart meters to smart dust [1]. Depending on the type of sensor, sensors are instruments used for distributed and automatic tracking of different parameters, such as temperature, orientation, noise or radioactivity levels, etc. Communication networks from Machine to Machine (M2M) usually consist of thousands of extremely resource constraint devices associated with complex and lossy wireless communications of mainly volatile nature, known as Low-Power and Lossy networks (LLNs). For LLNs, routing is of vital importance, as data has to be distributed through enormous quantities of embedded devices with resource restrictions. The protocol stacks to put IoTs and M2M communications into practice have been established by standardization groups, such as IETF, IEEE, 3GPP [2].

A detailed study of wireless network routing protocols was carried out [3]. The routing protocols is divided into four major divisions (in this situation, regional routing is used for clarification purposes in cluster-based routing, since nodes in the same geographic area are considered to be in the same cluster, though not necessarily):

1. **Proactive routing:** This method of routing method allows the network nodes to regularly swap their routing tables (e.g., Link-state routing). The periodic sharing of routing tables exhausts the energy of the nodes given the energy constraint in WSN. The problem is more serious in mobile cases, since the topology of the network will change easily. RPL and OLSR [3] are examples of constructive routing.
2. **Reactive routing:** On source node demand, route establishment is processed. Whenever a node needs a connection to a particular destination, the node will start sending messages demanding the route [4]. In order to create the path, the destination then replies to the route request message. This method of routing has its benefits for mobile nodes, as the routing tables

are not expected to be shared. The Ad hoc On-demand Distance Vector (AODV) routing protocol [5] is an example of reactive routing.

3. **Hybrid routing:** Path establishment in hybrid routing, like reactive routing, is based on distributing route requests and route reply messages on source node demand between both source and destination nodes. The nodes have to swap routing tables between the nodes to keep the routes current. The Dynamic Source Routing (DSR) protocol [3] is an example of this approach.
4. **Cluster-based routing:** The deployed nodes pick a cluster head to manage distributing their knowledge to other network clusters. The unbalanced energy usage in the cluster heads opposite the relative nodes [6] is a big problem with cluster-based routing. If the network topology varies, mobility raises the complexity of cluster-based routing, requiring a very fast collection of cluster-heads depending on how rapidly the topology of the network changes. The Low Energy Adaptive Clustering Hierarchy (LEACH) routing protocol [3] is an example of cluster-based routing.

Major studies have recently been carried out [7][8] to facilitate the integration of sensor networks with the IP environment and the accessibility of smart objects to the Internet. IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) was introduced by the IETF Working Group to allow IPv6 packets to be carried over IEEE 802.15.4. The IETF Working Group on Routing over Low Power and Lossy Networks (ROLL) ultimately developed a routing protocol called the Low Power and Lossy Networks IPv6 Routing Protocol (RPL). RPL was proposed because none of the existing protocols such as AODV, OLSR or OSPF fulfilled the unique Low Power and Lossy Networks criteria (LLN). The RPL protocol targets large-scale wireless sensor (WSN) networks and serves a range of applications such as robotics or smart grid for manufacturing, urban, home and construction applications. The ROLL Working Group Charter stipulates that a number of different link layers should be controlled by the built routing protocol, including, but not limited to, low power WSN [9].

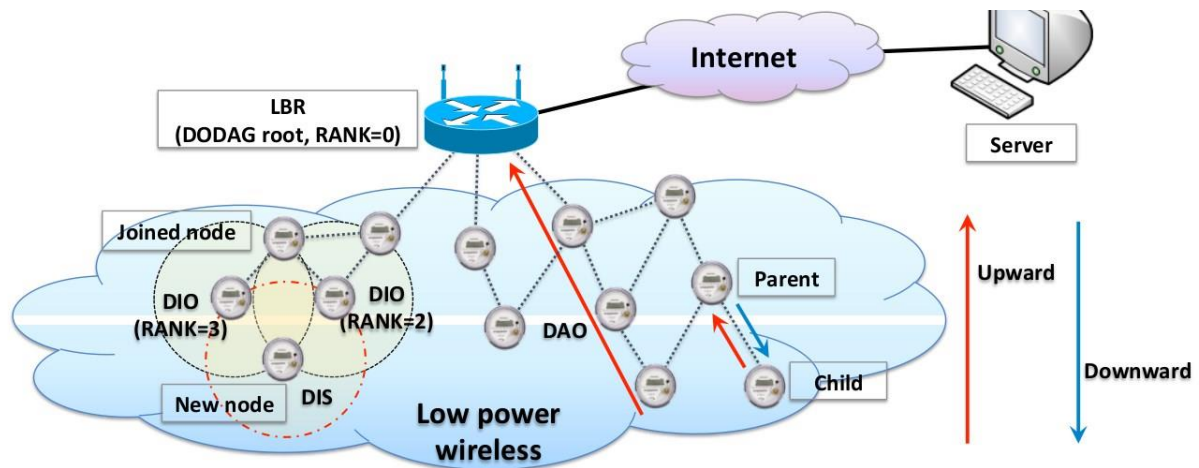


Figure 1.1: DODAG construction [6]

RPL organizes the network topology into a Destination-Oriented Graph (DAG), consisting of one or more Destination-Oriented Directed Acyclic Graphs, as seen in Figure 1.1. (DODAG). Each DODAG represents a routing tree, also known as a sink node or LBRR, generated by a root node (LLN Border Router). RPL uses the Objective Functions (OF) to create the DODAG, which adopts routing metrics to measure the optimal path between nodes and the DODAG root [10]. Thus, a logical topology based on a physical topology according to the OF used is the routing structure generated by the RPL.

To have effective routing support for the P2P traffic paradigm, RPL has been standardized. However, to the best of the researcher's understanding, owing to the technological specifications set out in [10], the implementation and architecture of RPLs in point-to-point communication is not yet satisfactory. Those parameters are presented as follows

**Traffic Support:** A LLN routing protocol must be capable of providing bi-directional communication between two arbitrary network nodes, allowing unicast, multicast, and any cast operation.

**Diversity of paths:** alternate paths for effective packet delivery (efficient packet delivery ratio of no more than three retransmissions) over lossy links need to be available.

**Convergence time:** It must converge within a few minutes of inserting a new node, within tens of seconds after re-establishing a node or losing connections, and in shorter seconds if no nodes have passed.

**Node property awareness:** Node specifications, such as power budget, memory and sleep interval, must be taken into consideration for routing. If necessary, it should be routed through mains-powered nodes.

## 1.2. Statement of the Problem

RPL builds a DODAG to enable routing for a source-destination pair RPL (RFC 6550 [11]) in a network in order to allow point-to-point data transmission in LLNs. The source node sends its message with DODAG to the root node, and root DODAG helps route messages between the source and the destination. Routing and preserving the route that the source node instantiates is the duty of the root node.

Low power and lossy network nodes are subject to extreme energy depletion by using point-to-point connectivity using RPL (P2P-RPL, from now on wards). This is due to the fact that the routing algorithms that work inside the nodes and the energy used during contact between the nodes. Because the performance of the network is strongly dependent on the energy available in the network nodes, for the longer life of the nodes and the network, energy reservation systems should be introduced. Constrained nodes are expected to send and receive control packets and this is extremely unsuccessful due to routing algorithms in play, P2P-RPL, and energy exhaustion can be induced.

Since nodes should relay their data message at hand through the root node and all the way to the destination, RPL is prodigal in power usage. Therefore, as a result of the implemented routing algorithm, all participating nodes were subjected to the ultimatum of losing resources.

An effort was made by researchers to address the question at hand. T. Winter, et al.[11] tried to build a P2P traffic support RPL network. A DODAG root must be able to redirect packets to a destination, but this has caused energy depletion to be severed by the nodes near the root node. In order to minimize control messages in P2P communication, Barriquello, Denardin, and Campos [12] merged RPL with a spatial routing strategy, but this work involves static nodes or nodes fitted with GPS. In order to save resources and build clear routes, Zhao, Ho and Chong [13] researched a region-based P2P route exploration that often involves certain location-aware nodes (e.g., via GPS), which is a complicated approach and adds additional new control messages in addition to



the default RPL messages. Anamalamudi, among others, et al. [14] reported paired DODAGs for P2P message exchange through asymmetric routes but the current version is still in draft form.

Therefore, the purpose of this study is to come up with a modified routing mechanism that reduces the waste of energy and to increase the packets delivered between the restricted nodes in low power and lossy networks in routing data packets and to improve the control messages for machine-to-machine communication specified in RPL (6550).

To this end, the current study attempts to investigate and answer the following research questions:

1. How to increase the packet delivery ratio for different message types exchanged by nodes in IoT scenarios?
2. How to reduce the energy required to route packets among nodes towards a more efficient network with lower overhead?
3. How to construct a robust and salient routing algorithm to IoT networks?
4. To what extent the routing algorithm improves IoT networks of node-to-node communication in a way to reduce time and energy for discovering the node of interest?

## 1.3. Objective of the study

### 1.3.1. General Objective

The general objective of this study is to design an algorithm for **Modified reactive route discovery algorithm for constrained machine to machine communication in low power and lossy networks (LLN)** so as to improve the point-to-point support of routing method of RPL.

### 1.3.2. Specific Objectives

To achieve the general objective of this study, the following specific objectives are considered.

- To understand low power and lossy networks by reviewing related works.
- To get knowledge of different simulator tools which are applied on low power and lossy networks.
- To increase the packet delivery ratio for different message types exchanged by nodes in IoT scenarios?

- To reduce the energy required to construct routes among nodes with a more efficient network and lower overhead
- To construct a simulation environment for the new proposed routing algorithm called M2M-IoT in section 3.
- To implement and measure the performance of the designed protocol.

#### 1.4. Methodology of the study

Methodology is a means of consistently addressing the issue of analysis using tools and procedures that are appropriate for discovering answers and answering research questions. This is used because it requires methods and processes to be specified in order to reach the intended goal.

##### 1.4.1. Research Design

This thesis follows Design Science Research (DSR), which is seen as a research practice that develops new or invents, creates inventive objects to fix problems or enhance the accomplishment of those new innovative artifacts, rather than describing or attempting to make sense of the current reality from it. It produces and assesses IT objects that are meant to address certain organizational challenges identified [15].

This research uses the model of the design science method suggested by Peffers [16] (see figure 1.2 below). It is a six-step process including challenge recognition and inspiration, solution target specification, design and development, demonstration, appraisal and communication. Study practices undertaken using the techniques and tools used are listed below. The authors of this study have provided a brief elucidation of the elements of analysis in design science and the work undertaken by the authors in each section.

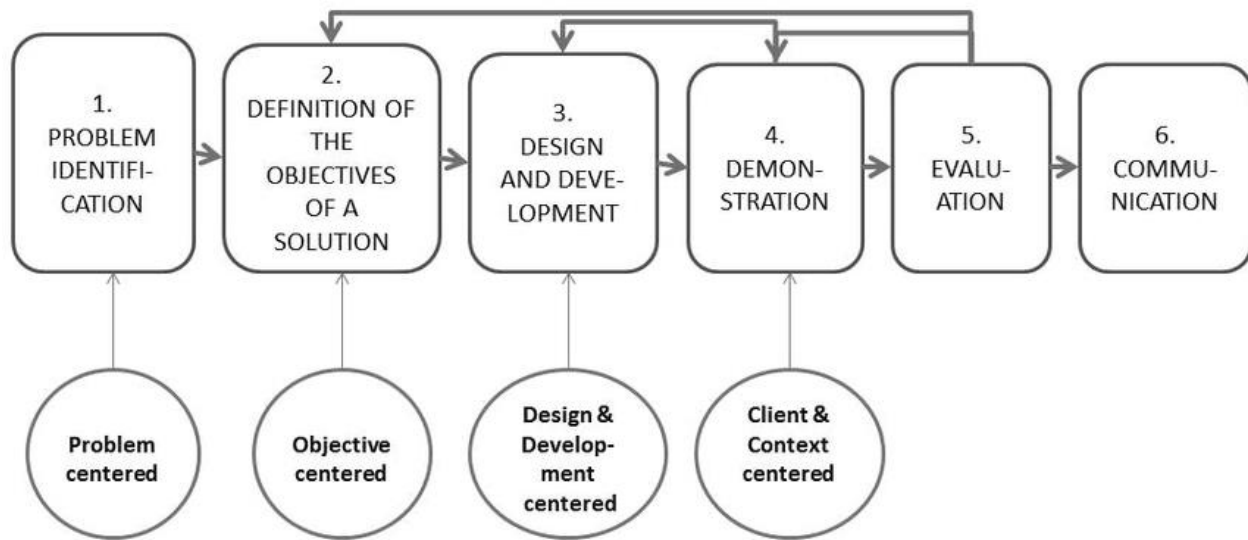


Figure 1.2: Design science research process (DSRP) model [15]

#### 1.4.2. Problem identification and motivation

This is the step in which the researcher can explain a solution's worth. This is useful for conceptually atomizing the issue so that the solution can capture the complexity of the issue. Two points are done by this. Next, the investigator and the listener are encouraged to find the solution and to embrace the findings. It also helps to explain the logic involved with an interpretation of the problem by the researcher. Therefore, by evaluating the method and understanding it fully, problems are found.

This is done by examining the existing algorithms and reading related works in depth from journal articles, conference papers, the Internet and simulation activities. The energy wasted and packets lost along the way are used as the motivation factor and detailed work is done to eliminate the identified problem.

#### 1.4.3. Objectives of a solution

Simulations is used to answer the issues for the design requirement and the solution is used in reducing the energy wasted in different scenarios like building, industrial and smart metering. The objective of the solution in this work is to eliminate the energy wasted and tackle the routing

problems in IoT by taking the issue one step forward. This in turn paves the way for more sophisticated devices to join the IoT community.

#### 1.4.4. Design and development

This aspect contributes to the construction, simulation, or instantiation of the work at hand, after the artifactual solution is narrowly established (Hevner et al. 2004). It helps to create a strong line between what to design and what not to design.

In his study the AODV algorithm is modified in a way it is used in IoT networks. The solution is developed via Contiki OS in the COOJA simulator because it is the environment highly supported by IoT devices (See detailed explanation in section 1.4.5).

#### 1.4.5. Demonstration

Demonstration implies the artifact's usefulness in solving the dilemma. Experimentation, simulation, case study, proof, or other relevant activity[16] could be involved. Therefore, experimentation and simulation was used in this research to demystify the accomplishment of the outcome.

For this purpose, COOJA (with Contiki OS) is used as a simulation tool: because of its popularity and applicability in the research field especially in IoT networks. COOJA comes with fully equipped protocols, models, algorithms and accessory tools, and it is an open software. Therefore, in terms of scientific acceptance, number of tools/modules and cost, COOJA would be an ideal choice for this study.

##### 1.4.5.1. Tools

###### 1.4.5.1.1. Contiki OS

Contiki is an Internet of Things open-source operating system. It links the Internet to lightweight, low-cost, low-power microcontrollers. It is a versatile toolbox designed to create complicated wireless networks.

Contiki offers efficient Internet connectivity with low power. Along with the latest low-power wireless standards: 6lowpan, RPL, CoAP, it supports fully standard IPv6 and IPv4. Even wireless routers can be battery-operated with ContikiMAC and sleepy routers from Contiki.

It offers multitasking and a built-in TCP/IP stack (Internet Protocol Suite), but requires just about 10 kilobytes of RAM and 30 kilobytes of read-only memory (ROM). A full device requires about 30 kilobytes of RAM, including a graphical user interface.

Contiki apps are written in standard C, Contiki networks can be emulated before burning into hardware with the COOJA emulator, and Instant Contiki offers a full development environment in a single download.

Contiki is open access, which means the source is always available and is always available. Without limits, Contiki can be used in both commercial and non-commercial systems[17].

#### 1.4.5.1.2. COOJA

A java-based wireless sensor network emulator cross-layer distributed with Contiki. It facilitates the simulation of various levels from the physical to the device layer, as well as the emulation of a collection of sensor nodes from the hardware [18].

The gui of the COOJA network emulator consists of five windows. The spatial structure of the nodes shows the network window. One could alter the physical location of the nodes in order to create a topology. Both the various colors are different due to their features in the network pane, i.e., the sink node has a green color and the sender node has a yellow color (See Figure 1.3). Node characteristics, each node's radio setting, node sort, and radio traffic between the nodes could also be seen visually in the windows of the network. The simulation control window allows one to control the simulation speed and stop, resume and restart the actual simulation that is running. The node window is used to write down the simulation principle and key points and save them in the node window [19].

