University of Kasdi Merbah Ouargla

Faculty of New Technologies of Information and Communication

Department of Computer Science and Information Technologies

Professional MASTER Thesis

Field: Computer Science and information technology

Branch: Computer Science

Specialty: Network Administration and Security

Presented by: Rechache Manar

Theme:

Study of Performance Evaluation of RPL Objective Functions (MRHOF and OFO) for IOTs

Publicly supported the: …../2021

In front of the jury:

Mr. Abd Kader BEN Mir	**President**	**UKM Ouargla**
Mr. Okba Nemli	**Examiner**	**UKM Ouargla**
Mr. Djediai AHmida	**Supervising**	**UKM Ouargla**

Year University: 2020/2021.

Acknowledgment

First, I would like to thank "ALLAH", our creator for giving me strength to accomplish this work.

I would like to expresse my special thanks of gratitude to my teacher (Mr. Djediai hmida) for accepting to supervise me, and for his incontestable instructions, patience, skills, and remarks that i have benefited. I would also like to thank the members of the jury for their precious time devoted to study my work.

My thanks and gratitude to our teachers who throughout the years of study have passed on their knowledge to us.

A special feeling of gratitude to my loving parents, my family and my best friends for their support and assistance through the provision of the comfort conditions.

Abstract

IPv6 routing protocol for low-power and lossy networks (RPL) is a proactive dynamic routing protocol based on IPV6 with tow known objective functions (OFs): objective function zero (OF0) and minimum rank with hysteresis objective function (MRHOF).

this memoir, provides an overiew of this protocol with a performance study of the two OFs used in RPL. Several scenarios have been tested with 20,30,40 and 50 nodes, with tow deffernt topologies (random and linear topology) and two parameters of comparisons were selected packet dilevery ratio and power consumption under differnt values of Packet Reception Ratio RX (20,40,60,80 and 100) in order to have an idea of suitability performance of RPL in each scenario.

The simulation is done using the cooja simulator in our implementation cooja is a flexible java-based simulator which support C java native interface. We have chosen a cooja simulator as it is a very useful tool for software development in wireless sensor networks and will provide a suitable method in which to set the environment needs.

Keywords: RPL, objective functions, packet dilevery ratio, low-power and lossy networks.

Résumé

Le protocole de routage IPv6 pour les réseaux à faible consommation et avec perte (RPL) est un protocole de routage dynamique proactif basé sur IPV6 avec deux fonctions objectives (OF) connues : fonction objectif zéro (OF0) et rang minimum avec fonction objectif d'hystérésis (MRHOF).

ce mémoire, donne un aperçu de ce protocole avec une étude des performances des deux OF utilisés en RPL. Plusieurs scénarios ont été testés avec 20,30,40 et 50 nœuds, avec deux topologies différentes (topologie aléatoire et linéaire) et deux paramètres de comparaisons ont été sélectionnés le ratio de distribution des paquets et la consommation électrique sous différentes valeurs du ratio de réception de paquets RX (20,40 ,60,80 et 100) afin d'avoir une idée de la performance d'adéquation du RPL dans chaque scénario.

La simulation est effectuée à l'aide du simulateur cooja dans notre implémentation cooja est un simulateur flexible basé sur Java qui prend en charge l'interface native C Java. Nous avons choisi un simulateur cooja car c'est un outil très utile pour le développement de logiciels dans les réseaux de capteurs sans fil et fournira une méthode appropriée pour définir les besoins de l'environnement.

الملخص

بروتوكول توجيه IPv6 للشبكات منخفضة الطاقة وفقدان (RPL) هو بروتوكول توجيه ديناميكي استباقي يعتمد على IPV6 مع اثنين من وظائف الهدف المعروفة :(OFs) الوظيفة الموضوعية صفر (OF0) والحد الأدنى من الرتبة مع وظيفة هدف التخلفية.(MRHOF)

تقدم هذه المذكرات نظرة شاملة لهذا البروتوكول مع دراسة أداء لاثنين من OFs المستخدمة في .RPL تم اختبار العديد من السيناريوهات باستخدام 20،30،40 و 50 عقدة ، مع طوبولوجيتين مختلفتين (طوبولوجيا عشوائية وخطية) وتم اختيار معلمتين للمقارنات نسبة تخفيف الحزمة واستهلاك الطاقة تحت قيم مختلفة من نسبة استقبال الحزم20) RX ، (40و 60 و 80 و 100) من أجل الحصول على فكرة عن مدى ملاءمة أداء RPL في كل سيناريو.

يتم إجراء المحاكاة باستخدام محاكي cooja في تطبيقنا cooja هو محاكي مرن قائم على جافا يدعم واجهة java ICالأصلية. لقد اخترنا جهاز محاكاة cooja لأنه أداة مفيدة للغاية لتطوير البرامج في شبكات الاستشعار اللاسلكية وسيوفر طريقة مناسبة لضبط احتياجات البيئة.

الكلمات المفتاحية RPL : الوظائف الموضوعية ، نسبة تخفيف الرزم ، الشبكات منخفضة الطاقة والفاقد.

Contents

Figures list

Tables list

List of Abbreviations

AODV: Ad-hoc On-Demand Distance Vector Routing

CARP: Channel Aware Routing Protocol

DAO: Object of update to the Destination

DAO-ACK: Destination advertisement Object Acknowledgement

DIO: Object of Information of the DAG

DIS: Information request DODAG

DODAG: Destination Oriented Directed Acyclic Graph

ETX: Expected Transmission Count

IPv6: Internet Protocol version 6

IOT: Internet of Things

LLN: Low-Power and Lossy Network

LPM: Low-power Mode

LOADng: Lightweight On-Demand Distance Vector Routing next generation

MRHOF: Minimum Rank Hysteresis Objective

NFC: Near Field Communication

OF0: Ojective Function Zero

PDR: Packet Delivery Ratio

RFID: Radio Frequency Identification

ROLL: Routing Over Low-power and Lossy

RPL: Routing Protocol for Low-Power

RX: Packet Reception Ratio

WSN: Wirelless Sensor Networks

WMN: Wireless Mesh Networks

General Introduction

General Introduction

The term The Internet of Things (IoT) is commonly used to name a set of objects (or things) that are directly connected to the Internet using the Internet Protocol (IP) stack. That is the main difference of wireless sensor networks (WSN) of previous generation where nodes were organized in a local network with special protocols like ZigBee or Wireless HART. Connection of objects to the global network in the IoT opens the opportunity for global data analysis. Typical applications for the IoT are home automation (e.g. smart home), (1) personal health monitoring (e.g. measurements of heart rate, pulse or temperature), building automation (e.g. control heating, electrical and ventilation systems of the building), industrial automation (e.g. control of the electrical grids) and smart cities.

Routing is an essential service in the IoT, since it enables the exchange of information between Things, by efficiently directing and reliably delivering data on the network from their sources to their destinations. However, routing in the IoT is also challenging, due to the global scale of the IoT, the massive number of Things in the IoT, the dynamic topology of the IoT, and the resource constraints of the IoT devices (2).

The Internet Engineering Task Force (IETF) quickly recognized the need to form a new Working Group (WG) to standardize an IPv6-based routing solution for IP smart object networks, which led to the formation of a new Working Group called ROLL (Routing Over Low power and Lossy) networks in 2008 (3).

The ROLL Working Group conducted a detailed analysis of the routing requirements focusing on several applications: urban networks including smart grid, industrial automation, home, and building automation. This set of applications has been recognized to be sufficiently wide to cover most of the applications of the Internet of Things. The objective of the WG was to design a routing protocol for LLNs, supporting a variety of link layers, sharing the common characteristics of being low bandwidth, lossy and low power. The result of this Working (4) Group was the "Ripple" routing protocol (RPL) specification, along with supporting specifications on routing metrics, objective functions and security.

which is considered as a high path selection process that impacts on routing behavior. More recently, the IETF RoLL working group developed the RPL standard, which is a routing protocol targeting IPv6-based LLNs. The RPL is a distance vector routing protocol for LLN that makes use IPv6 a standard for WSN. One of the key issue within RPL is selecting the Objective Function which is used to find the suitable path. Also (5), Tao and Xianfeng have defined the OF value using available metrics, which can be used to select a parent set and a preferred parent from a node's neighbors, and how this value is used to determine a node's rank. At present, only two different OFs have been selected namely Minimum Rank with Hysteresis Objective Function (MRHOF) and Objective Function zero (OF0). The OF0 is known as a basic OF that does not require any metric to be measured but will use default configurations. On the other hand, MRHOF is slightly more complicated and can compute a node's rank based on the additive metrics

The goal of our final year project is to do:

- Implementation of RPL protocol performance.
- Compare the performance of RPL engaged with OF0 and MRHOF in random and linear topologies for light density networks.

Our work is organized as follows

chapter 1: introduction to internet of things, chapter 2: routing in IOT network, chapter 3: presentation of the protocol RPL, chapter 4 implementation and analysis of RPL performance and finally conclusion of this contribution and future work.

Chapter1

Introduction to Internet Of Things

1.1.Introduction

Today, internet application development demand is very high. So IOT is a major technology by which we can produce various useful internet applications.

Basically, IOT is a network in which all physical objects are connected to the internet through network devices or routers and exchange data. IOT allows objects to be controlled remotely across existing network infrastructure.

Iot is a very good and intelligent technique that reduces human effort as well as easy access to physical devices. This technique also has autonomous control feature so that any device can control without any human interaction.

in this chapter we present an introduction to IOT, it covers a definition of this concept, its architecture, fundamental technologies and fields of application.