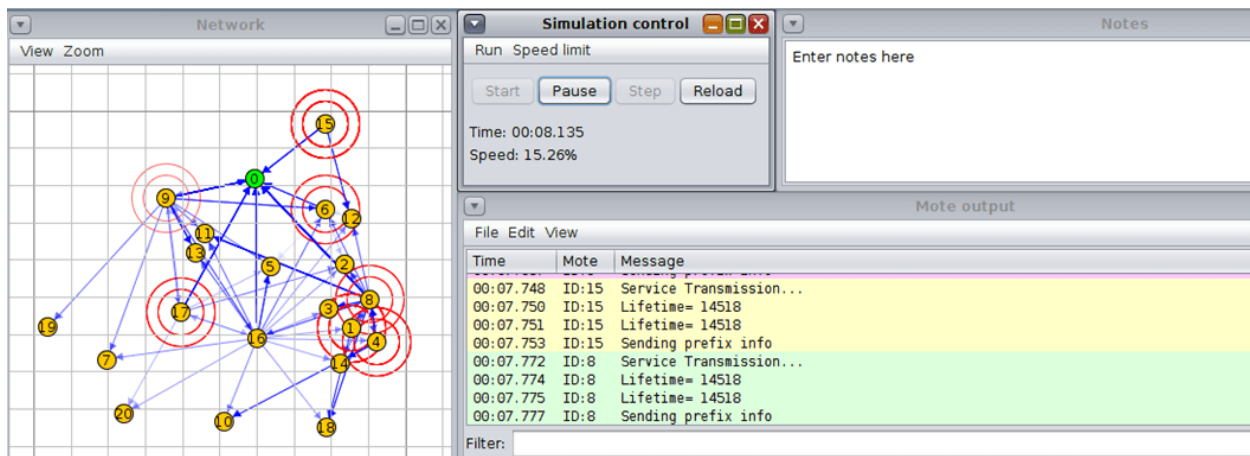


Figure 1.3: The COOJA Interface [18]

#### 1.4.6. Evaluation

This practice is used to observe and calculate how much an approach to the problem supports the artifact. This includes matching a solution's targets with real outcomes observed by the use of the artifact in the demonstration. Knowledge of applicable metrics and analytical techniques is needed.

The assessment process takes place between chapters and simulation effects at the conclusion of the deployment period and at any milestone. This allows the researcher to fill the holes that can exist in the road of addressing the issue at hand.

The most critical criteria need to be realized when determining the efficiency of the low power and lossy network routing guidelines. The investigator used two efficiency measures in this analysis to measure the performance of the proposed solution: energy and packet distribution ratio (See Section 4.7).

#### 1.4.7. Communication

This is the part where the stake holders are presented and to whom the research work is useful. Communication is the phase of this study where the final out put this research work is delivered to.

The result of the research work, problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness will be communicated to researchers and other relevant audiences. The thesis report will be submitted to the computing department for defense as partial fulfillment of the master's program. In addition, the researchers have also a plan to publish an article on journal and conference proceeding. The result of the study will be communicated for ethio-telecom for practical experimentation and to make them learn from the research experience.

### 1.5. Scope and Limitation of the study

The scope of this research work is to enhance the current route discovery mechanism used in Point-to-Point-RPL in memory constrained (non-storing), low power and lossy networks with IPv6 routing scheme having no mobility. Thus, in this study an effort is invested to design a routing protocol that finds a path to the destination node while increasing the delivered packets and decreasing energy wasted to discover routes. This is important in terms of saving power and minimizes continuous route discovery mechanism. Point to Multi point RPL (P2M-RPL) and Multipoint to Point RPL (M2P-RPL) are beyond the scope of this research work and will not be dealt with.

The proposed, M2M-IOT, is simulated and implemented using COOJA simulator in Contiki OS. Evaluation metrics are used to assess the performance of the routing mechanism. The detailed simulation procedures and parameters are presented in section 4 of this thesis.

An attempt was made to test the result with real IoT sensor nodes, due to the cost and material accessibility issues it was not attainable. In this study energy and packet delivery scenarios are evaluated. Route catching, error handling and other performance evaluation are left for future work. The control messages in P2P-RPL are no longer supported by the new modified algorithm even in some scenarios where the old algorithm works best comparing to M2M-IoT control messages.

## 1.6. Significance of the study

The significance of M2M-IoT is to provide connectivity to a large number of battery-operated embedded wireless devices that use low-power radios to communicate and deliver their data over multiple hops with each other. The practical implication of the design is suitable for resource-constrained devices in industrial, home, and urban environments. Further, it can be deployed in all memory and power constrained devices and can be used for machine-to-machine communication in the world of IoT.

The theoretical implication of deploying this work on machine-to-machine communication is to reduce the energy wasted in searching routing paths among the nodes. The study will also have a tremendous benefit for future researchers by indicating the state of the art and raising the unsolved issues in this work. Hence, researchers will be benefited in knowing the current state of the routing empire and they can do more to develop and modify related algorithms for another network types.



## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.1. Overview**

The Internet of Things (IoT) is called the interconnection of physical objects with an Internet access IP address [20]. Today, a large number of smart devices are related to the Internet. The number of smart devices interconnected through the mobile Internet is rising exponentially. IoT can be found in architectures, such as the [21] plan, which reflects a two-way communication architecture for smart energy meters and utility providers. IoT is a wireless sensor network that provides connectivity in the community region of a smart grid for metering devices. Mobility, which is a fundamental problem related to the identification of movement of mobile nodes and the availability of improved connections through an optimal range of routes, is another point discussed in the IoT [22]. There are a variety of contributions in the IoT literature, such as the following: analysis of topology control mechanisms [23], position and mobility in Wireless Sensor Networks (WSNs)[24] and routing dependent on objective functions[25][26][27][27]. The existence of devices such as cameras, Radio Frequency Identification (RFID) tags and smartphones, among other devices that can communicate with each other for a shared reason, is also known to be pervasive [28].

Initially founded in February 2008, the Routing over Low-Power and Lossy Networks (RoLL) working group specified the routing requirements for urban LLNs [29], industrial LLNs[30], home automation LLNs[31], and building automation LLNs[32]. The RoLL working group conducted a study to check whether the IETF standard routing protocols could satisfy the specified requirements in parallel with the specification of the routing requirements [33]. The RoLL detected, by the first assumptions, that the current routing solutions did not meet the specifications of LLNs. Since then, new routing solutions have been explored by the working group to include unique specifications for many forms of LLN applications [34] [35]. The IPv6 Routing Protocol for LLNs (RPL) was established as the standard routing protocol for LLN by the RoLL working group in March 2012. RPL is a constructive tree-based routing protocol, introduced in RFC 6550[36], which generates a guided acyclic graph between the leaf nodes and the boundary

path (sink node). While considered to be the basic routing protocol for IoT networks [37], RPL has posed many pitfalls since its development and new solutions have emerged to address them.

## 2.2. Characteristics of RPL

RPL is a constructive protocol for the distance variable [29]. A Destination Centered Guided Acyclic Graph (DODAG) is the basic construct in RPL, with a single RPL route serving as the root DODAG root. In addition to other RPL Routers, the DODAG Root has duties, including activating, configuring, and controlling DODAG, and (in some cases) serving as a central relay for traffic through and from other RPL Routers in the network. By generation and transmission of DIO (DODAG Knowledge Object) messages, the DODAG is built, indicating the rank of the router in the DODAG. Thus, RPL offers "upward" or "multipoint-to-point" routes to the DODAG root [36] from sensors within the network. By making sensors issue Destination Advertising Object (DAO) messages, "down-to-down routes" are allowed, propagating as unicast to the DODAG Root Object through preferred parents. For contact between devices inside the network and where none of the communicating devices is a DODAG root, 'point-to-point routes' are provided by default by letting the source sensor send a data packet through its default path to the DODAG root (i.e., using the upward routes). This would then either apply a source path to the received data packet to meet the destination sensor (downward routes in non-storage mode), or simply use hop-by-hop routing (downward routes in storage mode) to forward the data packet, depending on the "Mode of operation" for the DODAG [29].

### 2.2.1. Data traffic flow assumption

RPL makes a-priori assumptions of data traffic types and specifically describes three such types of traffic [36]: prevalent sensor-to-root data traffic (multipoint-to-point, MP2P), uncommon root-to-sensor data traffic (point-to-multipoint, P2MP) and exceedingly rare sensor-to-sensor data traffic (point-to-point, P2P). There are situations in actual systems where P2P traffic is a normal phenomenon. For starters, more than 30 percent of traffic can be P2P [38] in remote control in building automation. By using RPL, this will cause more network congestion and energy usage.

### 2.2.2. DODAG root requirement

It was with the principle of preventing a single point of failure that the Internet was designed: even if one or more routers cease service, the other routers in the network should be able to make the global network continue to run [39]. In the RPL, the DODAG Root is both clearly responsible and subject to particular requirements [40]. The DODAG Root is responsible for the determination and preservation of DODAG configuration parameters and the initiation of DIO emissions. The DODAG Root is also responsible (both in storage and non-storage mode) for providing ample topological knowledge to be able to create routes to all destinations in the network while downward routes are enabled. In theory, owing to the special memory/function requirement of DODAG core, RPL provides "Floating DODAGs" to provide internal communication in case the administratively provisioned DODAG fails. In such a case, the other network routers will either not have sufficient resources to act as DODAG roots or may both have to be supplied with sufficient resources to act as DODAG root roots (resources which is unused during normal network operation). Therefore, in an RPL routed network, the DODAG root reflects a possible single point of failure [29].

### 2.2.3. Fragmentation

In order to prevent link-layer fragmentation, it is desirable that applications in an AMI network generate small packets [41]. The frame size is only 127 bytes in 802.15.4[42], of which up to 25 bytes can be used for frame overhead, and another 21 bytes for link layer protection, leaving 81 bytes for layer-2 payload, respectively. The compressed IPv6 header absorbs (at least) 2 bytes by using the IPv6 compression mechanism [43], leaving (at best) 79 bytes for the payload of layer 3 data, such as routing protocol signals and device data, before fragmentation occurs. Although 79 octets may seem adequate to carry RPL control messages, note the following: ICMPv6 carries RPL control messages, and 4 octets are used for the mandatory ICMPv6 header. A further 24 bytes are consumed by the DIO base object of the RPL. If connection metrics are used, this consumes at least another 8 bytes, and this could take more by using a simple hop count metric. Up to a further 16 bytes are consumed by the DODAG Setup Object, for a total of 52 bytes [44]. Adding an Address Configuration Prefix Knowledge Object consumes another 32 bytes, for a total of 84 bytes, exceeding the 79 bytes required for the payload of layer 3 data and triggering link-layer fragmentation of such a DIO.

For data traffic, due to the use of source routing, RPL can further increase the risk of fragmentation in downward traffic for storage mode: a fixed source routing overhead of 8 bytes is levied for each data packet, plus a variable number of bytes for entries in the source route-the exact number of bytes depends on the address duration and the number of hops to be traversed. This would decrease the already small data payload space available, and raise the possibility of fragmentation. Of further notice, adding a source routing header to the DODAG root means that developers do not know what to expect from the MTU in advance, and thus applications can not accurately configure their data traffic to fit into an unfragmented frame.

#### 2.2.4. Link Bi-directionality

Parents (and the chosen parent) are picked based on reception of DIOs while a DODAG is constructed by RPL. This alone does not guarantee that an RPL router can interact efficiently with the parent. The specific usage of connections, though, is for "upward" paths, i.e., the use of a parent (the chosen parent) by the RPL Router as a relay to the DODAG Root - in the opposite direction to the one in which the DIO was received. In fact, unidirectional ties in wireless networks are not uncommon. Although RPL operations include bidirectional links, the RPL does not define precisely what methods should be used and how unidirectional links should be avoided. Winter et al. [45] proposed Bidirectional Forwarding Detection (BFD) or Neighbor Unreachability Detection to solve the issue (NUD). As it uses a constructive approach, BFD is specifically named "often not desirable" and is not treated (by RPL) as suited to LLNs. For NUD, it is invoked only when a switch fails. When attempting to communicate with the DODAG Core, an RPL Router can detect that its preferred parent is lost via NUD. If the RPL Router does not have any parents in its parent set, all it can do is wait: the RPL does not provide the RPL Router with any methods to respond to such an occurrence. Therefore, the RPL does not follow these mechanisms and does not specify an alternative mechanism [46].

#### 2.2.5. Loops

RPL' does not guarantee selection of loop free route or close convergence times for delay, but can find and restore a loop as soon as it is used. RPL uses this loop detection to ensure that packets move forward and, if necessary, cause repairs [45]. This means that only when data traffic

is routed across the network will a loop be observed and fixed. Data packets have to be buffered when a loop is detected and path repair is enabled. However, with restricted memory restrictions for LLNs, it might not be possible for all incoming data packets to buffer incoming packets during route repair, leading to dropped packets. This data packets must, depending on the transmission protocol, be retransmitted by the source (increasing the demand on the network) or be dropped.

### 2.3. Application of LLNs in relation to RPL

The RPL is used as a structured approach for the efficient provision of secure interoperability across arbitrary devices across IoT and M2M network domains [93]. However, the specifications of various routing applications for LLNs vary from one application to another, so the basic routing requirements should be handled in compliance with the specific routing application. The routing specifications for RPLs to enable various implementations of LLNs have been explored in depth in current literature, ranging from urban networks [29], industrial control [30], home automation [31], and building automation [32].

In this segment, two famous LLNs with RPL applications are added. Home Security and Building Monitoring The pervasiveness of Wireless Personal Area Networks (WPANs) and Body Sensor Networks (BSNs) has recently drawn significant interest in home automation applications, such as healthcare, window blind lighting control and automatic lighting. The building management framework comprises, in fact, of an interrelated subsystem of numerous roles, such as the HVAC system, the lighting system and the control system [93]. In addition, a vast range of actuators, controls, sensors and digital gadgets are used, such as mobile phones, laptops and smart watches, etc. However, it is almost difficult to achieve direct contact in a large-scale network due to the small coverage spectrum of the radio. In addition, wireless signals usually suffer from high interference and extreme path loss in the home and building area due to the cement construction system and dense spectrum resource use. Reliable networking is also of vital importance for the effective use of capital through energy efficiency and tighter regulation of home automation and construction control. A vast number of energy-constraint systems and insecure wireless channels, which are known as LLNs, are part of the home and development network. In addition, as RPL is considered to be the influential candidate to serve the home and development network, essential criteria need to be met [47][48]. Requirements include agility, handling, stability, protection, fast

convergence time, low cost of configuration and flexible choice of routes in compliance with the application.

Advanced Metering Service Services (AMI) [49] is an automated framework comprising of contact networks, smart meters and data collection systems. In the meanwhile, AMI (shown in Figure 2.1 below) facilitates the setup, calculation and regulation, delivery and utilization of resources by two-way communication, e.g., gas, electricity and water. In AMI networks, there are a wide number of endpoints that are linked by a wired or wireless networking network, such as smart meters and home area network components, etc. In fact, there is a back-haul network in the utility control office that offers software maintenance access. In addition, various wireless protocols, such as WiFi [50], Ethernet [51], IEEE 802.11ah [52] and IEEE 802.15.4 [53] and WiMax [54], are built into the field area router, which bridges the AMI system with the external networks. The AMI network needs a wide scale, self-configuration, efficient choice of paths, low maintenance costs, multicast and support for any routing. RFC work has described the applicability of RPL to AMI deployment [49]. In particular, the RPL is designed to use energy-efficient routing methods and energy-conscious metrics. RPL will easily support heterogeneous networks in which the nodes and connections are fitted with different technologies, with the ability to support different metrics and constraints. The problems discussed by [55],[56] for the effective collection of data in AMI with RPL.

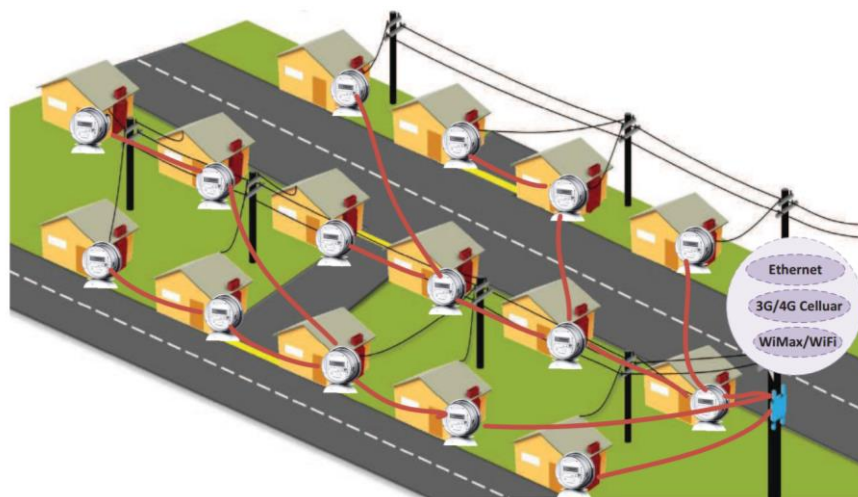


Figure 2.1: Architecture of RPL routing support for smart meter system [55]

#### 2.4. Challenges of LLNs in relation to RPL

RPL has emerged as a popular candidate for routing in IoTs and M2M communications due to its great flexibility [57]. Due to the extreme resource constraints and lossy environment of LLNs, it is not trivial for RPL to achieve good routing efficiency. In RPL and P2P-RPL, there are several open problems that need to be carefully handled for the omnipresent real-world use in LLNs applications. Any of the main issues are outlined below:

#### 2.4.1. Efficient routing support for generic traffic patterns with limited memory

Applications for LLNs include reliable routing support with heterogeneous node capabilities for generic traffic patterns, such as MP2P, P2P, and P2MP [58]. As stated earlier, RPL creates DODAGs in a way that optimizes the routing support for the traffic pattern of MP2P. However, data transmission needs to move through the pre-established DAG for other traffic patterns, such as P2P and P2MP. As a result, RPL does not have adequate routing support and longer latency and lossy connections suffer from data transmission. More precisely, P2P correspondence, which is a common prerequisite for different implementations of LLNs, needs to be supported by an RPL intermediary. The root must serve as an intermediary in the non-storing mode. As a consequence, when traffic is heavy, the root quickly becomes the bottleneck. Downward paths in a DODAG are used to support P2MP traffic. Due to the asymmetric design of wireless networks, downward routes may not, however, be the best-quality route. The asymmetric nature of wireless links, especially for LLNs, has a major effect on the efficiency of routing protocols. Protocols that do not understand connection asymmetry fail as asymmetric connections are found in real-world implementation [59].