1.2.Internet of things

The internet of things (IOT) is a recent communication paradigm that envisions a near future, in which the objects of everyday life will be equipped with microcontrollers, trans-ceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the internet. The IOT concept, hence, aims at making the internet even more immersive and pervasive. Furthermore, by enabling easy access and interaction with a wide variety of devices such as, for instance, home application, surveillance cameras, monitoring sensors, actuators, displays, vehicles, and so on (6). As the Internet of things ecosystem evolves through an increasing number of users, there is a wide range of requirements that needs to be met. The 5G network is expected to massively improve or expand IoT security, trustworthiness, wireless coverage, ultra-low latency, mass connectivity. To match up with these requirements, the Long-Term Evolution (LTE) and 5G technologies would provide/ introduce new connectivity interfaces for future IoT applications. The next generation of networks, 5G which is still at its early stage, would introduce new Radio Access technologies(RAT), well improved antenna (Smart antennas) and also make use of higher frequencies while also altering or re-architecting networks. greatly increase speed, boost cellular operation with increased bandwidth while also resolving several network challenges faced in the previous generations of mobile networks. the advent of 5G which is proposed to be fully operational in the near futur extensively and its interconnection with Internet of things would be explained as it would be the technology on which IoT would run.

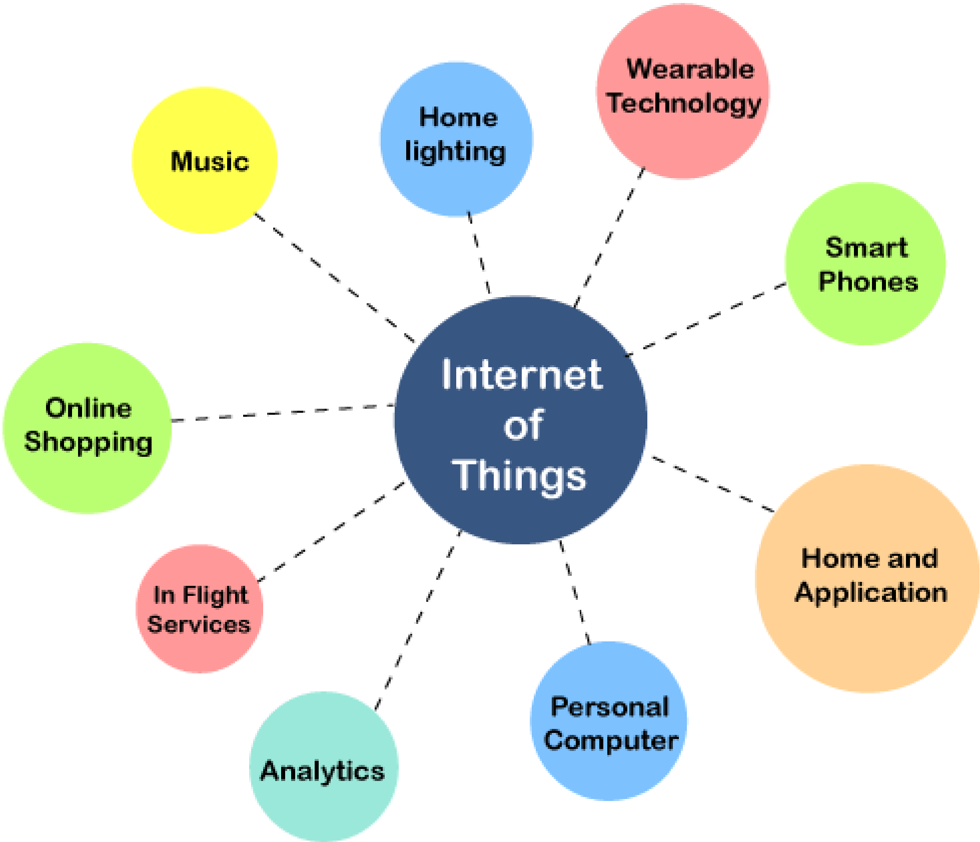


Figure 1 Definition of internet of thing

1.3. Objectives of the internet of things

by connecting all kinds of objects and systems, internet stuff can offer new ways to research and learn. The internet can also integrate university infrastructure linking physical buildings and their contents, such as classrooms, learning spaces, and administrative areas with communications systems and service systems that support them for example, through continuous regulation of heat and lighting (7).

Internet objects (IOT) also facilitates new types of tasks that explore the types of knowledge available from data when many are associated with each other. Students can build inexpensive IOT devices that allow them to conduct research that may have been possible only in large laboratories in the past.

1.4. IOT Element

IoT provides many benefits and facilities to users. Thus, in order to use them properly, there is a need for some elements. In this section, elements of IoT are discussed. Figure shows the elements needed to deliver the functionality of IoT. The names and details of these elements are as follows (8).

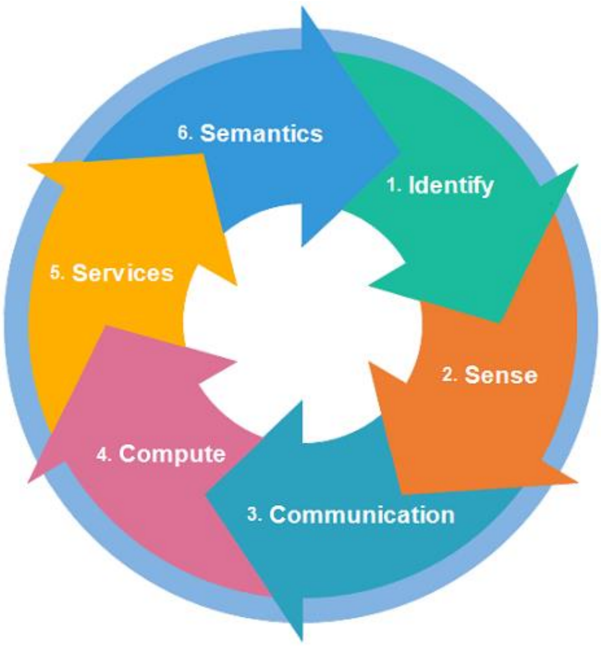


Figure 2 Iot element

1.4.1. Identification

Identification offer explicit identity for each object within network. There are two processes in identification; naming and addressing. Naming refers as name of the object while addressing is the unique address of specific object. These both terms are very different from each other because two or more objects may have same name but always different and unique address. There are many methods available that provide the naming facility to the objects in the network such as electron products codes (EPC) and ubiquitous codes. To assign the unique address to each object, IPv6 is used. Firstly, IPv4 was used to assign the address but it could not fulfill the need of addressing due to large amount of IoT devices. Therefore, IPv6 is used because it uses 128 bit number addressing scheme.

1.4.2. Sensing

The process of collecting information from objects is known as sensing. The collected information is sent to the storage media. There are many sensing devices to collect the information from objects such as actuators, RFID tags, smart sensors, wearable sensing devices, etc.

1.4.3. Communication

Communication is one of the main purposes of IoT in which different devices are connected to each other and communicate. In communication, devices may send and receive messages, files and other information. There are many technologies that provide facility of communication like Radio Frequency Identification (RFID), Near Field Communication (NFC), Bluetooth, Wi-Fi and Cellular (3G/4G/5G) and ZigBee.

- **Radio Frequency Identification (RFID**)

Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver and transmitter. When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifying inventory number, back to the reader. This number can be used to track inventory goods.

There are two types of RFID tags:

- *Passive tags* are powered by energy from the RFID reader's interrogating radio waves.
- *Active tags* are powered by a battery and thus can be read at a greater range from the RFID reader, up to hundreds of meters.

Unlike a barcode, the tag does not need to be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture (AIDC).

- **Near Field Communication (NFC)**

Near-field communication (NFC) is a short-range wireless technology that makes your smartphone, tablet, wearables, payment cards, and other devices even smarter. Near-field communication is the ultimate in connectivity. With NFC, you can transfer information between devices quickly and easily with a single touch—whether paying bills, exchanging business cards, downloading coupons, or sharing a research paper.

  - Near-field communication (NFC) is a short-range wireless connectivity technology that lets NFC-enabled devices communicate with each other.
  - NFC began in the payment-card industry and is evolving to include applications in numerous industries worldwide.

- **Bluetooth**

Defined in the category of Wireless Personal Area Networks, Bluetooth is a short-range communication technology well-positioned in the consumer marketplace. Bluetooth Classic was originally intended for point-to-point or point-to-multipoint (up to seven slave nodes) data exchange among consumer devices. Optimized for power consumption, Bluetooth Low-Energy was later introduced to address small-scale Consumer IoT applications.

- **Wi-Fi**

Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet. It allows these devices--and many more--to exchange information with one another, creating a network.
Internet connectivity occurs through a wireless router. When you access Wi-Fi, you are connecting to a wireless router that allows your Wi-Fi-compatible devices to interface with the Internet.

- **Zigbee and Other Mesh Protocols**

Zigbee is a short-range, low-power, wireless standard (IEEE 802.15.4), commonly deployed in mesh topology to extend coverage by relaying sensor data over multiple sensor nodes. Compared to LPWAN, Zigbee provides higher data rates, but at the same time, much less power-efficiency due to mesh configuration.

Because of their physical short-range (< 100m), Zigbee and similar mesh protocols (e.g. Z-Wave, Thread etc.) are best-suited for medium-range IoT applications with an even distribution of nodes in close proximity. Typically, Zigbee is a perfect complement to Wi-Fi for various home automation use cases like smart lighting, HVAC controls, security and energy management, etc. – leveraging home sensor networks.

Until the emergence of LPWAN, mesh networks have also been implemented in industrial contexts, supporting several remote monitoring solutions. Nevertheless, they are far from ideal for many industrial facilities that are geographically dispersed, and their theoretical scalability is often inhibited by increasingly complex network setup and management.

- Cellular (3G/4G/5G)

Well-established in the consumer mobile market, cellular networks offer reliable broadband communication supporting various voice calls and video streaming applications. On the downside, they impose very high operational costs and power requirements.

While cellular networks are not viable for the majority of IoT applications powered by battery-operated sensor networks, they fit well in specific use cases such as connected cars or fleet management in transportation and logistics. For example, in-car infotainment, traffic routing, advanced driver assistance systems (ADAS) alongside fleet telematics and tracking services can all rely on the ubiquitous and high bandwidth cellular connectivity.

Cellular next-gen 5G with high-speed mobility support and ultra-low latency is positioned to be the future of autonomous vehicles and augmented reality. 5G is also expected to enable real-time video surveillance for public safety, real-time mobile delivery of medical data sets for connected health, and several time-sensitive industrial automation applications in the future.

1.4.4. Services

There are four types of services that are provided by the IoT applications. The first one is an identity-related service. It is used to get the identity of objects that have sent the request. Information aggregation is another service whose purpose is to collect all the information from objects. Processing is also performed by the aggregation service. The third service is a collaborative service that makes decisions according to the collected information and sends appropriate responses to the devices. The last service is ubiquitous service, which is used to respond the devices immediately without rigidity about time and place (9).

1.4.5. Semantics

It is the responsibility of IoT to facilitate users by performing their tasks. It is the most important element of IoT to fulfill its responsibilities. It acts like the brain of IoT. It gets all information and makes appropriate decisions to send responses to the devices.

1.5. Architecture of IOT

There is no single consensus on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers. (10)

1.5.1. Three- and Five-layer architectures

The most basic architecture is a three-layer architecture [3–5] as shown in Figure 3. It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

i. **The *perception layer*** is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.

ii. **The *network layer*** is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.

iii. The ***application layer*** is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.

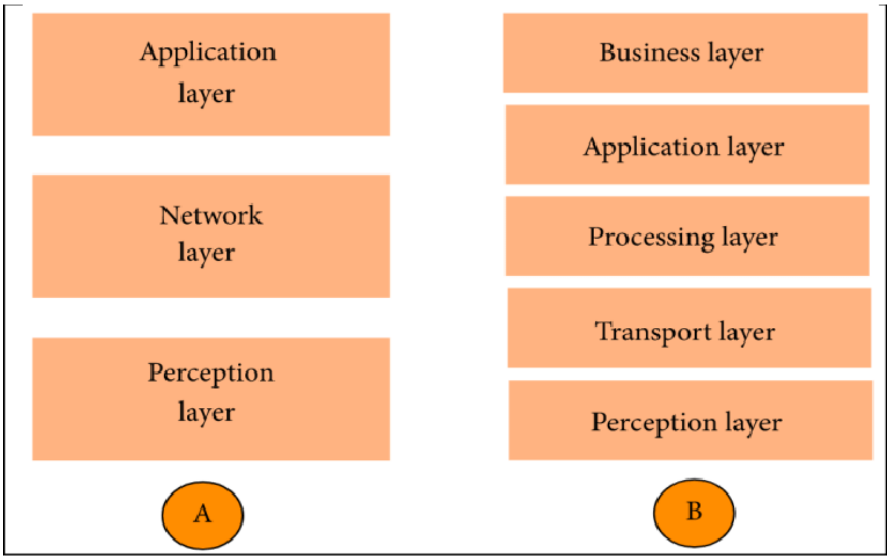


Figure 3 Architecture of IoT (A: three layers) (B: five layers).

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the five-layer architecture, which additionally includes the processing and business layers [3–6]. The five layers are perception, transport, processing, application, and business layers (see Figure 3). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers (11).

i. **The *transport layer*** transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.

ii. **The *processing layer*** is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.

iii. **The *business layer*** manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.

Another architecture proposed by Ning and Wang is inspired by the layers of processing in the human brain. It is inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physical environment. It is constituted of three parts. First is the human brain, which is analogous to the processing and data management unit or the data center. Second is the spinal cord, which is analogous to the distributed network of data processing nodes and smart gateways. Third is the network of nerves, which corresponds to the networking components and sensors.

1.6. IOT network

the internet of things compose of several types of networks including LLN (low power and lossy network) WSN (Wireless sensor networks) WMN (Wireless mesh network) which are discussed below

1.6.1. Low-power and lossy network (LLN)

low-Power and Lossy Network (LLN) the ROLL (Routing Over Low-Power and lossy) terminology document RFC 7102 defines LLNs as follows:

Low-Power and Lossy Network. Typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links, such as IEEE 802.15.4 or low-power Wi-Fi. There is a wide scope of application areas for LLNs, including industrial monitoring, building automation (heating, ventilation, and air conditioning (HVAC), lighting, access control, fire), connected home, health care, environmental monitoring, urban sensor networks, energy management, assets tracking, and refrigeration.

RFC 7228 further says, Low-Power and Lossy Network often exhibit considerable loss at the Physical Layer, with significant variability of the delivery rate, and some short-term unreliability, coupled with some medium-term stability that makes it worthwhile to both construct directed acyclic graphs that are medium-term stable for routing and do measurements on the edges such as Expected Transmission Count (ETX) RFC 6551. Not all LLNs comprise low-power nodes RPL-DEPLOYMENT.

Low-Power and Lossy Networks typically are composed of Constrained Nodes; this leads to the design of operation modes such as the "non-storing mode" defined by RPL (the IPv6 Routing Protocol for Low-Power and Lossy Networks RFC 6550). So, in the terminology of the present document, an LLN is a Constrained Node Constrained Network with certain network characteristics, which include constraints on the network as well.

1.6.2. Wireless sensor networks (WSN)

Many times, data from a single sensor is not useful in monitoring large areas and complex activities. Different sensor nodes need to interact with each other wirelessly. The disadvantage of non-IP technologies such as RFID, NFC, and Bluetooth is that their range is very small. So, they cannot be used in many applications, where a large area needs to be monitored through many sensor nodes deployed in diverse locations. A wireless sensor network (WSN) consists of tens to thousands of sensor nodes connected using wireless technologies. They collect data about the environment and communicate it to gateway devices that relay the information to the cloud over the

Internet. The communication between nodes in a WSN may be direct or multihop. The sensor nodes are of a constrained nature, but gateway nodes have sufficient power and processing resources. The popular network topologies used in a WSN are a star, a mesh, and a hybrid network. Most of the communication in WSN is based on the IEEE 802.15.4 standard. There are clearly a lot of protocols that can be used in IoT scenarios. Let us discuss the design of a typical IoT network protocol stack with the most popular alternatives (12).

1.6.3. Wireless mesh networks (wmn)

is a communications network made up of radio nodes organized in a mesh topology. It can also be a form of wireless ad hoc network.

A mesh refers to rich interconnection among devices or nodes. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. Mobility of nodes is less frequent. If nodes constantly or frequently move, the mesh spends more time updating routes than delivering data. In a wireless mesh network, topology tends to be more static, so that routes computation can converge and delivery of data to their destinations can occur. Hence, this is a low-mobility centralized form of wireless ad hoc network. Also, because it sometimes relies on static nodes to act as gateways, it is not a truly all-wireless ad hoc network.

Mesh clients are often laptops, cell phones, and other wireless devices. Mesh routers forward traffic to and from the gateways, which may, but need not, be connected to the Internet. The coverage area of all radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud depends on the radio nodes working together to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks can self form and self heal. Wireless mesh networks work with different wireless technologies including 802.11, 802.15, 802.16, cellular technologies and need not be restricted to any one technology or protocol. (13)

1.7. Applications of IOT

There are a diverse set of areas in which intelligent applications have been developed. All of these applications are not yet readily available; however, preliminary research indicates the potential of IoT in improving the quality of life in our society. Some uses of IoT applications are in home automation, fitness tracking, health monitoring, environment protection, smart cities, and industrial settings (14).

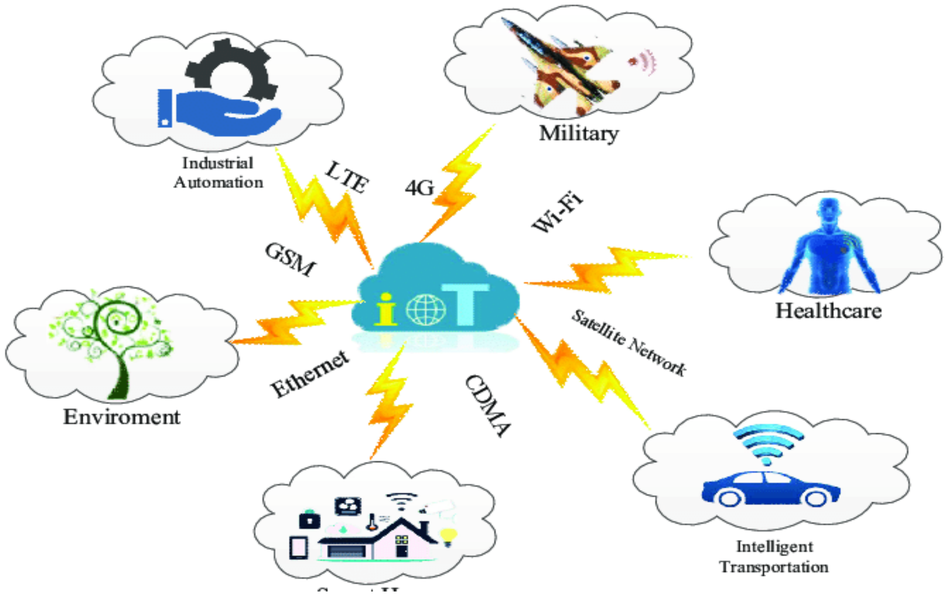


Figure 4 Examples of IOT applications

1.8. Conclusion

the internet of things is of considerable interest. In fact, the more new technologies increase, the more the iot evolves and takes up space in our lives.

in this first chapter, we have described the elements of iot, as well as their main fields of application, the iot architecture and the different types of networks such as LLN, WSN, WMN ... etc. however, we have noticed that several factors complicate the management of this type of networks insufficient power, very limited computing power and memory capacity. the following chapter is dedicated to a study on routing in IOT networks, more precisely in LLNs networks.