#### 2.4.2. Energy-efficient route discovery under severe resource constraints

In LLNs, because of limited memory and buffer space, the optimum route between two arbitrary nodes is not given by design. So, to facilitate P2P communications, route discovery is normally needed. P2P-RPL seeks the best quality route as a reactive routing protocol, resulting in a large number of head controls, especially in dense large-scale networks. Both nodes in the network need to engage in the creation of temporary DODAGs during path exploration, contributing to considerable energy costs. It is important to discover the optimal route in an energy-efficient manner in LLNs [60]. In protocol architecture, achieving energy-efficient route discovery without losing reliability is also a key issue.

### 2.4.3. Reliable and energy-efficient routing in LLNs.

Two key priorities for developing routing protocols for LLNs are power efficiency and efficient data distribution. Although RPL supports multicast, according to a basic objective function, it selects a single node as its preferred parent. However, the complex and lossy wireless networks do not cope well with single path routing. Wireless channel unreliability leads to packet loss and substantial retransmission, resulting in high energy usage and long occupancy period of the channel. Energy efficiency and reliability are a difficult challenge to achieve simultaneously, especially in LLNs.

### 2.4.4. Congestion detection and control

Network congestion occurs at both the level of the node and the level of the connection, and also occurs in LLNs. Nodes in LLNs typically have a small buffer size, resulting in high traffic overflows, especially with burst traffic. In addition, congestion degrades the overall efficiency of the service and boosts error rates, leading to channel contention, packet drop and increased delays. Several approaches to alleviate the dilemma of network congestion have been proposed. Three key approaches exist: changing the level of traffic, re-routing the traffic and splitting the traffic into multipaths.

**Adjusting the traffic rate** [61], Which notes that congestion causes deterioration and error rates to rise across all channel quality in wireless sensor networks, leading to buffer declines and increased delays (as in wired networks), and appears to be grossly unjust to ward nodes whose data must pass a greater number of radio hops.

**Re-routing the traffic as congestion occurs** [62], each sensor node can have a different priority, because sensor nodes can be mounted in an area with different kinds of sensors.

**Splitting traffic to multipath** [63], This provides the value of storing only the required paths, eliminating the need for broadcasting, reducing memory needs and excessive repetition. This is a loop-free path preserved with the use of sequence numbers of destinations and is scalable to large communities of nodes.

However, these current methods do not have effective routing support for LLNs without recognizing the lossy existence of LLNs. The RPL specification does not have a good framework for handling congestion. Therefore, an effective method of identification and control of congestion is in urgent demand to mitigate the problem of congestion and boost RPL efficiency [92].



#### 2.4.5. Mobility support

For static networks, RPL is designed [26]. However, many applications for LLNs need mobile node routing support. Mobility increases the dynamics of networks significantly. For instance, the preferred parent of a node is temporarily not available, forcing it to drop packets and transfer the preferred parent to. The latency of data transmission is greatly increased by this process. The RPL needs appropriate modifications to support networks consisting of entirely or partly mobile nodes [32].

#### 2.4.6. High throughput with a low duty cycling of lower layer

IEEE 802.15.4[64] is intended to reduce interruption and multipath fading and runs on incredibly low power and is known as the ideal candidate for layer protocols for medium access control (MAC) to support IoTs and M2M communications. Reservation of guaranteed time-slots, exceptionally low-power consumption with low service cycles and a carrier sense multiple access-collision avoidance (CSMA-CA) device are some other significant features of IEEE 802.15.4. Dynamic duty cycling has been shown to have a substantial effect on network layer protocol performance, causing long latency, low packet delivery ratio, and low throughput [65]. The functionality of other layer protocols should be included in developing routing protocols. A cross layer architecture is therefore required to optimize the efficiency of the RPL.

#### 2.4.7. Workload balancing strategy for RPL

The random implementation of nodes and heterogeneous traffic trends in LLNs results in unbalanced workload distribution. As a consequence, nodes exhaust their resources rapidly in the hotspot zones. Nodes near the gateway typically deplete their resources faster than other nodes, known as the "Energy Hole Problem"[66], in data collection applications, which seriously impact network performance. To mitigate the problem while preserving the optimal reliability, an effective data collection method is required [67]. Workload sharing is also an optimal solution to addressing the issue of power gaps and maximizing the existence of the network.

#### 2.4.8. Security issues

In RPL, the protection architecture is not up to the mark. Techniques for forming stable connections and sharing keys are not specified for RPL authentication and management [68]. In

RPL, DODAG's joining mechanism is not stable. Packets may be dropped and if any malicious node enters a DODAG, data may leak. RPL is easily exposed to attacks as a result. In addition, applications for LLNs, such as the e-Health system, typically handle very private and sensitive information that cannot be disclosed to unauthorized parties [69],[70]. It is therefore essential to design security mechanisms and improve the preservation of privacy in the RPL. Information must first be encrypted and transmitted as cipher-text in order to preserve user privacy. Encryption, however, increases the size of data and creates overhead communication, which may be unacceptable for some applications of LLNs, particularly when information is frequently collected [71]. Furthermore, end-to-end encryption not only has a high computing burden and energy consumption, but also increases latency. Further research is needed to develop security mechanisms that are appropriate for LLNs.

## 2.5. Routing protocol in LLNs

LLN applications have gained increasing interest from both research entities and industries in recent years, calling for a universal solution to allow omnipresent connectivity for huge numbers of low-cost and low-power embedded devices. By describing the features of the main routing protocols and providing a comparison of their features, the key insight underlying this section is to survey and discuss a comprehensive set of routing protocols proposed for LLNs. Apart from the high-level clarification in section 1.1. of the routing protocols the next section presents the existing LLNs routing protocol categories: proactive routing, re-active (on-demand) routing and geographic routing highly related with this study.

A number of reactive routing protocols have been proposed to provide routing support for LLNs based on Ad hoc On-Demand Distance Vector Routing (AODV) [72], including AODVjr [73], AODVbis [74], LoWPAN-AODV [75], LOAD(ng) [76], [77], TinyAODV [78], NST-AODV [79]. Such routing protocols make AODV adaptation/simplification low-footprint and appropriate for resource constraints and dynamic network environment.

A second set of proactive routing protocols, including but not limited to the Collection Tree Protocol (CTP)[80], Hydro[81], ZigBee Cluster Tree[82] and RPL[83], are also proposed.

The third category is geographic routing, where the location or coordinates are known either as a priori knowledge or through a self-configuration localization scheme for each node or partial node. One of the geographic routing protocols designed to support routing for LLNs is Beacon Vector Routing (BVR)[80].

Moreover, as a star-based topology, the IEEE 802.15.4/ZigBee Cluster-Tree protocol [84] forms the network. In particular, through periodic beacon frames, the synchronization in the ZigBee Cluster-Tree protocol is achieved. In addition, the Cluster-Tree protocol supports multi-hop networking. There is a Zigbee coordinator governing every cluster as a hierarchical routing protocol. However, if the beacons are sent in an unorganized fashion, the collision takes place easily. In addition, an approach to time division is proposed in [85], which addresses the problem of the beacon collision. As a star-based network, however, the Cluster-Tree protocol does not offer support for scalability, as the number of nodes is restricted by the Zigbee coordinator's limited coverage. This is especially unacceptable for LLNs that are usually large-scale networks. A reactive routing protocol derived from AODV for LLNs is a Lightweight On-demand Ad-hoc Distance-vector Routing Protocol-Next Generation (LOADng) [86].

LOADng's simple operation is identical to that of AODV, which makes certain simplifications feasible. Path request (RREQ) messages are spread across the network during the route discovery period. When the destination receives an RREQ response, the route-reply (RREP) message responds through the reverse direction. More track patterns are provided by LOADng, such as point-to-point (P2P), point-to-multipoint (P2MP), and multipoint-to-point (MP2P). But this indicates a downside relative to RPL [87] in terms of a lot of overhead for MP2P traffic pattern. The key explanation behind this is that, given a clear goal, LOADng distributes control messages across the network for the best route exploration. Different traffic dynamics have been used for the efficiency comparison and study of LOADng with RPL [88],[89].

TinyAODV[78] is a simpler version of AODV introduced on the MICAz TinyOS operating system. Similar to LOADng, RREP messages are created only by the destination node. TinyAODV is implemented with a link failure detection feature that is disabled by default. TinyAODV discards the undelivered data packets originating from the link split in order to attack

static networks. In comparison, the local fix is not supported by TinyAODV and hop counts are taken as its routing metric.

TinyAODV Version 2 supports multi point to point (MP2P) traffic where the destination node can only be the sink node. Though TinyAODV Release 3 allows for connectivity between two arbitrary network nodes successfully [79]. Hydro [81], a hybrid routing protocol combining local agility with centralized control, is proposed to provide efficient data collection and powerful point-to-point connectivity support on the basis of the priori work in[90]. A distributed algorithm is used in Hydro to form a direct-acyclic-graph for routing data from network nodes to boundary routers. Specifically, nodes periodically send the topology reports to the border routers to allow the border routers to have a knowledge of global topology. This allows basic point-to-point routing with the b-order router, which serves as an intermediary for the movement of packets to the destination [81]. Beacon Vector Routing (BVR) [84], proposed for LLNs, is a geographical routing protocol. With the position comprehension of a series of landmarks, virtual coordinates are obtained by each node in the network. In a greedy way, the package is sent to the destination. In fact, nodes select the node nearest to the destination as their next hop to the destination of the liver data packet.

Geographic routing has the benefits of allowing overhead and scalability, but when choosing the next hop, it does not take into account the lossy existence of wireless connections. Geographic routing will however not cope well with the lossy wireless medium and provide LLNs with effective support for data transmission. In addition, certain regional routing protocols enable nodes to retain multiple states and have to regularly swap the one hop or even two hop neighbor table [91], which is very expensive for a network limited by capital. CTP [92] seeks to promote efficient data collection as a constructive gradient-based routing protocol. In LLN applications, the prevailing coordination model is collection-oriented, also known as multipoint-to-point/many-to-one flow.

As a tree-based collection protocol, CTP uses the expected transmissions (ETX) for next-hop selection as the routing metric. In particular, in CTP, an accurate link estimator is developed that uses the data and control traffic to report the link estimates. In addition, an additive cost is calculated in CTP based on the link lossy rate. In CTP, a node chooses the node that, as its next hop, provides the lowest accumulated ETX value. It has been mentioned that the two problems

that can occur in CTP[80] are routing loops and packet duplication. RPL is a CTP extension that inherits and enhances the validation of the data path and adaptive beaconing from CTP. The current LLN routing protocols either optimize for data collection traffic or focus exclusively on the paradigm of point-to-point traffic in homogeneous networks. An increasing support for a hybrid of these traffic paradigms in heterogeneous networks is expected to be motivated by the fact that the wide variety of LLN applications are becoming more general. RPL is considered as the most promising routing protocol for LLNs because of its comprehensive features and great flexibility. Specifically, as a proactive routing protocol, RPL supports various traffic patterns, including multi point-to-point (MP2P), point-to-point (P2P), and point-to-multipoint (P2MP). It thus prevents the use of the RREQ message and supports the low overhead delivery of data. In addition, RPL provides local and global repair support for the benefit of both flat and hierarchical topologies to be resilient to the dynamics of LLNs.

## 2.6. Related Works

T. An RPL routing protocol supporting P2P, P2MP and MP2P traffic was standardized by Winter, et al. [11]. However, the DODAG root must be able to route packets to a destination in the case of point-to-point communication, but this leads to exposed nodes near the root node to cut energy depletion (See section 2.7).

The geographic routing approach for 6LoWPAN was presented by Barriquello, Denardin and Campos [12]. RPL and GOAFR (Greedy Other Adaptive Face Routing) [93] are the basis of the proposed GeoRank. In networks with high link density, the GOAFR algorithm is able to seek optimal or sub-optimal routes. However, RPL can demonstrate better performance than GOAFR when considering networks with low link density. The authors therefore suggested GeoRank, seeking to combine the best of two approaches. The objective of the approach is to improve 6LoWPAN's P2P support and to reduce the amount of control messages required for this type of traffic. The GeoRank algorithm initially calculates the distance between the source node and the destination based on the DODAG root list during its operation. After that, the root with the lowest absolute angle difference is selected as the anchor node between the source and the destination. Subsequently, using greedy forwarding, the algorithm attempts to perform packet routing. The node holding the message tries to send it to its neighbor with one hop in this mode to reach the destination of the message. If this is not possible, the GeoRank mode is assumed by the algorithm

and the packet is then forwarded to the preferred parent on the path to the selected anchor. This forwarding process should take place until a node nearer the destination than the anchor node is reached by the message. If this condition is achieved, it is again assumed that the greedy forwarding mode. Otherwise, the message reaches the anchor and is forwarded until it reaches its destination in the GOAFR face-routing mode. In GeoRank, all nodes of the network must be static or equipped with GPS due to the use of geometric calculation. If they can communicate with a static node using just one hop, mobile nodes can be used. In addition, the message to be routed must store information about its anchor's location. Although the authors used the smart lighting framework as an example of the GeoRank application, they emphasized that the suggested solution could not satisfy the specifications of this form of application.

Provided that the majority of RPL P2P routing protocols flood the network with control packets to create DODAG paths, causing high overhead and energy consumption, Zhao et al.[13] suggested the Routing Protocol based on the Energy-Efficient Region[13] (ER-RPL). The goal of the approach is to allow energy-efficient P2P communication without damaging the stability of the network. A hybrid solution is proposed by ER-RPL, combining RPL-based constructive and reactive functions. The protocol's key concept is to segment the network into various regions and realize the exploration of the P2P path, only considering the areas in which the nodes are situated. To this end, ER-RPL requires location-aware (e.g., equipped with GPS) nodes in the network, called reference nodes, to exist (RN). In order to segment the network into separate regions and to measure the distance between nodes and RNs, the protocol uses RN coordinates. After that, the nodes should pick their areas, depending on the distance to the RNs. Each area is defined by a binary number called the Region Code (RC). This process happens as the RNs overload the network with Area Formation Object (RFO) control messages at the initial stage of the protocol. For P2P contact, the source node can first send a P2P path request using the root node, i.e. the default RPL route, to the destination node. A control message called Message Request Object is used to render this request (MRO). The destination node can check, after obtaining the MRO, if the current path is acceptable on the basis of the cost of the route. If valid, the destination node should notify the source node, through the reverse path and using the MRO, to start sending data. Otherwise, the destination will start the region-based route exploration process. The destination node uses MRO in this method to construct a temporary DODAG, considering only the regions between it and the source. This DODAG is subsequently used to send packets of data. Note that

RN does not realize any mission at this stage. Thus, although complicated, ER-RPL working will minimize the power consumption of the network by preventing the flooding of the entire network with the P2P route discovery packet. In addition, the solution facilitates the sending of P2P messages without the use of a root node, providing near-optimal routes that can satisfy applications' reliability requirements. ER-RPL uses the framework provided by the default RPL working for other traffic patterns, such as MP2P.

The Ad hoc On-Demand Distance Vector Routing-Based RPL (AODV-RPL) [71] appears as an RPL enhancement to support the P2P traffic pattern throughout the process of route exploration, considering both the symmetric and asymmetric connections. The peer-to-peer paths in AODV-RPL are built on demand as P2P-RPL. When the current path does not satisfy the implementation criteria or the intended path does not exist, a source node starts the route construction process to the destination. The source node must then send DIO-RREQ (DIO with Route Request Content) messages to create an instance of RREQ (DODAG generated by the RREQ message originator) to find a path to the requested destination node. The DIO-RREQ area provides details about whether the path is symmetrical or asymmetrical (S field). Each node receiving the DIO-RREQ must check the bidirectional relation state, update the S field if appropriate, and choose whether to enter the RREQ-instance. In this case, all routes that use this connection are called asymmetric if the link is set as asymmetric. When DIO-RREQ reaches its destination, the node must choose how to address the request for route formation, depending on the S field. The destination node may also wait to receive DIO-RREQs from other routes for a predefined time. If the message field S indicates that the created route is symmetrical, DIO-RREP (DIO with Route Reply Content) should be unicast by the destination node to the originator DIO-RREQ through the created direction. This single path can then be used for data transport in both directions, since it is symmetrical. Otherwise, if the generated route is asymmetric, the destination node could start generating a DIO-RREP (DODAG created by the destination of the RREQ message) multicast to its neighbors. DIO-RREPs are forwarded to validate the relation symmetry, similar to DIO-RREQs, before the DIO-RREQ originator is reached, which should initiate the transmission of data messages along the route generated by the DIO-RREP after receiving it. Notice that a pair of DODAGs (RREQ-instance and RREP-instance) with a single-route discovery method can be generated if AODV-RPL does not find a symmetric path between two nodes. Therefore, two separate routes can be used to exchange P2P data messages: a route from A to B

and another from B to A. AODV-RPL, however, is still an Internet-Draft IETF and can undergo modifications before it is fully specified. Table 2-11 provides a description of the associated works analyzed.

## 2.7. Research gap

For point-to-point (P2P) traffic, RPL DODAGs have a simple framework. A DODAG root must be able to redirect packets to a destination in order for an RPL network to serve P2P traffic [11]. A packet flows to a root before the root that has a known path to the destination is reached. If nodes are unable to store paths, the common ancestor is the DODAG root (non-storing mode). It could be a node closer to both the source and the destination in other situations (storing mode).