Chapter2

Routing in IOT networks

2.1. Introduction

routing in LLNs presents many challenges for the scientific community because of their unique characteristics such as insufficient power, very limited computing power and memory capacity, highly asymmetric link characteristics, significant data loss and short communication distances .... etc. therefore, several routing protocols were proposed to meet the requirements of LLNs networks.

this chapter is devoted to routing in a general way and more specifically to rpl routing protocol which interested researchers in order to improve routing performance in networks. with this in mind, we will introduce the main routing protocols, according to the different classifications, in particular detailing the RPL, CORPL, CARP, AODV, LOADng, and ADODVv2 protocols.

2.2. Routing

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet (15).

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

2.2.1. Routing Protocol Metrics

There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and differentiate between the available paths. This is accomplished through the use of routing *metrics* (16).

A metric is a measurable value that is assigned by the routing protocol to different routes based on the usefulness of that route. In situations where there are multiple paths to the same remote network, the routing metrics are used to determine the overall “cost” of a path from source to destination. Routing protocols determine the best path based on the route with the lowest cost.

Different routing protocols use different metrics. The metric used by one routing protocol is not comparable to the metric used by another routing protocol. Two different routing protocols might choose different paths to the same destination.

The most common metric values are hop, bandwidth, delay, reliability, load, and cost.

2.3. Proactive and Reactive Routing Protocols

2.3.1. Proactive Routing protocols

Proactive or Table-driven protocols maintain routing information even before this information is required. Each node maintains routing information to every other node in the network. Route information is generally stored in routing tables and is periodically updated with any change in the network topology. the protocols that fall under this category maintain different numbers of tables. Also, they are not suitable for large scale networks, because they need to maintain entries for each node in the routing table (17).

2.3.2. Reactive Routing Protocol

In reactive or demand protocols, n odes initiate route discovery throughout the network, only when they want to send packets to the destination. For this purpose, the route discovery process is completed once a route is established or all possible variations have been examined. Once a route has been established, it is maintained by a route maintenance process until either the destination becomes inaccessible along every path from the source or until the route is no longer desired through the use of timers

2.4. Routing protocols

In order to cope with the limitations of the IoT systems, a routing protocol should meet specific requirements and employ different strategies. Such a protocol needs to match the traffic pattern of its deployment area and be resourceful in terms of power consumption. Also, it has to scale in terms of memory and performance, while being able to cope with sparse location changes. Moreover, an IoT routing protocol is required to recognize and avoid one-way links and be conservative on the transmitter energy usage. Last but not least, supporting IPv6 and mobility are considered as essential qualities. The strategies used include proactive routing, by trying to have an global view of the whole network topology at all times, and reactive routing, by searching the routes on demand. provides a taxonomy of the most important routing protocols in IoT domain (18).

2.4.1. RPL

In 2012, IETF released a Distance Vector Routing Protocol for Low Power and Lossy Networks (RPL). RPL creates a Destination Oriented Directed Acyclic Graph (DODAG) which contains just a single path from every leaf node to the root. The whole traffic from the node will be forwarded to the root. The root decides the forwarding of a Destination Advertisement Object (DAO) from a node that needs to communicate. Also, it handles the DODAG Information Solicitation (DIS) requests of nodes that want to join the network. RPL nodes can be either stateless, by keeping tracks of its parents only, or stateful by keeping track of its children and parents (19).

2.4.2. RPL Enhancements

Various enhancements have been proposed to improve the performance of basic RPL protocol. P2P RPL is a standardized, point-to-point reactive RPL (P2P-RPL) that enables an IPv6 router in a LLN to discover paths to one or more IPv6 routers in the LLN on demand. Enhanced-RPL is an enhancement for RPL protocol aiming at enhancing its reliability. Dynamic RPL (D-RPL) is used for the dynamic applications of IoT. D-RPL improves the energy efficiency of the network and the end-to-end delay and more importantly it adapts to mobility changes better than relevant RPL-based protocols. mRPL is the mobile version of RPL, focusing on the mobility management in IoT environments. However, it neglects other metrics resulting in unneeded handovers and sometimes the establishment of unreliable connections. Furthermore, a "Smarter-HOP" version of mRPL for mobility optimization in RPL was proposed, denoted as mRPL++ (20).

2.4.3. CORPL

CORPL is a nonstandard extension of RPL that is built for cognitive networks and employs DODAG topology generation. CORPL uses opportunistic data transmission to forward the packet by choosing multiple forwarders (forwarder set). It coordinates them so as to choose the optimal next hop to relay packets to. DODAG is designed similarly to RPL. Every node keeps a forwarding set instead of its parent only and informs its neighbor with its changes using DAG Information Object (DIO) messages. According to the up-to-date information, every node dynamically updates its neighbor priorities so as to build the forwarder set (21).

2.4.4. CARP

Channel-Aware Routing Protocol is a nonstandard distributed routing protocol used in Underwater Wireless Sensor Networks (UWSNs). Its assets include delivering packets in reasonable time with low energy demands. In addition, it is able to support link quality information that is calculated from historical successful data transfers. The history is collected from adjacent sensors in order to choose the forwarding nodes. The main weakness of CARP is that it does not allow reusing previously gathered data. An enhancement of CARP is denoted as E-CARP. E-CARP allows the sink node to save previously received sensor data. Hence, E-CARP drastically decreases the communication overhead (22).

2.4.5. AODV, LOADng, and AODVv2

Ad Hoc On-Demand Distance Vector Routing (AODV) is classified as hop-by-hop reactive routing protocol, defined in 2003 by IETF. It employs a Route Request- (RREQ-) Route Reply- (RREP-) cycle that is initiated each time a packet needs to be transferred to an unknown destination. Two successors of AODV are (a) the Lightweight On-Demand Ad Hoc Distance Vector Routing Protocol-Next Generation (LOADng) and (b) the AODVv2. Contrary to AODV which just uses hop-count as a routing metric, its two successors accept various metrics, possibly enabling the use of an energy-aware metric. There are also some other routing protocols that make simplifications on AODV in order to reduce footprint and be well-suited for the dynamic and resource-limited network environment. These are AODVbis, AODVjr, LOAD(ng), LoWPAN-AODV, NST-AODV, and TinyAODV (23).

2.5. Routing protocols in IoT domain: features and characteristics.

Table 1 Routing protocols in IoT domain: features and characteristics.

Routing protocol name	RPL	P2P-RPL	CORPL	CARP	LOADng
Strategy	Proactive	Reactive	Proactive	Reactive	Reactive
Traffic type	MP2P, P2P & P2MP	P2P	MP2P, P2P & P2MP	MP2P, P2P & P2MP	P2P
Mechanism	Energy-aware metrics & multipath routing	Energy-aware metrics	Energy-aware metrics & multipath routing	Energy-aware metrics & multipath routing	Energy-aware metrics
Algorithm	(i) Distance vector (ii) Source routing	(i) Distance vector (ii) Source routing	Distance vector	Link state	Distance Vector
IPv6 support	Yes	Yes	Yes	Yes	Yes
IoT Routing challenges met	(i) Local and global repairs (ii) Energy usage low (iii) Mobility (iv) High scalability (v) Low memory usage	(i) Local and global repairs (ii) Energy usage low (iii) Mobility (iv) High scalability	(i) Data management (ii) Server technologies	(i) Data management (ii) Storage management	(i) Energy usage low (ii) Mobility (iii) High scalability (iv) Low memory usage
Main features	(i) Loop detection and avoidance (ii) Self-configuration (iii) Timer management	Discovers the best-quality route for any source-destination pair	Opportunistic forwarding approach based on RPL	(i) Link quality selection for packet forwarding (ii) High packet delivery ratio for increasing traffic	(i) A lightweight variation of AODV (ii) Suitable for a more general traffic pattern

Disadvantages	No security	(i) No security (ii) High memory usage	(i) No security (ii) No storage management	(i) No security (ii) No server technologies (iii) No reusability of previously collected data	(i) No security (ii) No local repair (iii) High delay in the route discovery

2.6. Conclusion

in this chapter, we talked about routing in a general way and then we gave a little overview on the routing protocols in internet of things.

There exists routing protocols developed for sensor networks and further gradually adapted to the IOTs due to the limitations in power and bandwidth. One of the routing protocols, RPL facilitates bi-directional communication between source and sink nodes. Further, multiple modes of operation such as Multipoint to point, Multipoint to point and point to multipoint communication which we are going to see in the next chapter.

Chapter3

Presentation of the protocol RPL

3.1. Introduction

Low-power and Lossy Networks (LLNs) consist largely of constrained nodes (with limited processing power, memory, and sometimes energy when they are battery operated or energy scavenging). These routers are interconnected by lossy links, typically supporting only low data rates, that are usually unstable with relatively low packet delivery rates. Another characteristic of such networks is that the traffic patterns are not simply point-to-point, but in many cases point-to- multipoint or multipoint-to-point. Furthermore, such networks may potentially comprise up to thousands of nodes. These characteristics offer unique challenges to a routing solution

3.2. RPL protocol

RPL (Routing Protocol for low power and Lossy networks with low power consumption and generally susceptible to packet loss. It is a proactive protocol based on distance vectors and operates on IEEE 802.15.4, optimized for multi-hop and many-to-one messages.

RPL can support a wide variety of link layers, including those with limitations, with potential losses or that are used in devices with limited resources, this protocol can quickly create network routes, share routing knowledge and adapt the topology in an efficient way (24).

3.3. Implementation of the RPL protocol

The implementation of the RPL protocol occurs in wireless sensors and networks, the most used operating system for its implementation is Contiki which is a small systems ranging from 8-bit computers to integrated systems on microcontrollers, including sensor network nodes (25).

3.4. Control messages

New types of ICMPV6 control messages have been proposed in RPL to build a network topology (DODAG) .

RPL uses following four main types of messages for the topology formation and its maintenance (26):

3.4.1. DIS (information request DODAG)

Used to request information from nearby DODAG, analogous to router request messages used to discover existing networks.

3.4.2. DIO(object of information of the DAG)

Message that shares information from the DAG, sent in response to DIS messages, as well as used periodically to refresh the information of the nodes on the topology of the network.