The key concern discussed in this research is the incompetence of machine-to-machine interaction. In the IoT environment, this is found in power and memory limited devices. The current RPL protocol facilitates an unreliable machine-to-machine routing system for power and time. Therefore, this thesis offers an updated algorithm, M2M-IoT, to solve the problem described above. In cases where only point-to-point communication is required instead of using RPL as the switched mode of operation or in standalone but not concurrently, the suggested approach is used.



Table 2-1: Related Works summary

<b>Authors</b>	<b>Topic</b>	<b>Approach</b>	<b>Remarks</b>
T. Winter, R. Alexander et al [11]	<ul style="list-style-type: none"> <li>- RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks</li> </ul>	<ul style="list-style-type: none"> <li>- A packet flows towards a root until it reaches the root that has a known route to the destination.</li> </ul>	<ul style="list-style-type: none"> <li>- The root nodes are depleted and vulnerable to extreme energy loss.</li> </ul>
Barriquello, C.H et al. [12]	<ul style="list-style-type: none"> <li>- A geographic routing approach for IPv6 in large-scale low-power and lossy networks</li> </ul>	<ul style="list-style-type: none"> <li>- Stops DAO messages from being received.</li> <li>- Improves scalability thus decreasing memory consumption</li> </ul>	<ul style="list-style-type: none"> <li>- Includes static nodes or GPS-enabled nodes.</li> </ul>
Zhao, M. et al. [13]	<ul style="list-style-type: none"> <li>- An Energy-Efficient and Self-Regioning Based RPL for Low-Power and Lossy Networks</li> </ul>	<ul style="list-style-type: none"> <li>- Stops the whole network from overflowing of P2P control messages, resulting in substantial energy savings.</li> <li>- Raises the ratio of P2P packet distribution</li> </ul>	<ul style="list-style-type: none"> <li>- Some location-aware nodes are needed (e.g., with GPS)</li> <li>- A multifaceted approach</li> <li>- In addition to the default RPL messages, additional control messages are added.</li> </ul>
Anamalamudi, S. et al. [14]	<ul style="list-style-type: none"> <li>- AODV based RPL Extensions for Supporting Asymmetric P2P Links in Low-Power and Lossy Networks</li> </ul>	<ul style="list-style-type: none"> <li>- During route exploration, the bidirectional relation state is taken into consideration.</li> <li>- Monitoring signals may be rendered smaller.</li> </ul>	<ul style="list-style-type: none"> <li>- Establishes paired DODAGs for P2P message sharing via asymmetric routes.</li> </ul>

# **CHAPTER THREE**

## **DESIGN AND DEVELOPMENT**

### 3.1. Overview

The goal of this research is to change an algorithm used to build an energy-efficient and time-efficient routing protocol for M2M-IoT communication. Due to the energy constraints of IoT equipment, increasing the life cycle and device efficiency of wireless sensor networks are critical goals. Routing protocols are introduced when a source node requests to transfer data to a destination, to balance the traffic flow between the nodes in the network. Not only does an IoT routing protocol have to accurately deliver data between a different source node and a destination node, but it also needs to be energy and time efficient.

With IoT, energy is a vital object requiring protocol awareness [94][95] A cumbersome problem is the conservation of energy in wireless sensor networks. The issue extends to a level where sensing capabilities are carefully considered before they are added to the wireless node. The application type is an important factor in the energy utilization of sensor networks because it reflects the level of service required by the end user. In various environments, sensor nodes are expected to be deployed: indoor and outdoor [96] Indoor environments provide the luxury of an infinite AC power source that reduces the energy constraints to none. In outdoor environments, however, sensor nodes rely on the source of battery power to exchange information with each other. Applications range from civilian-based mobile networks (e.g., cattle monitoring) to high-level applications based on mobility (e.g., military tracking and observation). In order to extend the lifetime of the networks and with a mild effect on the overall system throughput, data transmission and reception between sensor nodes must be balanced and light [97].

Supporting efficient communications is the main objective of any routing protocol. The design of a routing protocol must be based on the features of its target networks in order to achieve this objective. Due to the severely limited resources and highly dynamic nature of wireless communication, this requirement for network-specific design is particularly important for wireless networks. The strict energy constraints of sensor networks, for example, require energy efficient routing to be designed. Node mobility in ad hoc networks requires routing protocols that can

quickly converge. In mesh networks, the heavy traffic load requires load-balanced routing systems. Existing literature focuses on designing different routing metrics for different wireless networks in order to satisfy such diversified requirements. For example, some routing metrics capture a path's stability, some concentrate on energy consumption, and some are more concerned with a path's bandwidth.

### 3.2. M2M-IoT Route Discovery

When a node wants to send a data message, its Routing Set should look for a route to the destination of the message. The node should forward the message to its destination via the next hop node if the path is found. The node should, however, start a new route discovery process if the desired destination is not found. The node generates a new route request (RREQ) message in the routing discovery process and defines itself as the originator and the address of the desired destination in the destination field. A unique sequence number for the RREQ should also be set and the other message fields defined. The node should then transmit, to its neighbors, the generated RREQ.

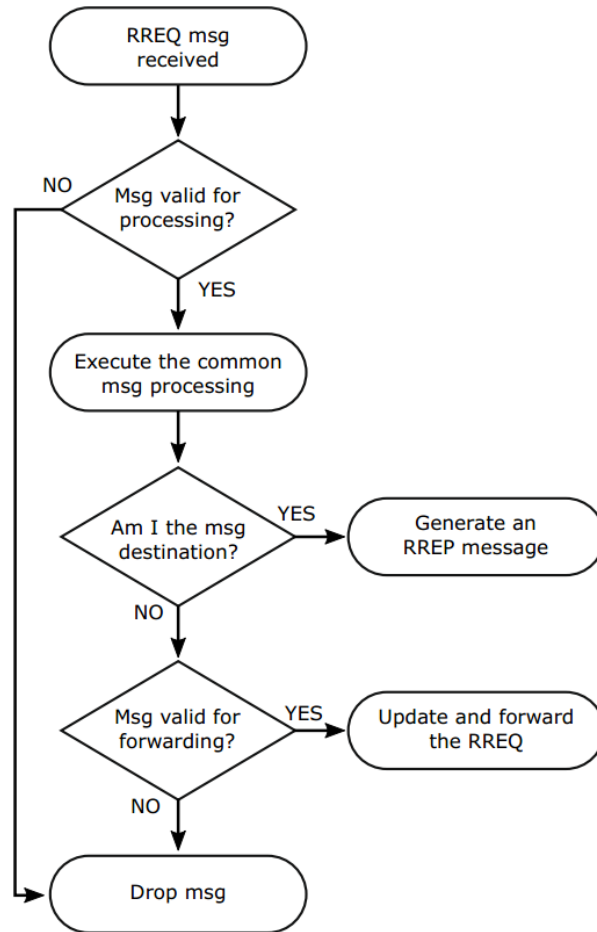


Figure 3.1: RREQ Message Processing [53]

According to the flowchart presented in Figure 3.1, each receiver of the RREQ message should execute its processing. The generated RREP message should have the RREQ originator address as the destination, its originator address in the originator field, and a unique seq-number. The RREP should be sent in unicast to its destination after being generated. Thus, the originator of the RREP should look for a route entry on its Route Set to the destination and forward the message to the next hop node. Note that the route entry should be located after the received RREQ message has been created.

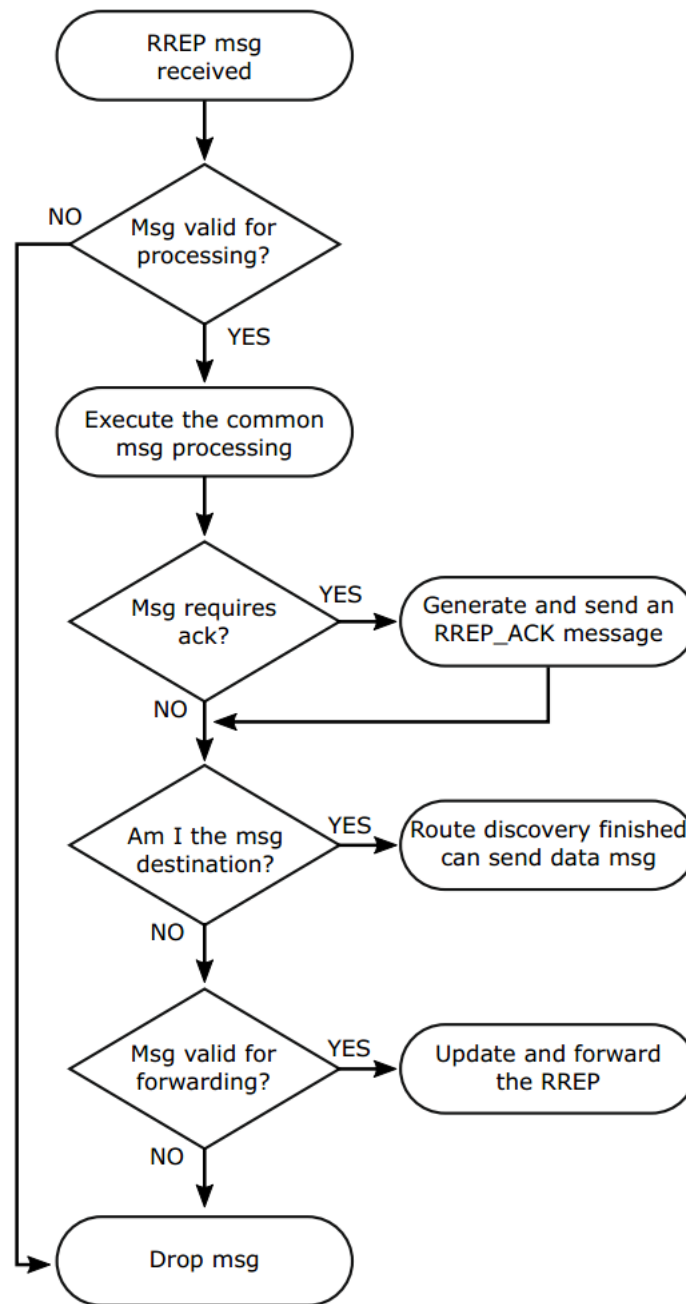


Figure 3.2: RREP Message processing [54]

As described in the flowchart in Figure 3.2, a node that receives the RREP message should perform its processing. The message is submitted to common message processing after the first validation (similar to an RREQ message and following the flowchart in Figure 3.3). The RREP receiver should verify the need to generate and send an RREP ACK message after this processing. In sequence, the node should verify whether this is the message destination. If not, the node should

check whether the message is valid for forwarding, check its Routing Set for an entry to the RREP destination, and use unicast to send the message to the next hop node. Otherwise, the route discovery process is completed if the node is the RREP destination and the data message can be sent using the constructed path.

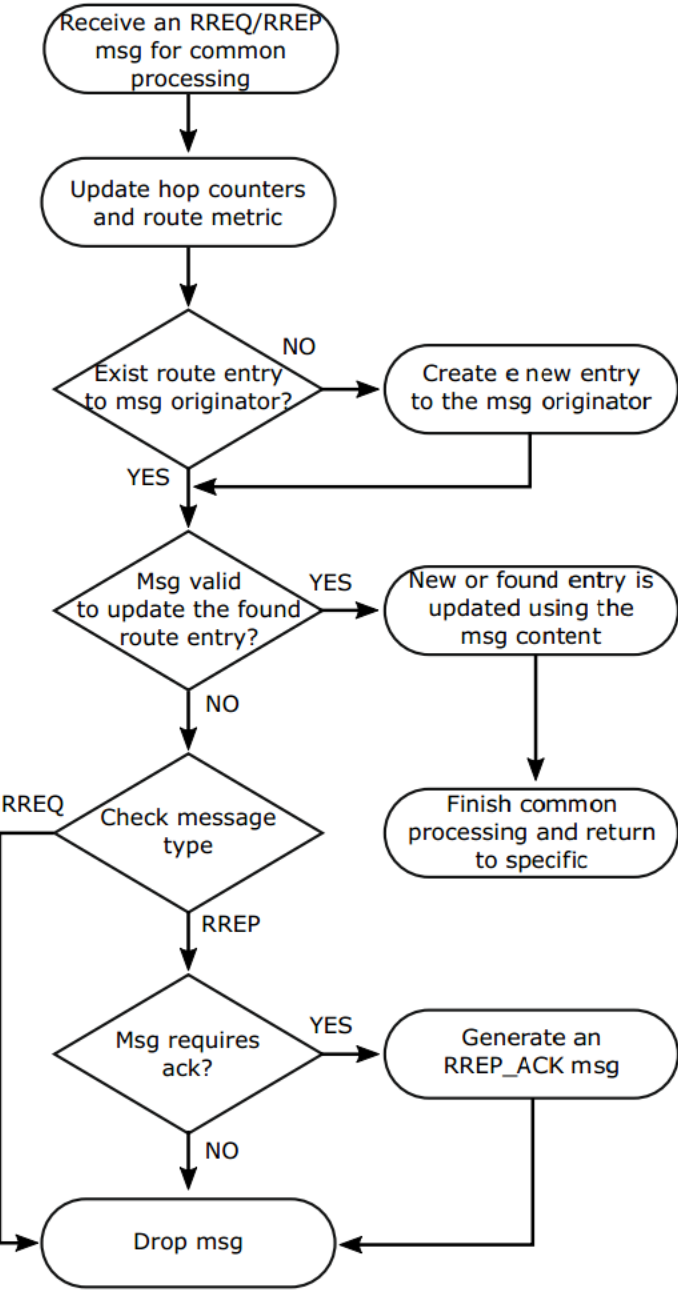


Figure 3.3: Common Message processing [55]

The message, if considered valid, is subject to common processing used for both RREQ and Route Reply (RREP) messages in the first verification that checks the length of addresses and their validity. The node should update the hop-count, hop-limit, and route-metric fields from the message in the common processing (presented in the flowchart in Figure 3.3). In sequence, the node should search in its Routing Set for a route entry for the message originator. A new route entry for the message originator is created if the route is not found. The created or discovered route entry is then matched with the received message fields to check whether the message can be used to correct the route entry or not. If the message is correct, the route entry will be changed, the typical processing will be done, and the message will return to its particular processing. If, on the other hand, the message is not used to change the route entry, the node can check the message form, send RREP-ACK if possible, and remove the message if necessary. When the message returns to a particular RREQ processor, the node can validate that it is the destination of the message. If negative, the node can verify that the message is legitimate for forwarding (check the hop-count and hop-limit), change its fields, and forward the message via broadcast. Otherwise, if the node is the RREQ destination, an RREP message should be generated to respond to the request from the originator of the RREQ.

### 3.3. Metric Evaluation

A routing metric is a quantity or a value that specifies the reliability level of the route between a given source and a given destination [98]. The routing protocol follows a series of rules or calculations to decide the appropriate path to provide the optimum path from one source to one destination on a network. These measures are referred to as metrics for routing [98]. Routing metrics collect different kinds of information about the consistency of the route between the source and destination nodes.

In order to function effectively, a routing protocol needs to comply with three properties, according to Yalling et al.[98]. Below are these properties presented:

1. **Consistency:** For path  $p(S, D)$  where  $S$  is the source and  $D$  is the destination, if data is transmitted between  $S$  and  $D$  across intermediate nodes in order,  $R_i (S, R_1, R_2, \dots, R_n, D)$  a routing protocol is compatible.

2. **Optimality:** If it chooses the lightest path (according to the metric type used) between any pair of nodes, a routing protocol is considered optimal. We evaluate this point by implementing a case study network where the links can be fitted with random metric values and the routing protocol operation can be observed accordingly.
3. **Loop-Freeness:** A routing protocol is loop-free if it does not create a packet forward loop.

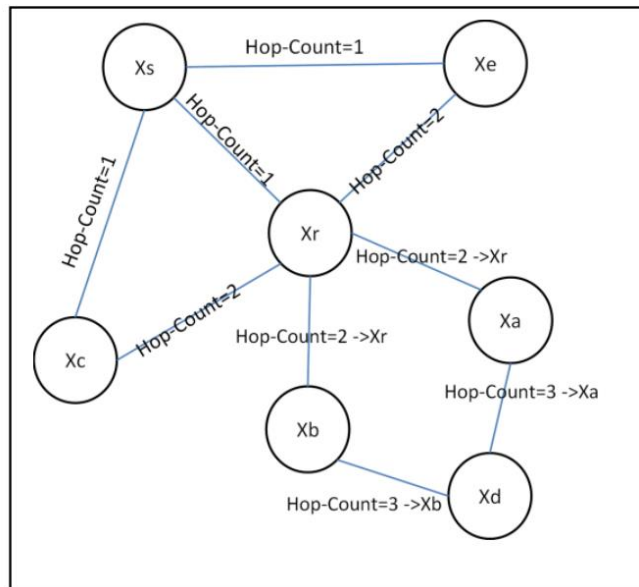


Figure 3.4: Evaluation metric [60]

**Consistency:** M2M-IoT operation based on hop-count metric shall create these links (see Figure 3.4),

- Forward links:  $Xs \rightarrow Xr \rightarrow Xa \parallel Xb \rightarrow Xd$ .
- Reverse links:  $Xd \rightarrow Xa \parallel Xb \rightarrow Xr \rightarrow Xs$ .

A consistency issue rises as the data forwarding links and reverse links such as  $Xr \rightarrow Xd$  and  $Xd \rightarrow Xr$  have the same load.

**Optimality:** The lightest path according to the hop-count metric used is selected by M2M-IoT.

**Loop-Freeness** M2M-IoT is generally loop-free because a sequence number is applied by the protocol. Mechanism that prevents the use of stale routes and answers to the same source of the message request (whether the source or destination nodes and route request or route reply messages).



A pseudo code in Figure 3.5 can be used to model the operation of the route selection by M2M-IoT operation using the hop-count metric. Assuming that the network converged; that is, for all the nodes in the network, the list of neighbors is established. Node Xs is the node of interest that has information to be forwarded as the destination to Node Xd. Xs broadcasts a Route Request Message (RREQ) in this scenario, which has the sequence number information and the hop counter to the neighbor nodes (Figure 3.5 (line 1-4)). The RREQ is an investigation to verify whether the neighboring nodes have a valid route to the Xdd destination (Figure 3.4). The adjacent Xc, Xe and Xr nodes search their routing tables to verify whether the path to Xd is correct (Figure 3.5 (line 5-12)). They will forward the RREQ to their nearest neighbors if the nodes do not have a valid path. The final stage is represented by Xd receiving the RREQ (Figure 3.5 (line 5-12)) and using a Path Return Message (RREP) to reply to Xd receiving the RREQ (Figure 3.5 (line 13-16)). The RREP message is forwarded back to node Xs by the intermediate node Xr (Figure 3.5 (line 17-24)). Xr can deal with the received RREP message and change its routing table accordingly. RREP messages from Xc, Xe and Xr are then received by Xs. The route with the least hop-count measured is chosen according to the number of hops counted through the RREQ and RREP flooding method and a relation is formed between Xs and Xd (Figure 3.5 (line 17-24)). The attached sequence number in the plotted scenario is replaced with the same number as Xs begins broadcasting RREQ messages. It selects the least hop-count determined path at the end of the flooding process and Xs receives the RREP messages from the neighbors.

```

Line1: //Broadcasting RREQ messages
Line2: SendRREQ (nodeX)
Line3: {SET Sqn#_rq =1, Hop_count_rq = 0
Line4: BROADCAST RREQ to Neighbors}
Line5: //Function for handling RREQ messages
Line6: ReceiverRREQ (RREQ, nodeX){
Line7: IF (nodeX == Destination) UPDATE Route, SendRREP (nodeX, RREQ)
Line8: ELSE IF (nodeX != Destination){
Line9:   IF   (Seq#_rq  >  Seq#_tb)   OR   ((Seq#_rq==Seq#_tb)   AND
(Hop_Count_rq<Hop_Count_tb))
Line10: UPDATE, FORWARD RREQ
Line11:   ELSE   FORWARD   RREQ,   UPDATE   RREQ:   Seq#_tb=Seq#_rq,
Hop_Count_tb=Hop_Count_rq +1}
Line12: UPDATE Route, Seq#_tb = Seq#_rq, Hop_Count_tb= Hop_Count_rq}
Line13: //Broadcasting RREP messages
Line14: SendRREP (nodeX, RREQ)
Line15: {SET Sqn#_rp = Seq#_rq, Hop_count_rp = 0
Line16: BROADCAST RREP to Neighbors}
Line17: //Function for handling RREP messages
Line18: ReceiverRREP (RREP, nodeX)
Line19: {IF (nodeX == Source) UPDATE Route, DATA
Line20:   IF (node X != Destination) {
Line21:   IF   (Seq#_rp  >  Seq#_tb)   OR   ((Seq#_rp  ==  Seq#_tb)   AND
(Hop_Count_rp < Hop_
Line22: Count_tb) UPDATE, FORWARD RREP
Line23: ELSE FORWARD RREP, UPDATE RREP: Seq#_tb = Seq#_rp, Hop_Count_tb
= Hop_Count_rq +1}

```

Figure 3.5: M2M-IoT protocol algorithm [61]

### 3.4. M2M-IoT Algorithms

These are the algorithms used in the real machine-to-machine communication implementation test since they are probably time- and energy-efficient.

A M2M-IoT router must first verify whether the request is invalid for processing while receiving an RREQ or RREP packet. The RREQ/RREP obtained is invalid for processing and must be discarded under certain conditions defined in the 3.1 algorithm. A message is deleted if the message

- The RREQ/RREP packet loops back to the originator
- The metric used is not by hop count
- The required packet length is absent
- The route is blacklisted

---

**Algorithm 3.1 Identifying invalid RREQ and RREP Messages**

---

```

1: procedure isValidMessage(M2M-IoT_packet)
2:   if <originator> contains an address of this router then
3:     return false
4:   end if
5:   repeat for each Routing Tuple
6:     Read Routing Tuple in the Routing Set
7:     until R_dest_addr = <originator> and R_seq_num > <seq-
      num>
8:     if matching Routing Tuple found then
9:       return false
10:    end if
11:    if <metrics> ≠ interface metrics then
12:      return false
13:    end if
14:    if some Type Length Values required by the metric are absent then
15:      return false
16:    end if
17:    if <type> = RREQ_TYPE and previous-hop is blacklisted then
18:      return false
19:    end if . additional reasons for identifying invalid packet can be added
20:    return true
21: end procedure

```

---

Table 3-1: Identifying valid RREQ and RREP Messages [73]

On receiving a RREQ message, a M2M-IoT router must process the message according to algorithm 3.2.

---

Algorithm 3.2 RREQ Processing algorithm

---

```

1: procedure Process_RREQ (M2M-IoT_packet)
2:   if isValidMessage(M2M-IoT_packet) = false then
3:     return false           ▷ message discarded without further processing for forwarding
4:   elseif CommonProcess_RREQ_or_RREP(M2M-IoT_packet) = false then
5:     return false
6:   end if
7:   if <destination> ≠ an address of this router then
8:     return true           ▷ message considered for forwarding
9:   else
10:    Generate_RREP(M2M-IoT_packet)
11:    return false
12:  end if
13: end procedure

```

---

Table 3-2: RREQ Processing algorithm

When the RREQ reaches its destination, an RREP is generated. This is considered by the Generate RREP feature: in response to the M2M-IoT packet, an RREP is generated according to algorithm 3.3 and then unicast along the reverse path to the next hop towards the RREQ originator.

---

Algorithm 3.3 RREP Processing algorithm

---

```

1: procedure Process_RREP(M2M-IoT_packet)
2:   if isValidMessage(RREP)= false then
3:     return false   ▷ message discarded without further processing
                     ▷ message not considered for forwarding
4:   else if CommonProcess_RREQ_or_RREP(M2M-IoT_packet)= false then
5:     return false
6:   end if
7:   if ACK-REQUIRED flag = 1 then
8:     Send_RREP_ACK(M2M-IoT_packet)           ▷ send RREP_ACK to the previous-hop
9:   end if
10:  if <destination> ≠ an address of this router then
11:    return true   ▷ message considered for forwarding
12:  end if
13: end procedure

```

---

Table 3-3:RREP Processing algorithm

The CheckPending feature tests if a related RREP is pending, i.e., if a tuple (P next hop, P originator, P seq num, P ack timeout) is included in the Pending Acknowledgment Collection, such as:

- P next hop is the address of the adjacent M2M-IoT router that received the RREP-ACK from the destination;
- P originator applies to the RREP-ACKK field <originator>.

Algorithm 3.4 below shows the mechanism used to handle the errors occurred while forwarding route requests.

---

Algorithm 3.4 RERR Processing algorithm

---

```

1: procedure Process_RERR(M2M-IoT_packet)
2: Process_TypeLengthValues(M2M-IoT_packet)
3:   repeat                                     ▷ for each Routing Tuple
4:     Read Routing Tuple in the Routing Set
5:   until
6:     R_dest_addr = <destination> and R_next_addr = previous-hop
7: if no matching Routing Tuple found then
8:     . RERR not processed further, and not considered for forwarding
9:     return false
10: else if matching Routing Tuple found then
11:     . update this matching Routing Tuple
12:     R_valid_time ← expired
13:     return true                               ▷. Consider the RERR for forwarding
14: end if
15: end procedure

```

---

Table 3-4: RERR Processing algorithm

On receiving a RREP-ACK from a M2M-IoT neighbor router, a M2M-IoT router should run the algorithm 3.5, in which it updates its routing set if necessary.

---

**Algorithm 3.5 RREP–ACK Processing algorithm**

---

```
1: procedure Process_RREP–ACK(M2M-IoT_packet)
2:   Process_TypeLengthValues(M2M-IoT_packet)
3:   CheckPending(neighbor,originator,seq-num)
4:   if matching Tuple is found then
5:     discard the tuple
6:   end if
7: end procedure
```

---

Table 3-5:RREP–ACK Processing algorithm

### 3.5. Smart Route request Enhancement

The SmartRREQ [99] improvement was proposed for M2M-IoT in order to reduce the amount of control messages exchanged during the route discovery process. The node can launch the route discovery process by using SmartRREQ with an RREQ containing a new smart-route request flag set to be valid. In RREQ message handling, each node that receives a SmartRREQ (RREQ message with smart-route request true) can perform additional processing. The node can conduct the basic processing of SmartRREQ after performing all the initial processing, and after checking if the message is correct for forwarding. The node then tests if it owns a path entry that is distinct from the previous hop of the obtained SmartRREQ on its Routing Collection to the next hop message destination. If this criterion is fulfilled, the unicast SmartRREQ message should be transmitted by the node to the next address identified. Before the message hits the final destination, the next hop receiving the SmartRREQ message can perform the same processing. If the route entry for the SmartRREQ destination is not identified by a node, the message should be forwarded via broadcast. A SmartRREQ's destination should respond to the request by generating a normal RREP. The SmartRREQ enhancement will also minimize the number of transmitted broadcasts, thus reducing the overhead control message needed to find a new route and reducing the energy usage of the network.

### 3.6. Route Cache for M2M-IoT

A method to store the recently used destination addresses for function use is used by M2M-IoT. These addresses, stored as The Routing Collection in the memory grab, are composed of

entries of route tuples that store neighbor node data. A node may check the presence of a path to a destination or the need to start a new route discovery process, depending on the routing collection. Both route entries in the routing set may be deleted in the process of network service until the valid time expires. This method helps nodes to decrease the use of memory and to make it easier to build pathways to other nodes. In the M2M-IoT, the valid time of the standard routes should be changed to the planned network traffic.

The entire route exploration process can be done all over again anytime a node wants to send a new message to a different node in the network, sending multiple control messages and expending more network energy. M2M-IoT includes an optional upgrade to reduce the control message overhead during the construction of new routes to reduce this issue. The most important information about the last path entries deleted from the routing collection is stored by this method, Route Cache for M2M-IoT (RCMI, hereafter). The node can then search its RCMI to verify the presence of a previously known path when it is required to conduct a route discovery. If positive, the node will lead the exploration of the path to the destination of the entry contained in the RCMI.

Owing to a legitimate expiration period or loss of memory for the insertion of a new entry, an entry may be deleted from the routing set. Thus, by using the RCMI, a new path cache entry that is inserted in the RCMI set is generated using its next hop address and destination address. The number of route cache entries should be specified earlier and the memory cap of the nodes should be taken into account. For every four possible entries in the routing table, the authors recommend that this number be raised by one. Thus, the number of RCMI entries should be one if the size of the routing table is four; if the size of the routing table is eight, the number of RCMI entries should be two. It is also possible to consider reducing the number of routing entries in order to allow the use of the RCMI in devices with extreme memory constraints.

RCMI entries are not legitimate and can only be deleted after sending an RERR message (discussed in section 3.6). Similar to the number of route entries specified in the RCMI, when a new entry needs to be added, the oldest entries are deleted. Furthermore, in the package, the quest for an RCMI entry should always get the most recent entry. Therefore, the RCMI set should function like a stack, where a new entry must be added at the beginning of the set, and the list head

should always be returned until the entry is found. If the collection is complete, the node should delete the last item in the list and insert a new entry at the start of the list.

Before beginning a new route discovery process, the nodes can check their route cache set while using the RCMI. The node can lead the route discovery process to the endpoint of the discovered entry if an entry is identified. The node then produces an M2M-IoT with a destination equal to the destination address identified and transfers the message to the next hop in Unicast. During RREQ processing, the node receiving the RREQ should usually know the message handling, as stated in Figure 3.1, a node that does not have a route should consult its routing collection to verify the presence of some transient route. Please notice that at this stage, as is the case with regular RREQ-IoT processing, it is possible to adjust the destination of the unicasted RREQ and redirect the message to another node with a proper routing package.

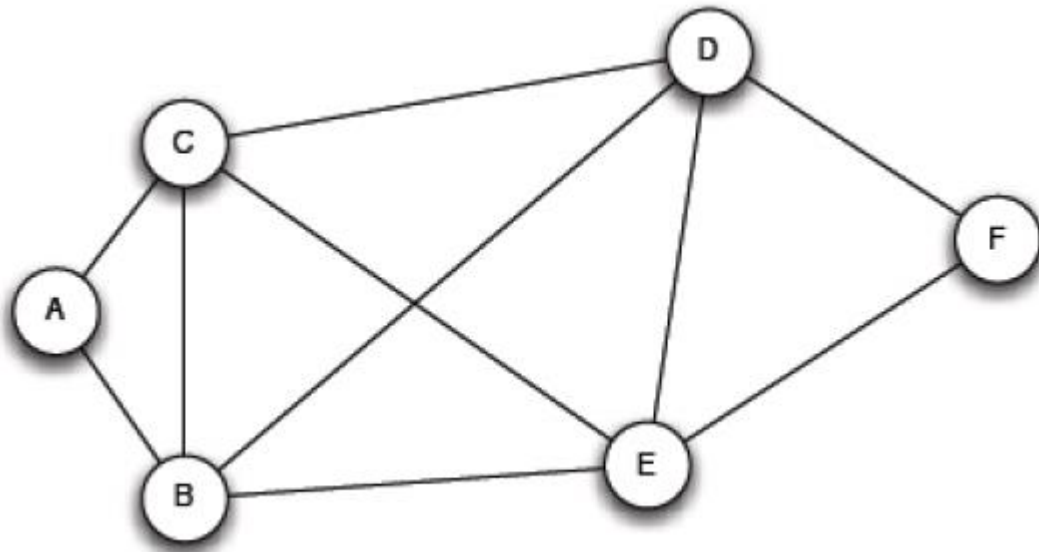


Figure 3.6: M2M-IoT route discovery process [66]

Figure 3.6 exemplifies this condition. Consider that node A needs to send a message and, on its routing, set does not find a route; A tests its RCMI and finds an entry to F via E with the next hop B. Therefore, A produces an RREQ with a destination equal to the address F and unicasts it to node B. (the found next hop to F). B collects the RREQ from A and usually executes its encoding. B, however, discovers a path to node C while testing its routing range. Thus, B updates the destination of RREQ received to C and sends the message in unicast. The request originating from A is then answered by Node C, consulting its routing collection and identifying a path and



forwarding the route to E. This behavior is acknowledged since the object of an RREQ is to achieve a minimum broadcast path, regardless of the node that provides the route. Furthermore, this RREQ redirection ensures that the method of route exploration follows with the most recent knowledge (considering that the information provided by the routing set is frequently newer).

However, if a route is not found in the intermediate node's routing set, the intermediate node should check its RCMI, change the destination of the message (if necessary), and then forward the unicast message to the node found to deliver the RREQ originator request. Finally, the node can update the destination address of the RREQ to the same address as its originator, if the RCMI set is zero, and submit the message during the broadcast. This approach "converts" the RREQ obtained in unicast into a standard RREQ to be broadcast and once the desired node is reached, the route discovery process can proceed.

Using the RCMI protocol allows nodes to reduce the amount of control messages needed for a node of interest to be built. The cache function is used to direct the RREQ-IoTs to a destination address previously identified. The RCMI thus aims to reduce the number of packet collisions as implemented, minimizes energy consumption, and increases network performance. As explained, the entries in the RCMI collection are only deleted due to a loss of memory or RERR message receipt.

### 3.7. Lost Error Code for M2M-IoT

The desired nodes will often go out of their neighbor nodes' relation due to unpredictable circumstances. A way of warning the neighbor nodes that the connection has been lost is of great benefit to discourage these neighbor nodes from sending RREQ messages when they have no link to the destination node. The intermediate node can start a new routing discovery process and send the RREQ message to its neighboring nodes if the node detects that the connection has been lost or that the forwarding cannot be realized. If the new route check is unsuccessful, the route error (RRER) message is created by the node, which has the same structure as the usual RERR, the originator as its own node address, and the destination as the originator of the unforwarded RREQ message. The message is then sent to the previous hop of the received RREQ message in unicast.

If the RERR receiver is using the RCMI, it should also check that an RERR originator entry is present on its RCMI set. This procedure prevents the node attempting to begin a new route discovery from using the node with the missing link knowledge. In order, the node verifies if the destination of the message itself is valid. The RERR method is finished, if valid, and the message is not forwarded. Otherwise, the node should verify if the message is eligible for forwarding, the message fields should be changed, and the message should be sent to its destination. An intermediate node in the path to the destination of a message may also produce an RERR message.

In order to find a new path, an intermediate node that receives an RREQ message and detects that the message destination has no active route should launch a new route discovery process. If the route is not created successfully, the RERR message is generated by the originator of the message. Using the suggested error message, the network will decrease the number of request routing messages sent to a node without a legitimate route. Thus, when they receive an RERR post, the nodes are able to search alternate routes. As a gain, it is possible to reduce the amount of packets dropped, which helps to increase network performance and stability.