3.4.3. DAO(object of update to the destination)

Sent in the direction of the DODAG, it is a message sent by the teams to update the information of their "parent" nodes throughout the DAG.

3.4.4. DAO-ACK(Destination advertisement object acknowledgement)

The DAO-ACK message is sent as a unicast packet by a DAO recipient (a DAO parent or DODAG root) in response to a unicast DAO message.

3.5.Routing metrics

A routing metric is a quantitative value used to find the cost of a path and helps in making the routing decision in case there are different routes available. In LLN a metric is a scalar used to find the best path according to the objective function (27).

Unlike traditional networks LLN also use node metric apart from link metrics. Therefore the metrics can be categorized as node metric and link metrics as stated below

Node metrics: Node State Attribute (NSA), Node Energy, Hop count

Link metrics: Throughput, Latency, Link Quality Level, ETX, Link Color

Hop Count: This metric counts the number of hops from the source to the destination. A hop count of 3 means there are 3 intermediate links between the source and destination.

Expected Transmission Count (ETX): ETX of a link is the expected number of transmissions required to send a packet over that link. The path ETX is the sum of the ETX of all the links along the path. The ETX of a path with 3 links of 100% delivery ratio is 3, whereas the ETX of a path with 2 links of 50% delivery ratio is 4.

Since low power networks have vastly varying requirements and characteristics like lossy links, resources constraints, mobility, a vast variety of applications, therefore RPL does not define any specific metrics or forwarding polices and these are described in other IETF Drafts.

Routing metrics are a critical component to the routing strategy. LLN has a wide variety applications and constraints which strongly appeal for dynamic metrics.

To better understand the need of dynamic metrics and difference between a metric and constraint for LLN, let's consider the following examples.

3.6.Routing constraint

A constraint is used to either include or exclude links from the routing path that do not meet the criteria specified in the objective function (28).

3.7.Topology construction

RPL has to discover links and then select peers in such a way that no cycles are present. To this end, a Directed Acyclic Graph (DAG) built according to one or more Destination Oriented DAGs (DODAGs), one DODAG per root using an Objective Function (OF) to reach specific objectives. RPL use ICMPv6 control messages to form and manage the nodes that constitute the WSN. Tree messages are present : DODAG Information Object (DIO), DODAG Information Solicitation (DIS) and the DODAG Destination Advertisement Object (DAO). In order to build a DODAG, the root sends periodically DIO to its neighbors containing several parameters such as rank, metric, routing cost and DODAGID. Then neighbours nodes decide to join DODAG according to the OF. The Algorithm of rank calculation is illustrated in fig5 (29).

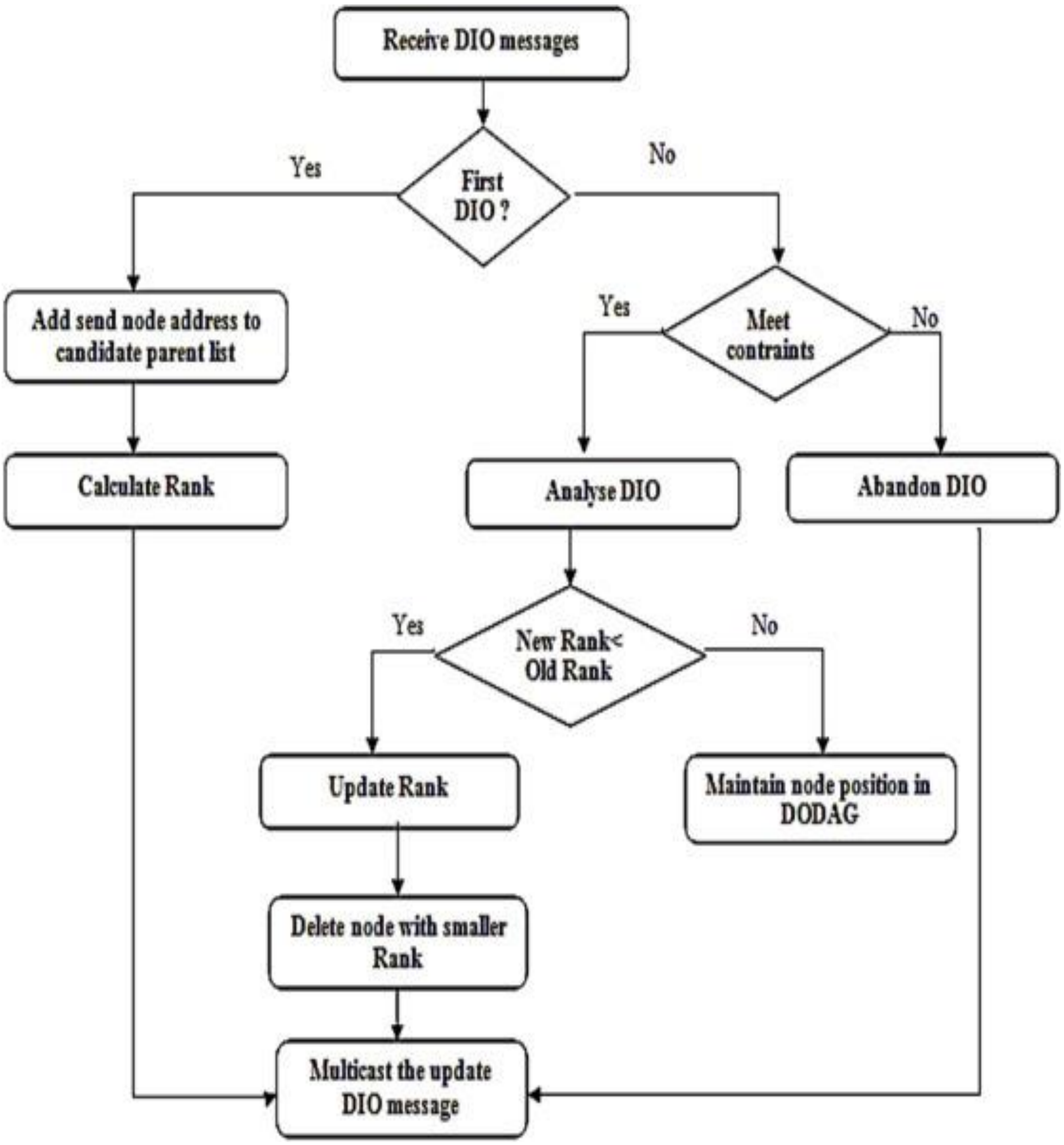


Figure 5 Process of calculation rank node

The process of building DODAG continue with nodes that decide to join the DODAG. Once this process is completed, each node has a routing table to its parent, hop-by-hop take to the root node. Also, the node may sends a DIS used to request information from its neighbors when waiting for DIO message. In order to maintain the network more stable, RPL uses the Trickle algorithm, to periodically refresh the DODAG. The DAO are transmitted according to two modes of operation (MOP); storing mode and non-storing mode. In the first one, once the neighbors nodes recept the DAO from the sensors, RPL maintain a routing table containing all reachable destinations. In second mode, the DAO messages are directly unicast to the root. The structure of RPL and its creation has been illustrated in fig.6.

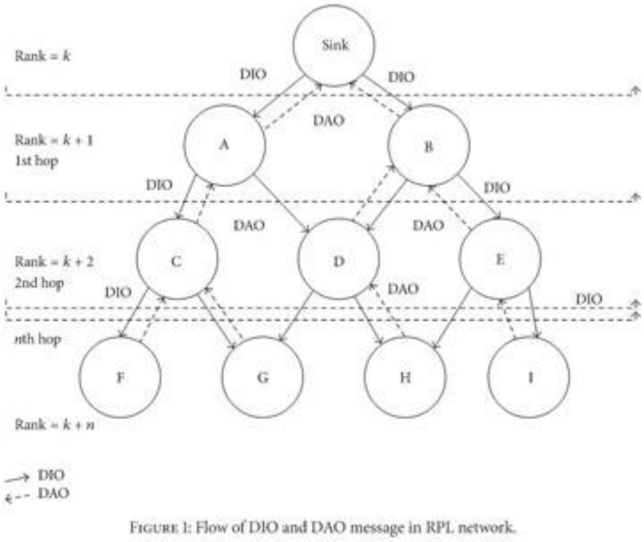


Figure 6 Process of DODAG construction with RPL

3.8. Path selection mecanism by objective function

The Objective Function is used to define one or more metrics to help nodes to translate these metrics into ranks. It is responsible for selecting the routes in a DODAG. Rank computation is fulfill using the OF depending on routing metrics as a reference like link quality and delay, and the other side to express the distance between a node in the network and the DODAG root. RPL can separate the OFs from the core of the protocol which allows it to meet the different optmization criteria required. Each DODAG instance in RPL's DAG is associated with a particular OF. Otherwise, two objective functions are defined in RPL : Objective Function Zero (OF0) and Minimum Rank Hysteresis Objective Function (MRHOF). MRHOF is an objective function that use minimum value of Expected Transmission Count (ETX) on parent node selection. ETX is an expected number of transmission that required for it to be received without error at its destination. OF0 is an objective function that use minimum value of hop to reach root node. Each node will calculate rank based on the hop value to the root node. The fewer number of jumps will get higher priority link to be selected by OF0. Rank value on child node is always higher than the parent node (30)

3.9. Repair mechanisms of dodag

RPL has two mechanisms to repair the topology of DODAG, which are complementary, the global and local repair. The global repair is triggered only from the root, it's a graphic reconstruction mechanism from scratch. Which the root begins incrementing the version number of the DODAG when sending DIO for a new DODAGVersion. When nodes receive DIO, they accept only the whose version number is greater than or equal to the current number. This version number ensures that information circulating in the network is up to date, to the extent that the former DIO are "crush" with the most recent. The global repair is an optimization technique, but it has a cost of additional control traffic in the network and delay to repair depends on sequence number refresh rate. The local repair is complementary to the global, subsequently the global repair. Which allow the DODAG repaired within the DODAG Version. In which Each node can detach from the DODAG, moves its parent to its routing table, local poison the sub-DODAG by advertising the rank of infinity, and the end, it re-attach to the original or a newbranch DODAG. This technique presents the risk of creating a loop and count infinity, it Used DAG Hop Timer to wait for poisoning to occur. The local repair is not implemented in the RPL module with ContikiRPL (31)

Link between G and C fails:

- Choose another parent with a lower rank

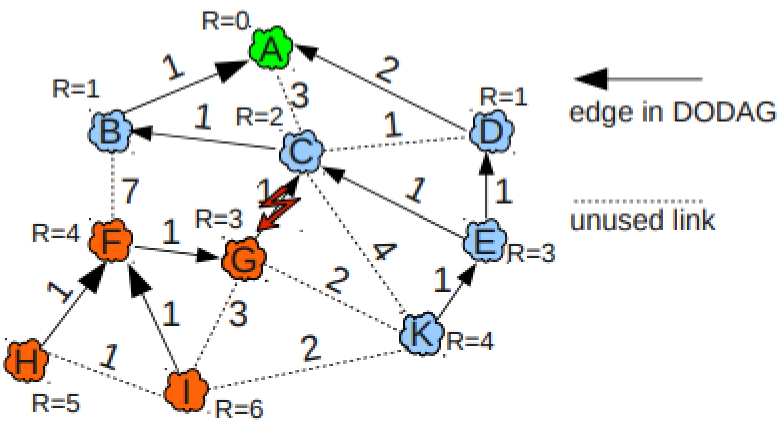


Figure 7

- ➢ Global repair- makes use of DODAG Sequence Numbers
- ➢ Local repair - poison the sub-DODAG by advertising the rank of INFINITY

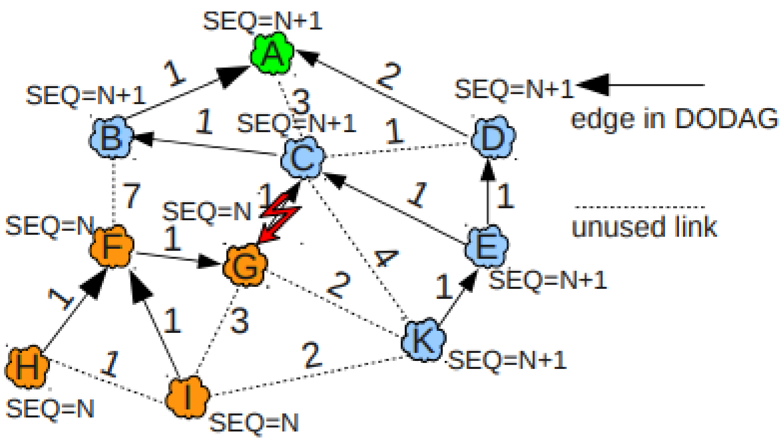


Figure 8

3.10. Conclusion

- LLNs and WSNs are rapidly emerging as a new type of distributed systems.
- RPL was specified and developed in order to overcome these requirements about high delivery ratio and energy efficient at same time.
- RPL also allows optimization of the network for different application scenarios and deployments.

The next chapter is about rpl objective function implementation and study of the RPL performance in different scenarios.

Chapter4

Implementation and analysis of RPL performance

4.1. Introduction

It is necessary to evaluate OFs first, and then evaluate RPL performance in terms of performance metrics for one preferred OF. As a result we need to implement a Cooja simulation experiment in order to fill the lack of the work statement:

We have used a Cooja simulator in our implementation. Cooja is a flexible java-based simulator which supports C program language as the software design language by using Java Native Interface. We have chosen a Cooja simulator as it is a very useful tool for software development in wireless sensor networks, and will provide a suitable method in which to set the environment needs. In this study we

4.2. Contiki Operating System

Contiki is a wireless sensor network operating system and consists of the kernel, libraries, the program loader, and a set of processes. It is used in networked embedded systems and smart objects.

Contiki provides mechanisms that assist in programming the smart object applications. It provides libraries for memory allocation, linked list manipulation and communication abstractions. It is the first operating system that provided IP communication. It is developed in C, all its applications are also developed in C programming language, and therefore it is highly portable to different architectures like Texas Instruments MSP430, and currently Contiki 2.7 to ST microelectronics STM32 families.

Contiki is an event-driven system in which processes are implemented as event handlers that run to completion. A Contiki system is partitioned into two parts: the core and the loaded programs. The core consists of the Contiki kernel, the program loader, the language run-time, and a communication stack with device drivers for the communication hardware. (32)

4.3. Cooja simulator

Cooja is a Java-based simulator designed for simulating sensor networks running the Contiki sensor network operating system. The simulator is implemented in Java but allows sensor node software to be written in C.

One of the differentiating features is that Cooja allows for simultaneous simulations at three different levels: Network Level, Operating System Level and Machine code instruction level. Cooja can also run Contiki programs either compiled natively on the host CPU or compiled for device emulator.

In Cooja all the interactions with the simulated nodes are performed via plugins like Simulation Visualizer, Timeline, and Radio logger. It stores the simulation in an xml file with extension 'csc' (Cooja simulation Configuration). This file contains information about the simulation environment, plugins, the nodes and its positions, random seed and radio medium etc (33).

4.4. RPL implementation

In this study we have simulated a network with a single server node, and we have used Random and linear topology in order to distribute nodes in a squared area with a side L= 1000 meters, with the server placed at the center. We have designed RPL network using OF0 and MRHOF by setting the experiments under different light densities: RPL network containing (20, 30, 40, and 50 nodes) including the server node. Also, we varied the RX values (20, 40, 60, 80, and 100%) and investigated the RPL behavior in terms of packet delivery ratio and power consumption. The main default RPL parameters used in the simulations are listed in Tab. 2

Table 2 simulation parameters

Parameters	Value
OF	OF0, MRHOF
TX Ratio	100%
TX Range	100m
RX Ratio	20-40-60-80-100%
Topologies	Random, linear
Simulation Time	1800 second
squared area	1000 meters

4.5. OBJECTIVE FUNCTION

RPL uses OF to construct the DODAG. OF is also used to define the rank of a node, which is a node's distance from a DODAG root node. RPL determines the whole topology by building the DODAGs within instances, where each instance is associated with a specific OF. OF combines the metrics and constraints to find the best path. However, RPL's main specification has no default OF. Therefore, OF0 is designed as a default function that is common to all implementations and provides interoperability between different implementations.

4.6. PERFORMANCE METRICS

We have used two standard performance metrics: Packet Delivery Ratio (PDR) and power consumption, to evaluate the performance of RPL. The first metric performance is packet delivery ratio (PDR). which is defined as the Rtio of number of packets delivered in total to the total number of packets sent from source node to destination node in the network . We have averaged PDR of all the packets received successfully at the node. In order to compute the average PDR, we have measured the number of successfully received packets at the server and divide it by the number of sent packets from all the nodes to the sink. The second metric is Energy Consumption: To compute the power consumption, we use the mechanism of Power-trace system available in Contiki. Using power state tracking, Power-trace provides an estimation for a system's power usage. Structures known as energy capsule. the power consumption indicates the energy measured from nodes in the network over the network lifetime. it's the sum of power used in each node on the network. There are four types in power measurement: low power mode (LPM), CPU power, radio listen, and radio transmit. Power consumption is a total of all calculation off all type above. LPM is a power consumption parameter that indicates the power used when in sleep condition CPU power is a power parameter that indicates the level of node processing. While radio listen and transmit is parameter related with node communication (transmit and receive). The formula used to calculate the energy of nodes according to the following equation

4.7. NETWORK TOPOLOGIES

4.7.1. RANDOM TOPOLOGY

We have used Random topology in our experiments, as show in Fig.9, it is a distribution node in randomly forms that allow nodes to reach the server directly or contact each other in order to reach the server, especial nodes in the edges. However, many ‘real world’ applications use this type of topology. Such applications use wireless sensors that are dispersed or scattered in a specific areas of interest with the purpose of gathering data from that environment. This topology consists of two types of node, the node number 1 with the blue colour is representative of the server node. The non-sink (client) nodes have been placed randomly in the limited area consists 1000 meter. These nodes are yellow coloured and are representative of client nodes in our experiments.

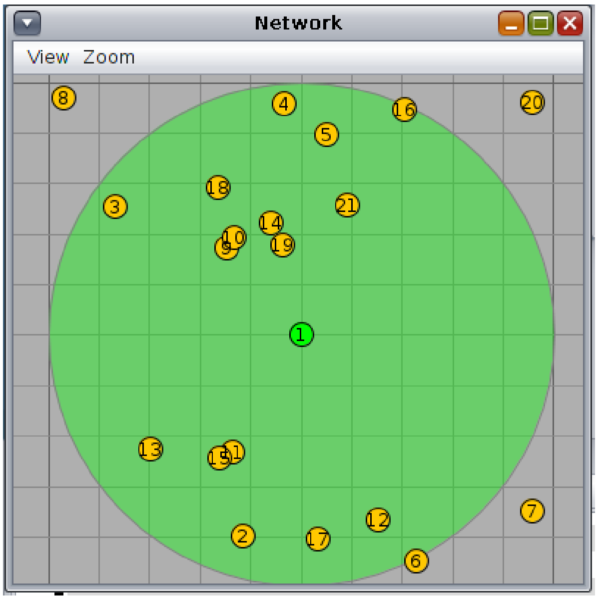


Figure 9 RANDOM TOPOLOGY

4.7.2. LINEAR TOPOLOGY

We have used the linear topologies show in Fig. 10, it is a distribution nodes in forms that allow nodes to contact each other in order to reach the server, especial nodes in the edges. This topology consists of two types of node, node number one is colored green and represents the server node.. The non-sink (client) nodes are yellow colored and have ordered methodically around the server. However the topologies differ based on the number of nodes. We can see from Fig. 10a: that the distance between any two nodes is 20m, in this case we have distributed 20 nodes. The distance changed if we distributed a different quantity of nodes