# CHAPTER FOUR

## DEMONSTRATION

### 4.1. Simulation and Result

It is possible to define simulation as impersonating or analyzing how instances will arise in a genuine situation [100]. It can be worried about complicated numerical showing, pretending without the creativity guide, or mixing. The appreciation lies in placing you under fair circumstances, and then affects the actions of others so that you do not anticipate the arrangement of occasions or the final outcome [101].

### 4.2. Contiki OS Files system

This section shows the filesystem hierarchy of the rime stack and the location of the modules modified.

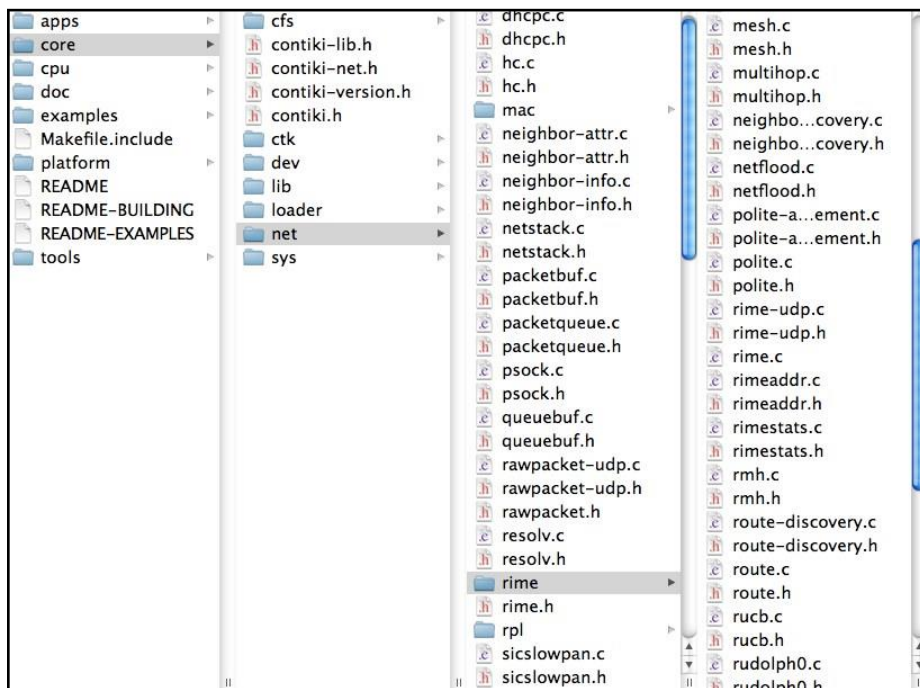


Figure 4.1: Contiki filesystem hierarchy [99]

- **Core:** The core/folder includes the Contiki kernel source files.

- **Net:** The network/folder includes source files related to network communication, such as the medium access techniques in the mac/folder, the Rime stack in the rime/folder or the RPL implementation of ContikiRPL in the rpl/folder added in Contiki OS version 2.7.
- **Rime:** The root files associated with the rime stack are found in the rime/ folder. It includes, for example, the mesh.h library for the mesh module, the path.h library for the route module, and the header for route-discovery.h for the route-discovery module.

### 4.3. M2M-IoT Observations

The basic operations of M2M-IoT as a reactive protocol include the generation of Route Requests (RREQs) by an M2M-IoT Router (originator) when a route to a destination is found. Forwarding of such RREQs until they reach the M2M-IoT Router endpoint, generation of Route Answers (RREPs) by the indicated destination upon receipt of an RREQ, and unicast hop-by-hop the propagation of these RREPs to the originator.

- 1) **Data traffic flow assumption:** M2M-IoT does not presume the type of data traffic used by the protocol, but has a general point-to-point networking system that is similar to the traditional Internet architecture: no one router serves as a relay for all traffic on the Internet. Which is facilitated by the protocol being extensible (in a backward/forward compatible fashion) in order to provide more reliable efficiency when subject to other traffic patterns, such as data collection or broadcasting.
- 2) **No Root - No Requirements:** No router plays some unique function in the M2M-IoT network. The same conduct occurs with all routers (signaling and processing). While there is a logical "root" when using a selection tree extension, the router that serves as the conceptual "root" has no extra signaling or processing criteria when opposed to other routers in the network.
- 3) **Fragmentation:** M2M-IoT uses a generalized message format, specifically built for ad hoc networks [23], to reduce the overhead of routing control messages. It not only reduces the overall size of the control packets created by M2M-IoT, but also enables the creation of protocol extensions. In comparison, a standard M2M-IoT control message size is about 30 bytes (depending on the address length used) by being frugal in the provided details in M2M-IoT control messages, which conveniently fits into a single 802.15.4 frame. M2M-

IoT does not need routing-related information (such as a source routing header, or fields that show the packet's direction) to be applied to the IP header for data traffic. Applications should then build their data traffic correctly and reliably to "fit" within an unfragmented frame.

- 4) **Link Bi-directionality:** In networks where unidirectional connections exist, M2M-IoT is designed to operate. A bi-directionality search is carried out using the "blacklist" in the core M2M-IoT specification. When a Route Reply message is received by an M2M-IoT router, a Route Reply Recognition message is required by default. If the acknowledgment is not obtained on time, this Route Reply's "next hop" is blacklisted, and in a subsequent route discovery process it is not expected to enter the route. When doing so, only bi-directional connections are used in M2M-IoT to forward data packets.
- 5) **Loops:** The M2M-IoT routing messages such as Route Request and Route Reply generated by a given M2M-IoT Router share a single unique sequence number that is monotonically increasing. Meanwhile, a Route Request is only allowed to respond to a destination, which guarantees loop independence.

#### 4.4. Module

M2M-IoT implementation modifies two modules of Contiki: the route module, and the route-discovery module.

#### 4.5. Descriptions of the simulation

Several simulations were conducted with the COOJA simulator to test the general behavior of M2M-IoT as a Contiki routing protocol for IoT/WSN. In a WSN setting, these simulations test point-to-point (machine to machine) communications.

Between each attempt to send a data packet, the root node waits for an interlude. This interlude period is set to be sufficiently long to:

1. Ensure there are not packets – Either data packets or M2M-IoT packets from past network propagating operations. The reason is to prevent collisions that can lead to ideal paths not being identified.

2. Ensure that all current routes in the routing table of each node expire. The explanation is that all phases of route exploration are initiated under the same initial conditions.

The former conditions are satisfied by setting an interlude time longer than the convergence time of the network (for item 1) and by setting an interlude time greater than the convergence time plus the expiration time of the path (for item 2). The protocol for sending a data packet is as follows: the M2M-IoT path discovery procedure is called to receive the requested route while the root node begins to send a new data packet. Each leaf node sends the recognition data packet back to the root node after the data packet has been sent. The reverse route is mounted during the M2M-IoT route discovery procedure, so the destination leaf node does not need to find a new connection to the root node.

#### 4.5.1. Scenarios

In a flat area, sensor nodes are deployed and placed uniformly, as seen in Figure 4.2 In the simulation architecture, some limitations are needed in the communication of nodes:

- **Transmitting Range:** A transmitting node can only reach its nearest neighbors (in figure 4.2, to its four nearest neighbors).
- **Interference Range:** Interferences might affect, at most, to the two-hop away neighbors (in figure 4.2, the eight nearest neighbors) of a transmitting node, and should not affect to further nodes.

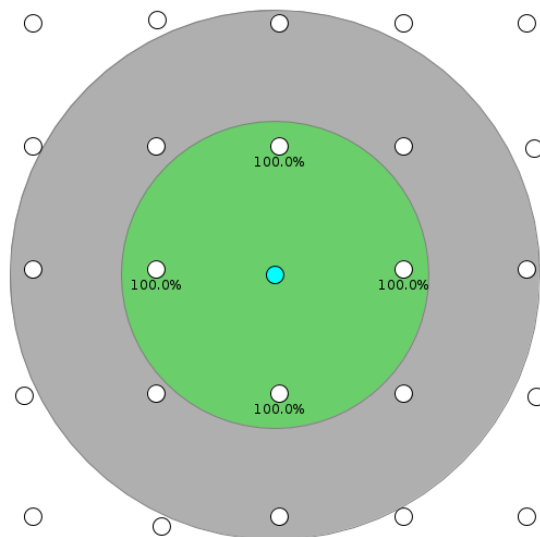


Figure 4.2: Transmitting and Interference ranges in COOJA simulation scenario

Simulation scenarios and parameters (as seen in Table 4-1) consist of a uniformly distributed set of nodes with a density of 4 nodes per  $(100m)^2$  in a flat grid area. The minimum distance between nodes is set at 50 meters, while the range of transmission is 55 meters. The radio medium chosen is UDGM, with an optimal transmitting and reception success ratio. The UDGM model still indicates loss at reception when interruption occurs. This is a conservative paradigm, since not all intervention means lack of reception in reality. It is possible to balance this effect by selecting narrower interference ranges. Usually, it is believed that the interfering frequency is two times the propagation range. In these simulations, though, this range is set to 1.7 times the transmission range (i.e., 85 meters). The model turned out to be more practical when doing this; the adopted interference range encompasses 4 nodes rather than 8 nodes that would be influenced by picking the wider interference range.

Parameter	Value
Simulator	COOJA
Radio medium	UDGM
Grid size	variable
Density of nodes	Constant 4 nodes/ $(100m)^2$
Number of nodes	25, 113
Node separation	50m
Transmitting range	55m
Interference range	85m
Success ratio tx / rx	1.0 / 1.0

Table 4-1: COOJA simulation parameters

#### 4.5.2. Platforms

In this analysis, several sensor node platforms such as Tmote Sky and MicazZ were used to run simulations.

Tmote Sky is a mote-based network with a wide range of sensors. With a 16-bit RISC cpu, it produces the Texas Instruments TI MSP430 F1611 microcontroller. To connect with the cost

device, it uses a USB controller and features the IEEE 802.15.4 compatible Chipcon CC2420 radio. A pseudo-omni directional antenna with a coverage of up to 50 meters indoors and up to 125 meters outdoors is the internal Inverted-F microstrip antenna.

Centered on the Atmel ATmega128L, the MicaZ platform produces an MPR2400 processor module. The 51-pin expansion connector supports Analog Inputs, Optical I/O, I2C, SPI and UART interfaces and can be fitted with various sensors. For both programming and data transmission, it uses a serial/USB interface. Its RF transceiver complies with IEEE 802.15.4; a dipole antenna reaches a length of up to 30 meters indoors and up to 100 meters outdoors.

Instead of the regular AODV routing protocol, sensor nodes are expected to operate a changed Contiki operating system where the routing protocol has been replaced by M2M-IoT.

For contact between nodes, the Rime stack has been used. Specifically, with the mesh network, the virtual nodes transmit packets that use multi-hop connectivity through the multi-hop module. The data packet sent by the root node comprises a 100-byte payload. The payload for data acknowledgement has 11 bytes.

A summary of the Contiki configuration is shown in Table 4.2.

Parameter	Value
Platform	Tmote Sky, MicaZ
Contiki	version 2.7
Transport protocol	Rime mesh
Data packet	100 bytes
Data ACK packet	11 bytes

Table 4-2:Contiki parameters in simulated sensor nodes

The M2M-IoT parameters were set in line with Table 4.3. Net traversal time has been detected to be below 2 seconds in these simulations. Path lifetime has been set more than two times the net traversal time to prevent loops in RREQ flooding. The time for direct link contact was less than 50 ms, so the RREP-ACK timeout was set to 100ms. In compliance with a hop-count metric, the best routes are picked. The method of route exploration is attempted once for each desired route.



The explanation is that the likelihood of success (and other statistics) remains stable with each attempt, such that the probability of success (and other statistics) can be derived from the outcomes of these experiments for more than one attempt.

In all the simulations, hop-count metrics are used. This is a strong metric for use in models to measure the optimality of the routes encountered, but it is not the most common applicable metric for actual applications.

M2M-progress IoT's in finding the best routes to eliminate collisions in the propagation of RREQ broadcast. For that function, prior to RREQ broadcast broadcasts, a uniformly distributed jitter time was set until. Some experiments have shown that a jitter time between 0 and 200 ms improves the success rate and the optimality of the routes found in this type of topology, whereas the number of re-attempts to find a route decrease.

Parameter	Value
Number of retries	1 attempt
Metrics	0 (hop-count)
Route lifetime	5 seconds
Net traversal time	2 seconds
Blacklist time	10 seconds
Backoff	0–200 ms (uniform)
ACK-REQUIRED	Yes
RREP-ACK timeout	100 ms

Table 4-3: M2M-IoT parameters in simulated sensor nodes

## 4.6. Demonstration and Evaluation

### 4.6.1. M2M-IoT module installation

The following files must be changed in order to overwrite the Contiki OS Rime routing protocol, which is AODV, with M2M-IoT:

- **route.h:** It is the router's heart. A path module includes and manages its routes in the routing table.

- **route.c:** This is a module containing the features defined in the route.h module. This is the spot where the routing is handled. This functionality finds the lowest cost (i.e., minimal hop) path to forward a post.
- **route-discovery.h & route-discovery.c:** Used by the router, the route-discovery module offers a method to explore new paths. The source code for the route-discover header and route-discovery file modules will be changed to replace the M2M-IoT protocol with the AODV protocol.
- **mesh.c:** The mesh module is responsible for the multi-hop routing of packets through the multi-hop module.

## 4.7. Evaluation

The performance evaluation carried out to determine the actions of the suggested approach is discussed in this section. For this reason, a COOJA simulator/emulator was used, which is part of the Contiki O.S. While the use of computer simulations cannot accurately reflect the behavior of a network in the real world, it does allow for a reasonable comparison between routing protocols, since it makes it possible for all the proposals examined to replicate an identical environment [102]. Furthermore, since it acts as an emulation, COOJA enables individual nodes such as Tmote Sky, MicaZ, and others to simulate the hardware conditions. Thus, in terms of memory consumption and processing power, each emulated node reflects the same hardware conditions of real devices.

### 4.7.1. Testing procedure

There are two sets of tests available [103]; the first test is called the tuning test and the second test is the test of contrast. The tuning test is a method of checking the parameters of a given routing protocol in which the object of comparison testing is to compare the performance of two (or more) different routing protocols. Hence, a distinction is made to determine the efficiency of two routing protocols in this report. The same traffic models and patterns are used for various simulation environment.

The M2M-IoT suggested was contrasted with the RPL variant of Contiki. In various situations, the aim was to evaluate the action of the proposed solution with RPL. Thus, with two

topology organizations, circumstances were developed: grid sparse and random dense. The number of nodes in the network changed from 25 to 100 for all the topologies. This quantity was selected because it can reflect much of the latest small-scale IoT implementation scenarios (25 nodes), especially in smart homes and in business scenarios on a broad scale (100 nodes). More material on the used grid and random topologies is provided in the accompanying itemization.

- **Grid Sparse Scenarios:** The network nodes were arranged in a  $n \times n$  node linear grid. Along with the number of nodes, the simulation area expanded. A fixed network density was then maintained where the nodes had two to four neighbors.
- **Random Dense Scenarios:** The numerous amounts of nodes were uniformly deployed only once in an area of 100 square meters. Thus, the random deployments for all comparative plan is the same. For the varying amounts of nodes, the virtual field was the same. The network density has also risen with the growth in the number of nodes.

The simulation time was 600s for both scenarios and the varying amounts of nodes. Both network nodes in the program produce and transmit data messages at variable intervals of between 10 and 15s. To prevent the nodes from being overwhelmed with many data messages while still realizing a route discovery process, the minimum data message interval was specified as 10. This measure was necessary because the nodes do not enforce a large buffer for data messages in the routing layer. All data messages produced within the phase of route discovery are therefore lost.

#### 4.7.2. Packet Delivery Ratio

The PDR statistic reflects the amount of data messages sent to the destination node successfully. A high PDR thus represents an effective network that can provide highly accurate data messages created with high reliability. The consistency of the connections between nodes, the radio interference caused by neighboring machines, and collisions with other data and control messages are continuously influenced by this metric. The network PDR value was obtained in accordance with Equation [28]:

$$PDR = \frac{\sum_{i=1}^N Pr_i}{\sum_{i=1}^N Ps_i}$$

Where  $N$  is the number of network nodes,  $P_{ri}$  is the number of received data packets for each  $i$ -node, and  $P_{si}$  is the number of submitted data packets for each  $i$ -node. Therefore, the following figures indicate the PDR determined for the proposed routing protocol (M2M-IoT) and the current routing protocol (see Figure 4.5 and Figure 4.6) (P2P-RPL).

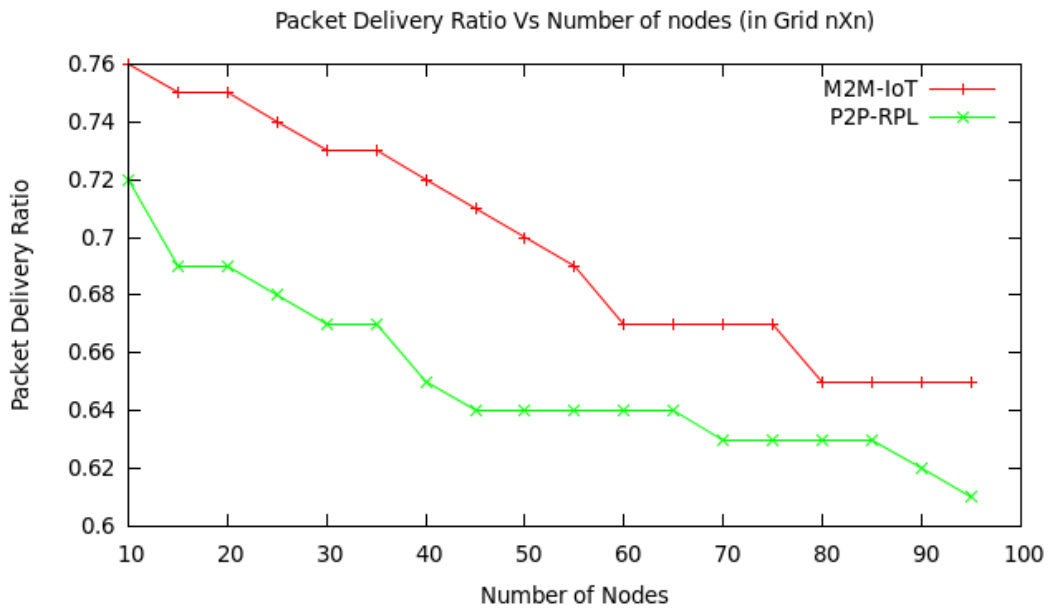


Figure 4.3: Packet Delivery Ratio for grid deployment of nodes

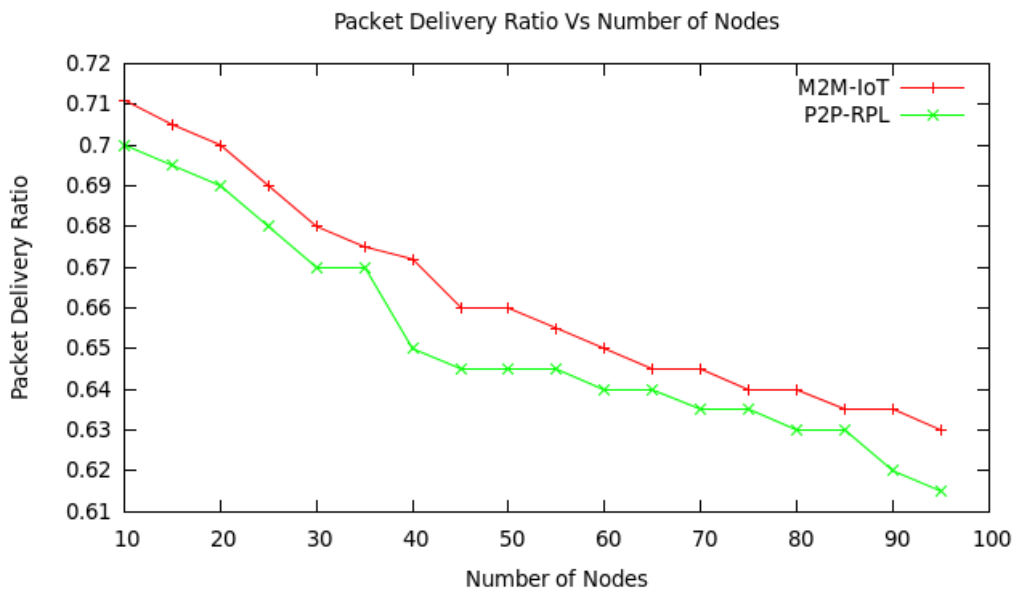


Figure 4.4: Packet Delivery Ratio for random dense deployment of nodes

### 4.7.3. Average Energy Spent per Delivered Data Bit

The average energy spent per data bit metric supplied reflects the amount of energy spent by the network to send each data bit to its destination successfully. Therefore, the less resources expended efficiently transmitting the data, the greater the network's power consumption. The energy consumption of the nodes and the packet distribution ratio influence the results produced by this metric. The metric is determined by means of equation [104]:

$$AES = \frac{\sum_{i=1}^N Ec_i}{\sum_{i=1}^N Pr_i * M_{length}}$$

$E_{c_i}$  is the total energy absorbed (in millijoules) by each  $i$ -node.  $M_{length}$  is the length of the data message in bits, and  $Pr_i$  is the number of data packets obtained by each node  $I$  where  $N$  is the number of nodes in the network. The following estimates display the energy used in two situations (see Figure 4.7 and Figure 4.8). (Grid sparse and Random dense).

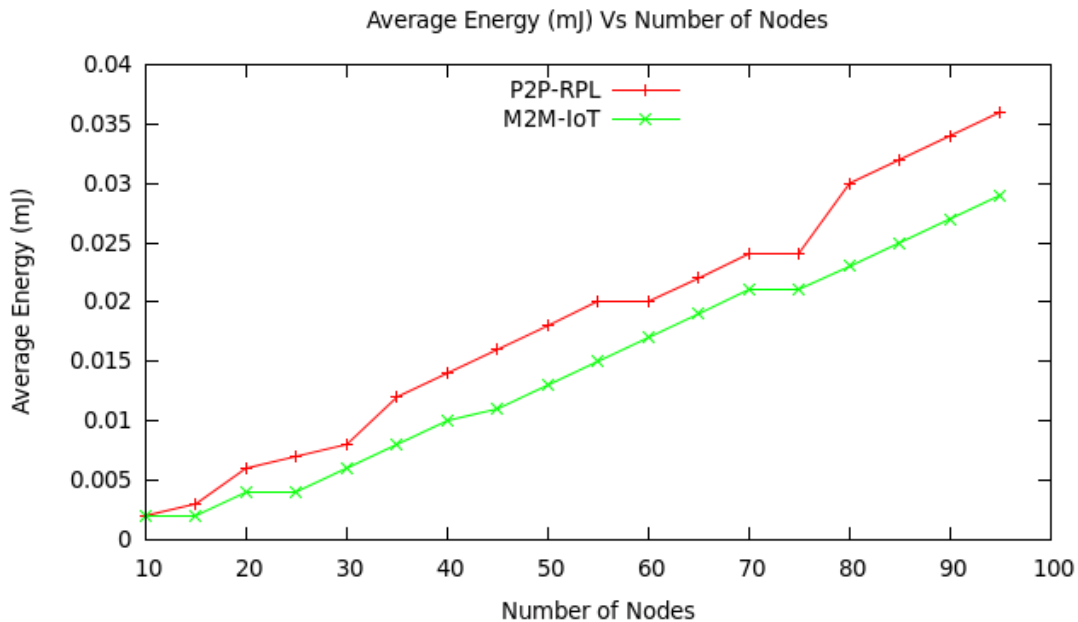


Figure 4.5: Average Energy for Grid Sparce deployment

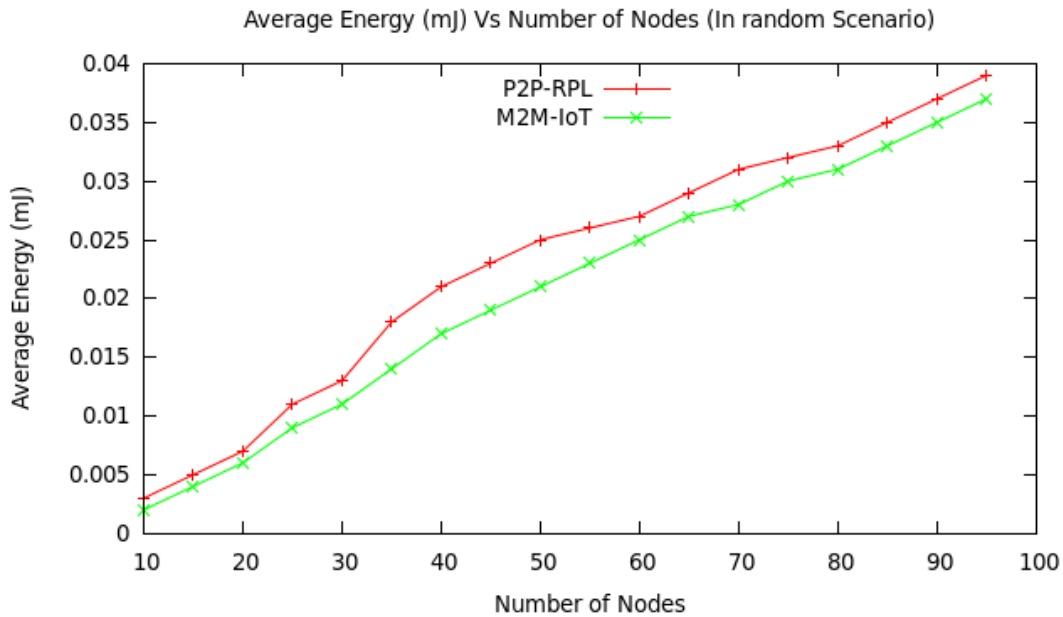


Figure 4.6: Average Energy for Random Dense deployment of nodes

#### 4.8. Discussion of result

M2M-IoT performs better than P2P-RPL, as seen in the preceding figures. To test the efficiency of the nodes, the two scenarios listed were used. M2M-IoT appears to operate well in grid sparse with the best energy utilization and high number of packets delivered.

The suggested solution presented satisfactory results in the grid case, where the network was sparse and the number of adjacent nodes was stable, demonstrating its scalability and achieving a PDR of between 75 percent and 80 percent. In comparison, with the increase in the number of nodes, the P2P-RPL solution reduced its efficiency. The justification for this action was the dependence on a set root node to deliver the messages.

In the grid case, the suggested solution is also able to provide an output of 73 percent better as compared to P2P-RPL in energy usage with 100 nodes. The reduction in the number of control messages used in the route discovery process usually allowed the proposed protocol to use less radio transmissions, resulting in a decrease in energy consumption. The enhanced route discovery mechanism for nodes also helped the protocol to find closer destinations for the messages to be forwarded. Therefore, fewer transmissions were needed for data messages sent to the destination nodes, leading to a reduction in energy usage. Less transmitting therefore ensures that packet

leakage caused by radio interference or packet collisions is less possible. M2M-IoT was thus able to expend less energy to transmit each data bit by reducing energy consumption and achieving a high packet distribution ratio, exposing a high-power performance relative to P2P-RPL.

It is worth noting that, as the network size increases from 25 to 100, the proposed model shows poorer efficiency in terms of energy used and packet distribution ratio from the simulation outcome. This is attributable to the reactive mechanism's inheritable existence as a single and standalone guideline. However, as the route to the destination nodes is known, without depending on the DODAG core, the source node can easily disseminate the packet to the intended node. Thus, the reactive routing protocol lets the proposed approach demonstrate improved efficiency in terms of performance metrics listed above.

# **CHAPTER FIVE**

## **CONCLUSION AND FUTURE WORK**

### **5.1. Conclusion**

In recent years, numerous research papers have been published on the development of road and energy-efficient protocols. The fact that computational constraints have been placed on restricted IoT and WSN nodes has led to creative algorithms that can satisfy the requirements of these systems. These nodes are mainly used for multiple sensing and transmission purposes of the sensed data to the central sink. Efforts are also being made to instigate appropriate routing protocols by the scientific community and well-known technology companies.

This work is devoted to contributing to modern routing protocol approaches. The new and default routing protocol in Contiki OS, AODV, is modified by this protocol, M2M-IoT, to replace the low power and lossy network RPL routing protocol. M2M-IoT is solely concerned with addressing the routing issues found in the IoT environment's machine-to-machine communication (M2M-IoT).

### **5.2. Contribution of the study**

This research has attempted to change the paradigm of seeing the RPL routing protocol as the only savior for machine-to-machine communication in the IoT world. The authors made it clear that in point-to-point communication, a reactive routing approach can be used, resulting in improved latency efficiency, packet distribution and energy minimization.

### **5.3. Future work**

To verify M2M-IoT performance, as well as to run M2M-IoT in a real application over a significant period of time to analyze effects, some tests in real testbed are required.

RPL is designed for use in communications between P2MP (Point to Multipoint), MP2P (Multipoint to Point) and P2P (Point to Point). In MP2P and P2P communications, researchers have found that RPL has output gaps. Researchers are now trying to develop much improved MP2P and P2P routing protocols to date.



As stated in section 2.4.4, congestion detection and mitigation approaches are still absent from the RPL. Therefore, RPL calls for networks to monitor congestion to facilitate the routing of LLNs effectively. While one approach to mitigate congestion is to change work-load speeds, it improves latency. Another option is to re-direct traffic where it is discovered that every node in the route is congested. In specific, the congestion conditions at other nodes should also be observed before re-routing traffic. In addition, when developing congestion detection systems, the connection failure rate needs to be addressed. Routing decisions in the RPL can then be taken by taking into account the degree of congestion of the proceeding nodes, which is determined according to network availability and dynamics.

RPL endorses optional secrecy and honesty of communications. However, because of the weakness of the construction and data distribution process, RPL is still subject to attacks. In addition, due to the RPL's self-organized function, errors will accumulate, leading to serious security problems. In [105] [106] The authors discussed the RPL protection problem and recommended strategies to discourage DODAG version numbers from being inappropriately increased by nodes in order to stop routing loops. Another significant design is to consider protection in the choosing of roads. Due to the lack of protection designs, attackers can easily mimic the process of entering DODAGs in RPL, and drop packets after joining the network. The protection in the RPL can be improved in terms of the objective feature by a reputation-based architecture. More precisely, neighbors are permitted to vote for each other such that a prestige is gained by each node. The highest-reputation node then has a higher priority to be chosen as the next hop. Mobility problems are still part of the work on future.

## 6. References

- [1] M. P. M. G. Emmanuel Baccelli, "The P2P-RPL Routing Protocol for IPv6 Sensor Networks: Testbed Experiments," in *19th International Conference on software, Telecommunication and Computer Networks*, Split, Croatia, 2011.
- [2] Y. S. Y. Y. V. A. M. J. L. K. Sheng Z, "A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities. *IEEE Wireless Communication*," pp. 91-98, 2013.
- [3] K. a. Y. M. Akkaya, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, pp. 325-349, 2005.
- [4] G. A. S. Muhammad O. Farooq, "A Reactive QoS Routing Protocol for MANET," *Ad hoc and Sensor Wireless Networks*, vol. 13, 2011.
- [5] C. E. a. R. E. M. Perkins, "Ad-hoc on-demand distance vector routing," *Mobile Computing Systems and Applications*, , pp. 90-100, 1999.
- [6] R. J. T. X. A. L. TENG GAO, "Energy-Efficient Hierarchical Routing for Wireless Sensor Networks," *Ad hoc and Sensor Wireless Networks*, vol. 11, pp. 35-72, 2011.
- [7] N. K. J. H. a. D. C. G. Montenegro, "Transmission of IPv6 packets over IEEE 802.15.4 networks," in *RFC 4944*, 2007.
- [8] A. T. a. S. D.-H. P. Levis, "Overview of existing routing protocols for low power and lossy networks," 2009.
- [9] C. C. B. T. Leila Ben Saad, "Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: two cases studies," in *SENSORCOMM*, Nice, France, Sep, 2011.
- [10] J. K. D. E. C. a. J. P. Hyung-Sin Kim, "Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey".
- [11] T. W. R. A. e. a. T. Winter, *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*, Internet Engineering Task Force (IETF): Request for Comments: 6550, March 2012, p. 27.
- [12] C. Barriquello, G. Denardin and A. Campos, "A geographic routing approach for IPv6 in large-scale low-power and lossy networks.," *Computer and Electrical Engineering* , vol. 55, pp. 182 - 191, 2015.
- [13] M. Zhao, I. Ho and P. Chong, "An Energy-Efficient Region-Based RPL Routing Protocol for Low-Power and Lossy Networks," in *IEEE Internet Things*, 2016, pp. 1319 - 1333.
- [14] S. Anamalamudi, M. Zhang, A. Sangi, C. Perkins, S. Anand and B. . and Remy, "Asymmetric AODV-P2P-RPL in Low-Power and Lossy Networks (LLNs)," in *draft-ietf-roll-rpl-03*, Fremont, CA, USA, 2018.
- [15] A. G. G. G. & B. W. Alturki, "The design science research roadmap: in progress evaluation," in *PACIS 2013 Proceedings*, 2013.

- [16] K. G. C. a. T. T. Peffers, "Extending critical success factors methodology to facilitate broadly participative information systems planning," *Journal of Management Information Systems* (, vol. 20, no. 1, pp. 51-85., 2003.
- [17] [Online]. Available: <https://iotbyhvm.ooo/contiki-the-open-source-os-for-iot/> . [Accessed 2 December 2020].
- [18] [Online]. Available: <https://www.igi-global.com/dictionary/cooja-simulator/50486> Accessed 2, 2020. [Accessed December 2020].
- [19] T. Mehmood, "COOJA Network Simulator: Exploring the Infinite Possible Ways to Compute the Performance Metrics of IOT Based Smart Devices to Understand the Working of IOT Based Compression & Routing Protocols".
- [20] S. Uma maheswari and A. Negi, "Internet of Things and RPL routing protocol: A study and evaluation.," in *Inproceeding of the 2017 International Confereance on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, , 5–7 January 2017..
- [21] M. Miguel, E. Jamhour, M. Pellenz and M. Penna, "A Power Planning Algorithm Based on RPL for AMI Wireless Sensor Networks," *Sensors*, vol. 17, p. 679, 2017.
- [22] J. Park, K. Kim and K. Kim, "An Algorithm for Timely Transmission of Solicitation Messages in RPL for Energy-Efficient Node Mobility," *Sensors*, vol. 17, p. 899, 2017.
- [23] V. Gokilapriya and P. Bhuvaneshwari, "Analysis of RPL routing protocol on topology control mechanism.," in *In Proceedings of the 2017 Fourth International Conference on, Signal Processing, Communication and Networking (ICSCN)*, Chennai, India, , 16–18 March 2017.
- [24] A. Alomari, W. Phillips, N. Aslam and F. Comeau, "Dynamic Fuzzy-Logic Based Path Planning for Mobility-Assisted Localization in Wireless Sensor Networks," in *Sensors*, 2017.
- [25] N. Pradeska, W. Widyawan, W. Najib and S. Kusumawardani, "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)*, Yogyakarta, Indonesia, 5–6 October 2016.
- [26] N. Shakya, M. Mani and N. Crespi, "SEEOF: Smart energy efficient objective function: Adapting RPL objective function to enable an IPv6 meshed topology solution for battery operated smart meters," in *In Proceedings of the 2017 Global Internet of Things Summit (GIoTS)*, Geneva, Switzerland, 6–9 June 2017.
- [27] N. Sousa, J. Sobral, J. Rodrigues, R. Rabelo and P. Solic, "ERAOF: A New RPL Protocol Objective Function for Internet of Things Applications.," in *In Proceedings of the 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, Split, Croatia, 12–14 July 2017.
- [28] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutor*, vol. 17, p. 2347–2376, 2015.
- [29] T. Watteyne, T. Winter, D. Barthel and M. Dohler, "Routing Requirements for Urban Low-Power and Lossy Networks," in *RFC 5548; IETF Secretariat*, Fremont, CA, USA, 2009.