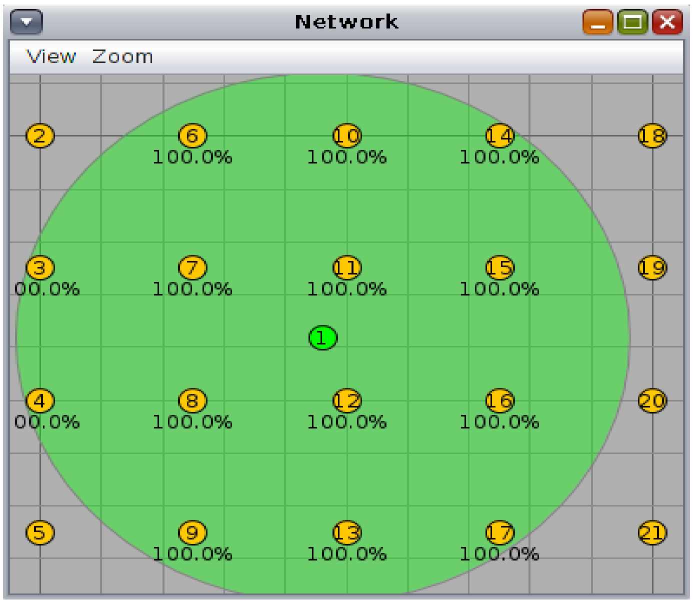


Figure 10 LINEAR TOPOLOGY

4.8.. RPL performance implementation relay on mrhof

We have set the experiments under different network densities (20, 30, 40, and 50 nodes) using Random and linear topologies so to observe the performance of MRHOF for different values of RX. We vary the RX values (20, 40, 60, 80, and 100%) and investigate the RPL behaviour in terms of packet delivery ratio and power consumption.

- Values of PDR under different values of RX using random topology:

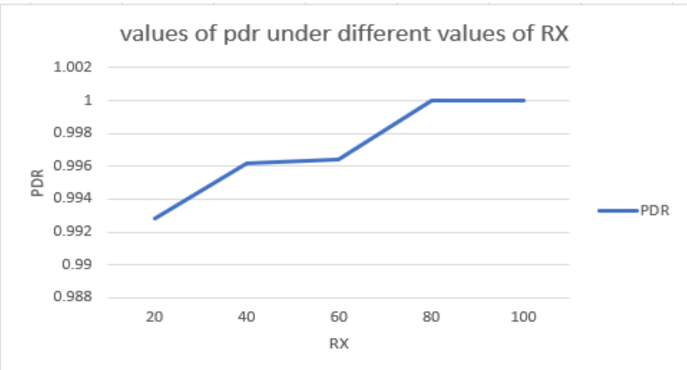


Fig.1: PDR under different values of RX Using Random topology When N=20

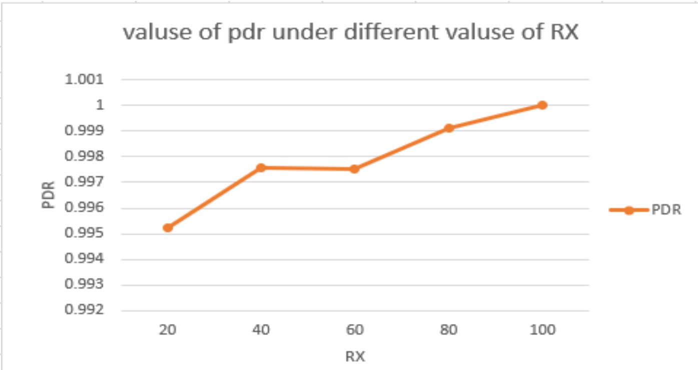


Fig.2: PDR under different values of RX Using Random topology when N=30

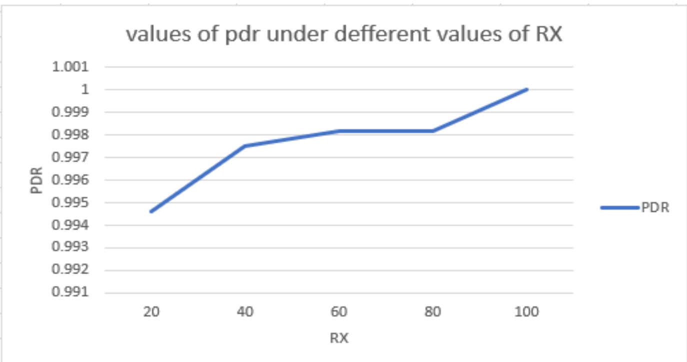


Fig.3: PDR under different values of RX Using Random topology When N=40

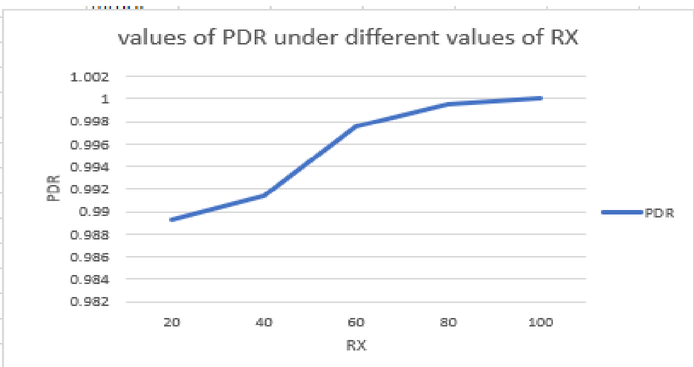


Fig.4: PDR under different values of RX Using Random topology when N=

Figure 11 Values of PDR under different values of RX using random topology

- Values of PDR under different values of RX using linear topology:

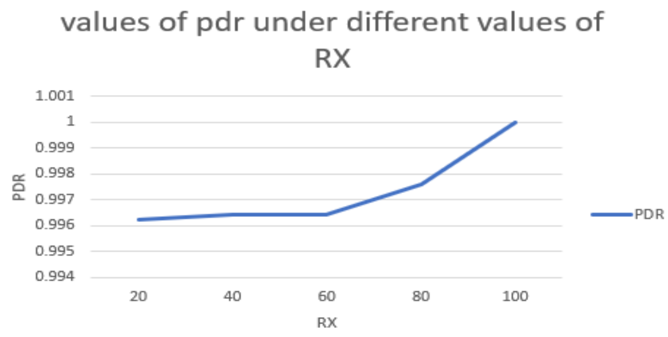


Fig.5:PDR under different values of RX Using linear topology when N=20

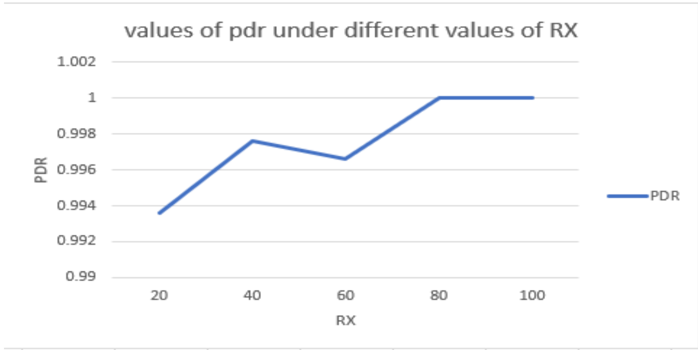


fig.6:Pdr under different of RX using linear topology when N=3

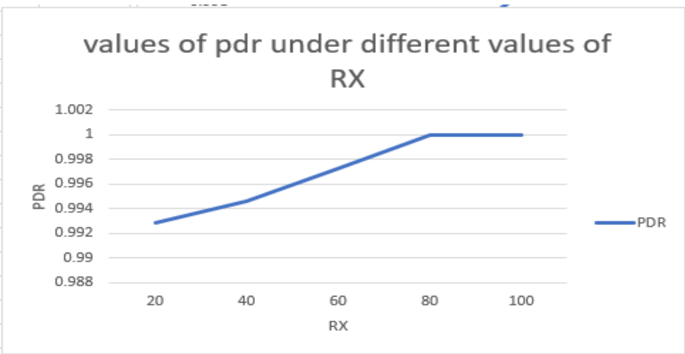


Fig.7: pdr under different values of RX using Linear topology when N=40

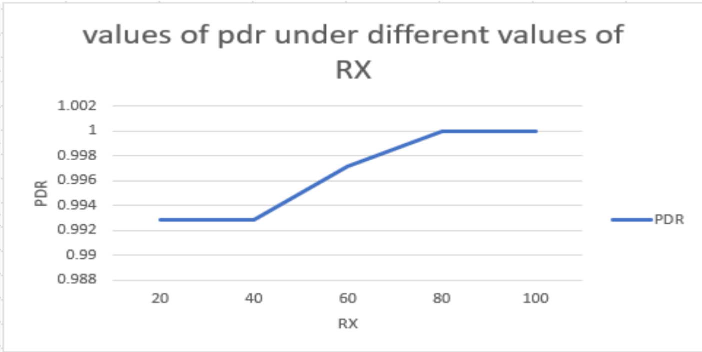


fig.8: pdr under different values of RX using linear topology when N=50

Figure 12 Values of PDR under different values of RX using linear topology

- **Performance analysis of packet delivery ratio.**

Fig. 1-4 show the performance of the PDR based on varied RX values when using Random topology. The PDR values increased as the RX values increased. besaid, we noticed that the PDR value reached 100% when RX is greater than or equal to 60%, meaning that we can use the value of RX= 60% instead of 100%. RPL provides a Poor Packet Delivery ratio of around 93% when RX is lower than 60% from the nodes installed MRHOF. We also observed that PDR increased from (60-100). A similar result of PDR was achieved when using linear topology in Fig.5-8.