- [30] K. Pister, T. Phinney, P. Thubert and S. Dwars, "Industrial Routing Requirements in Low-Power and Lossy Networks," in *RFC 5673; IETF Secretariat*, Fremont, CA, USA, 2009.
- [31] G. Porcu, J. Buron and A. Brandt, " Home Automation Routing Requirements in Low-Power and Lossy Networks," in *RFC 5826; IETF Secretariat*, Fremont, CA, USA, 2010.
- [32] J. Martocci, P. Mil, N. Riou and W. Vermeulen, " Building Automation Routing Requirements in Low-Power and Lossy Networks," in *RFC 5867; IETF Secretariat*, Fremont, CA, USA, 2010.
- [33] A. Tavakoli and S. Dawson-Haggerty, " Overview of Existing Routing Protocols for Low Power and Lossy Networks," in *Internet-Draft draft-ietf-roll-protocols-survey-07: Work in Progress; Internet Engineering Task Force*, Fremont, CA, USA, 2009.
- [34] J. Ko, A. Terzis, S. Dawson-Haggerty, D. Culler, J. Hui and P. Levis, "Connecting low-power and lossy networks to the internet," *IEEE Commun.*, vol. 49, pp. 96-100, 2011.
- [35] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann and K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wirel. Commun*, vol. 20, pp. 91-98, 2013.
- [36] R. Alexander, A. Brandt, J. Vasseur, J. Hui, K. Pister, P. Thubert, P. Levis, R. Struik, R. Kelsey and T. Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," in *RFC 6550; IETF Secretariat*, Fremont, CA, USA, 2012.
- [37] O. Iova, P. Picco, T. Istomin and C. Kiraly, "RPL: The Routing Standard for the Internet of Things... Or Is It?," *IEEE Commun*, vol. 54, pp. 16-22, 2016.
- [38] P. D. M. N. R. a. W. V. J. Martocci, "Building Automation Routing Requirements in Low-Power and Lossy Networks," *IETF RFC 5867*, June 2010.
- [39] L. W. a. V. D. S. S. R. Depuru, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and sustainable energy reviews*, Vols. 15, no. 6, pp. 2736-2742, 2011.
- [40] K. a. Gaddour O, "Rpl in a nutshell: A survey," *Comput Netw* , vol. 56, pp. 3163-3178, 2012.
- [41] G. M. a. C. S. N. Kushalnagar, "N. Kushalnagar, G. Montenegro, and C. Scumacher," in *IETF RFC 4919*, 2007.
- [42] "IEEE Std. 802.15.4-2003," in *Computer Society, IEEE*, 2003.
- [43] N. K. J. H. a. D. C. G. Montenegro, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," in *Standards Track RFC 4944*, 2007.
- [44] N. K. J. H. a. D. C. G. Montenegro, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," in *Standards Track RFC 4944*, 2007.
- [45] P. T. A. B. J. H. R. K. P. L. K. P. R. S. a. J. V. T. Winter, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," *IETF RFC 6550*, March 2012.
- [46] A. K. P. H. J. C. R. L. Ming Zhao, "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities".
- [47] R. V. P. a. I. G. N. S. Aust, "Ieee 802.11 ah: Advantages in standards and further challenges for sub 1 ghz wi-fi," *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 6885 - 6889, 2012.

- [48] M. C. a. S. C. W. Sun, "Ieee 802.11 ah: A long range 802.11 wlan at sub 1 ghz," *Journal of ICT Standardization*, vol. 1 no 1, pp. 83-108, 2013.
- [49] L. T. J. H. D. P. M. G. a. K. M. N. Cam-Winget, "Applicability statement for the routing protocol for low power and lossy networks (rpl) in ami networks," 2015.
- [50] E. a. G. M. X. Perahia, "Gigabit wireless LANs: an overview of IEEE 802.11 ac and 802.11 ad," *ACM SIGMOBILE Mobile Computing and Communications Review*, Vols. 15, no.3, pp. 23-33, 2011.
- [51] D. Cavendish, "Operation, administration, and maintenance of ethernet services in wide area networks," *IEEE Communications Magazine*, Vols. vol. 42, no. 3, pp. 72-79,, 2004.
- [52] M. Park, "Ieee 802.11 ah: s ub-1-gh z license-exempt operation for the internet of things," *IEEE Communications Magazine*, Vols. vol. 53, no. 9, pp. 145-151, , 2015..
- [53] A. A. a. d. E. C. F. Cuomo, "Cross-layer network formation for energy-efficient ieee 802.15. 4/zigbee wireless sensor networks," *Ad Hoc Networks*, Vols. vol. 11, no. 2, pp. 672-686, , 2013.
- [54] T. L. a. A. A.-A. B. A. Al-Omar, "Evaluation of wimax technology in smart grid communications," *Journal of Communications*, Vols. vol. 10, no. 10, 2015..
- [55] L. W. a. V. D. S. S. S. R. Depuru, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and sustainable energy reviews*, Vols. vol. 15, no. 6, pp. 2736-2742,, 2011..
- [56] D. S. T. K. c. S. E. C. B. C. C. a. G. P. H. V. C. Güngör, "Smart grid technologies: communication technologies and standards," *IEEE transactions on Industrial informatics*, Vols. vol. 7, no. 4, pp. 529-539, , 2011.
- [57] z. ming, "Energy-efficient and reliable routing techniques for M2M communications," 2016.
- [58] T. A. D.-H. S. Levis P, " Overview of existing routing protocols for l ow power and lossy networks," *Internet Engineering Task Force, Internet-Draft draftietf-roll-protocols-survey-07* .
- [59] A. N. O. D. J. S. Misra P, "Characterization of asymmetry in low-power wireless links: an empirical study," Springe, p. 340–351.
- [60] M. N. A. G. L. R. J. C. P. Zhao M, "An Energy-Efficient and Self-regioning based RPL for Low-power and Lossy Networks," in *The Proceedings of the 84th IEEE Vehicular Technology Conference*, 2016.
- [61] J. K. B. H. Hull B, "Mitigating congestion in wireless sensor networks," in *Proceedings of the 2nd inter-national conference on Embedded Networked Sensor Systems*, 2004.
- [62] L. B. S. K. D. M. H. Y. Wang C, "Upstream congestion control i n wireless sensor networks through cross-layer optimization," *IEEE J Sel Areas Commun*, vol. 25, pp. 786-795, 2007.
- [63] H. T. D. S. L. C. Ren F, "Traffic-aware dynamic routing to alleviate congestion in wireless sensor networks," *IEEE Trans Parallel Distrib Syst*, vol. 22, p. 1585–1599, 2011.
- [64] A. A. C. E. Cuomo F, " Cross-layer network formation for energy-efficient ieee 802.15. 4/zigbee wireless sensor networks," *Ad Hoc Networks*, vol. 11, p. 672–686, 2013.

- [65] G. O. D. S. T. L. J. D. Sun Y, "Adb: an efficient multihop broadcast protocol based on asynchronous duty-cycling in wireless sensor networks," in *The Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, 2009.
- [66] J. X. C. G. C. Z. Liu A, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," *Information Science*, vol. 230, p. 197–226, 2013.
- [67] D. M. O. K. L. A. H. S. Long J, "Reliability guaranteed efficient data gathering in wireless sensor networks," *IEEE Access*, vol. 3, pp. 430-444, 2015.
- [68] K. a. A. Gaddour O, "Rpl in a nutshell: A survey," *Computer Networks*, vol. 56, p. 3163–3178, 2012.
- [69] L. R. L. X. S. X. C. J. L. X. Li X, "Smart community: an internet of things application," *IEEE Commun Mag*, vol. 49, p. 68–75, 2011.
- [70] L. R. S. X. N. Y. K. N. Lin X, "Sage: a strong privacy-preserving scheme against global eavesdropping," 2009.
- [71] L. X. L. X. L. X. S. X. Lu R, "Eppa: an efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans Parallel Distrib Syst*, vol. 23, p. 1621–1631, 2012.
- [72] E. B.-R. a. S. D. C. Perkins, "Ad hoc on-demand distance vector (aodv) routing," *Technical Report*, 2003.
- [73] I. D. C. a. L. Klein-Berndt, "Aodvjr, aodv simplified," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, pp. 100 - 101, 2002.
- [74] C.-C. O. a. N. Faisal, "Implementation of geo cast-enhanced aodv-bis routing protocol in manet," *Proceedings of IEEE Region 10 Conference TENCON*, pp. 660-663, 2004.
- [75] G. M. a. N. Kushalnagar, "Aodv for IEEE 802.15.4 networks," *draft-montenegro-lowpan-aodv-00, IETF Internet Draft (Work in progress)*, 2005.
- [76] S. D. P. G. M. S. Y. a. N. K. K. Kim, "6lowpan ad hoc on-demand distance vector routing (load)," *Network WG Internet Draft (work in progress)*, vol. 19, 2007.
- [77] T. H. C. a. A. C. D. Verdière, "The Iln on-demand ad hoc distance-vector routing protocol next generation (loadng)," 2011.
- [78] T. s. c. repository, "Tymo: DYMO implementation for TinyOS," 2007. [Online]. Available: <http://tymo.sourceforge.net/>. [Accessed Online December 2007].
- [79] P. S. O. A. a. J. P. C. Gomez, "Adapting aodv for IEEE 802.15.4 mesh sensor networks: theoretical discussion and performance evaluation in a real environment," *Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks, IEEE Computer Society*, pp. 159-170, 2006.
- [80] R. F. K. J. D. M. a. P. L. O. Gnawali, "Collection tree protocol," *In the Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, pp. 1-14, 2009.
- [81] A. T. a. D. C. S. Dawson-Haggerty, "Hydro: A hybrid routing protocol for low-power and lossy networks," *Proceedings of the First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 268-273, 2010.

- [82] F. Z. G.-q. Z. a. D.-l. S. H.-f. Xie, "Simulation research on routing protocols in zigbee network," *the Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation, Springe .*, pp. 891-898, 2016 .
- [83] O. G. a. A. Koubâa, "Rpl in a nutshell: A survey," *Computer Networks*, vol. 56, pp. 3163-3178, 2012.
- [84] S. R. D. C. S. S. a. I. S. R. Fonseca, "Beacon vector routing: Scalable point-to-point in wireless sensor nets," *Berkeley: Intel Research*, vol. 14, 2004.
- [85] A. C. a. M. A. A. Koubaa, "A time division beacon scheduling mechanism for ieee 802.15.4/zigbee cluster-tree wireless sensor networks," *Proceedings of the 19th IEEE Euromicro Conference on Real-Time Systems (ECRTS'07)*, pp. 125-135, 2007.
- [86] T. H. C. a. A. C. D. Verdière, "The lln on-demand ad hoc distance-vector routing protocol-next generation (loadng)," 2011.
- [87] T. C. a. Y. I. J. Yi, "Evaluation of routing protocol for low power and lossy networks: Loadng and rpl," *the Proceedings of the IEEE Conference on Wireless Sensor (ICWISE)*, pp. 19-24, 2013.
- [88] U. H. e. a. T. Clausen, "A comparative performance study of the routing protocols load and rpl with bi-directional trac in low-power and lossy networks (lln)," *the Proceedings of the 8th ACM Symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, pp. 73-80, 2011.
- [89] B. T. a. A. D. M. Vucinic, "Performance comparison of the rpl and loadng routing protocols in a home automation scenario," *the Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1974-1979, 2013.
- [90] J. W. H. a. D. E. Culler, "Ip is dead, long live ip for wireless sensor networks," *In the Proceedings of the 6th ACM conference on Embedded network sensor systems*, pp. 15-2, 2008.
- [91] S. R. C. P. r. S. S. a. I. S. A. Rao, "Geographic routine without location information," in *the 9th ACM annual international conference on Mobile computing and networking*, 2003.
- [92] K. G. C. a. T. T. Peffers, "Extending critical success factors methodology to facilitate broadly participative information systems planning," *Journal of Management Information Systems*, vol. 20, no. 1, pp. 51-85, 2003b.
- [93] C. Barriquello, G. Denardin and A. Campos, " A geographic routing approach for IPv6 in large-scale low-power and lossy networks," *Comput. Electr. Eng.*, vol. 45, p. 182–191, 2015.
- [94] M. S. T. X. X. X.-Y. L. a. H. M. Xufei, "Energy-Efficient Opportunistic Routing in Wireless Sensor Networks," *Parallel and Distributed Systems, IEEE Transactions*, vol. 22, pp. 1934-1942, 2011.
- [95] R. J. Z. T. H. C. L. a. R. S. K. D. Fengyuan, "EBRP: Energy-Balanced Routing Protocol for Data Gathering in Wireless Sensor Networks," *Parallel and Distributed Systems, IEEE Transactions*, vol. 22, pp. 2108-2125, 2011.

- [96] L. C. C. Y.-Q. S. Z. W. a. Y. S. Yanjun, "Enhancing Real-Time Delivery in Wireless Sensor Networks With Two-Hop Information," *Industrial Informatics, IEEE Transactions*, vol. 5, pp. 113-122, 2011.
- [97] R. T. H. D. S. K. a. C. L. Fengyuan, "Traffic-Aware Dynamic Routing to Alleviate Congestion in Wireless Sensor Networks," *Parallel and Distributed Systems, IEEE Transactions*, vol. 22, pp. 1585-1599, 2011.
- [98] Y. a. J. W. Yaling, "Design Guidelines for Routing Metrics in Multihop Wireless Networks.," *The 27th Conference on Computer Communications*, pp. 1615-1623, 2008.
- [99] J. Yi, T. Clausen and A. Bas, "Smart Route Request for on-demand route discovery in constrained environments," in *Wireless Information Technology and Systems*, November 2012, 2012.
- [100] T. I. a. E. Hossain, *Introduction to Network Simulator*.
- [101] K. F. a. K. Varadhan, "The Ns Manual, the VINT Project," November 4, 2011 .
- [102] T. Clausen, J. Yi, A. Niktash, Y. Igarashi, H. Satoh, U. Herberg, C. Lavenue, T. Lys and J. Dean, "The Lightweight on-Demand ad hoc Distance-Vector Routing protocol-Next Generation (LOADng)," in *Internet-Draft*, Fremont, CA, USA, 2016.
- [103] V. N. a. T. Gross, *Simulation od Large Ad Hoc Network*.
- [104] T. Hui, R. Sherratt and D. Sánchez, " Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies.," *Future Gener. Comput. Syst.*, vol. 76, p. 358–369, 2017.
- [105] H. T. B. L. Dvir A, "Vera-version number and rank authentication in rpl," *International Conference on Mobile Adhoc and Sensor Systems 8th IEEE*, p. 709–714, 2011.
- [106] W. M. S. T. Landsmann M, "Topology authentication in rpl.," *IEEE Conference on Computer Communications*, p. 73–74, 2013.
- [107] A. K. P. H. J. C. a. R. L. Ming Zhao, "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities".
- [108] T. Watteyne, T. Winter, D. Barthel and M. Dohler, "Routing Requirements for Urban Low-Power and Lossy Networks; RFC 5548;," in *IETF Secretariat*, Fremont, CA, USA, 2009.
- [109] M. Goyal, E. Baccelli, M. Philipp, A. Brandt and J. Martocci, "Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks," in *RFC6997*, Fremont. CA,USA, 2013.
- [110] N. Bayazit, "Investigating design: A review of forty years of design research," in *Design Issues*, 2004.
- [111] B. S. Sanku Sinha, "Effect of Varying Node Density and Routing Zone Radius in ZRP: A Simulation Based Approach.," *International Journal on Computer Science and Engineering..*
- [112] N. H. V. Young-Bae Ko, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," no. Research reported is supported in part by Texas Advanced Technology Program grants.
- [113] F. Z. G.-q. Z. a. D.-l. S. H.-f. Xie, "Simulation research on routing protocols in zigbee network," in *Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation, Springer*, 2016.



- [114] J. X. C. G. C. Z. Liu A, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor," in *Information Science*, 2013.
- [115] D. M. O. K. L. A. H. S. Long J, "Reliability guaranteed efficient data gathering in wireless sensor networks," *IEEE Access* , vol. 3, p. 430–444, 2015.
- [116] A. Musaddiq, Y. Zikria, O. Hahm, H. Yu, A. Bashir and S. Kim, "A Survey on Resource Management in IoT Operating Systems," *IEEE Access* , vol. 6, p. 8459–8482, 2018.