- **Values of power consumption under different values of RX using random topology:**

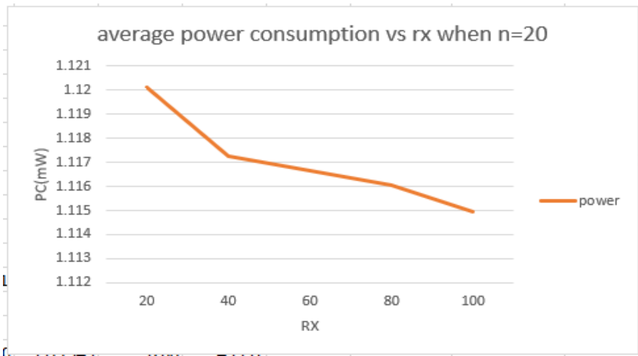


Fig.9 : Power under different RX when N=20

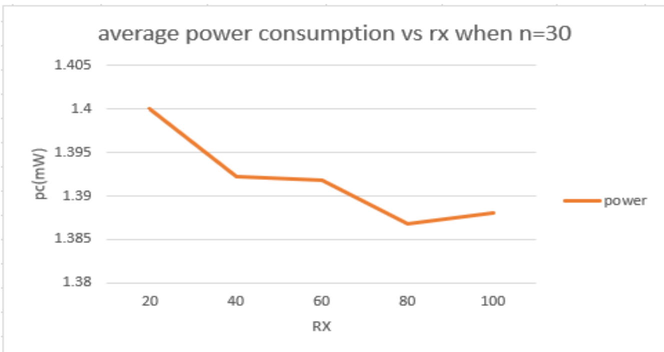


Fig.10 : Power under different RX when N=30

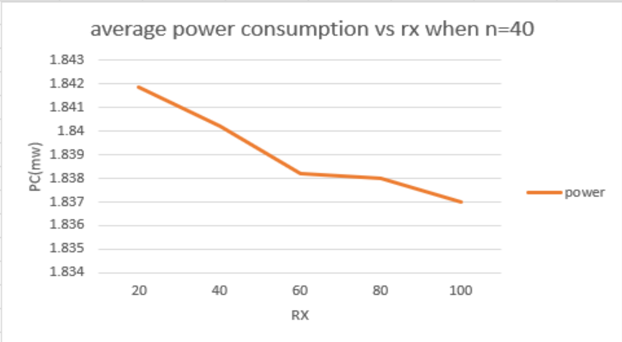


Fig.11 : Power under different RX when N=40

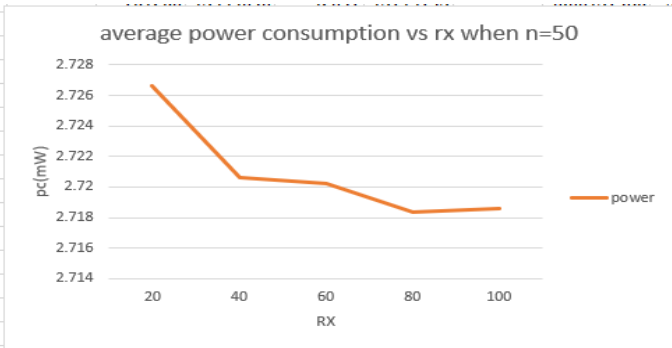


Fig.12 :Power under different RX when N=50

Figure 13 ***Values of power consumption under different values of RX using random topology***

- **Values of power consumption under different values of RX using linear topology:**

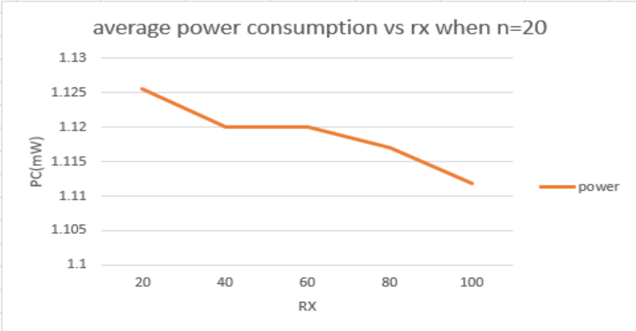


Fig.13 :Power under different RX when N=20

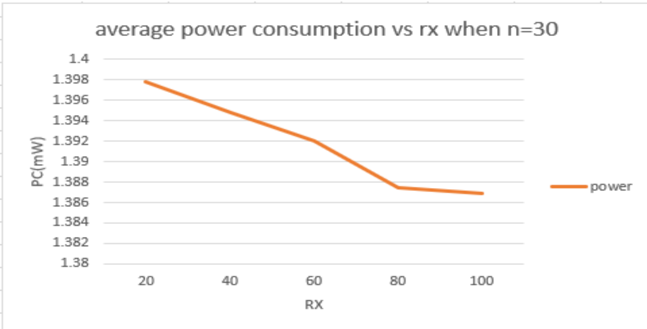


Fig.14 : Power under different RX when N=30

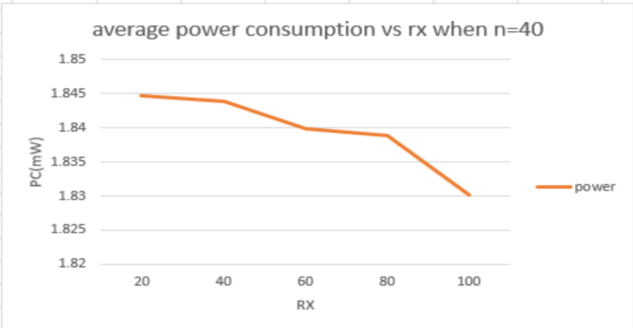


Fig.15 :Power under different RX when N=40

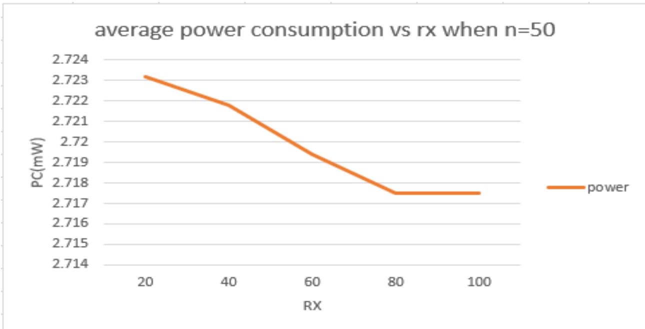


Fig.16 :power under different RX when N=50

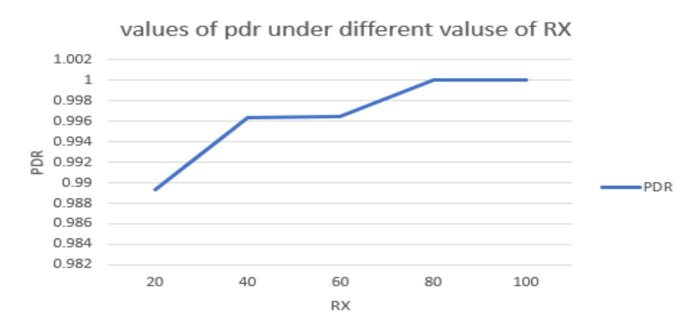
Figure 14 ***Values of power consumption under different values of RX using linear topology***

- **Performance analysis of power consumption**

Fig9_12. show the behavior of the power consumption based on varied RX values first for random topology, we noticed that The power consumption values decreased as the RX values increased. Moreover, we observed that the average power consumption value is fair when RX is greater than or equal to 60%. So that its ranging from 1.12mW to 2.7mW. However, in Fig.13_16, RPL provides a similar average power consumption ratio for linear topology. The reason for this is that the value of RX is not sensed after 60% which is sufficient to reduce the power consumption while deliver the required frequent messages of the LLN.

4.9. RPL PERFORMANCE IMPLEMENTATION RELY ON OF0.

- Values of PDR under different values of RX using random topology:



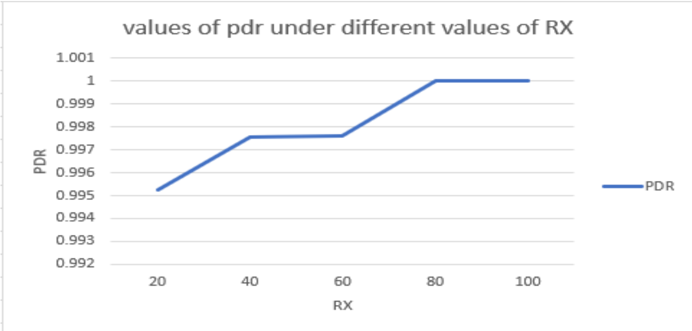
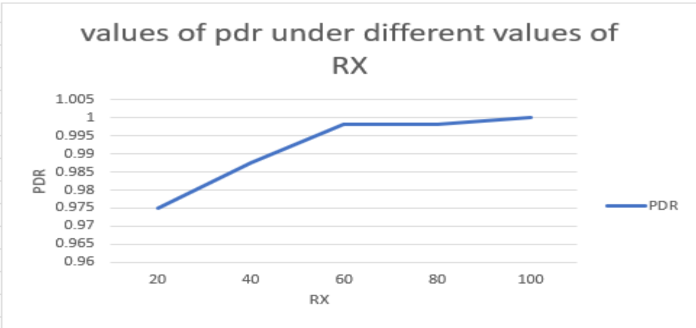


Fig.17 :pdr uder different values of RX using Random topology when N=20

fig.18: pdr under different values of RX using random topology when N=30



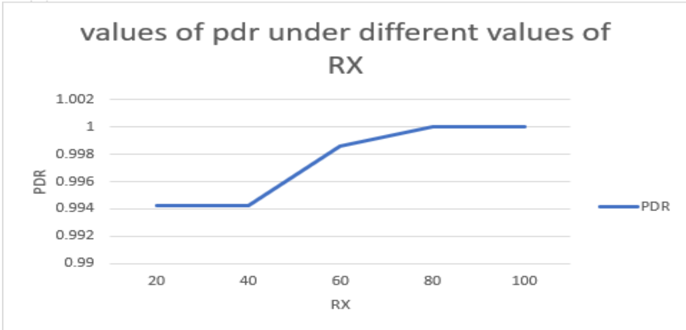
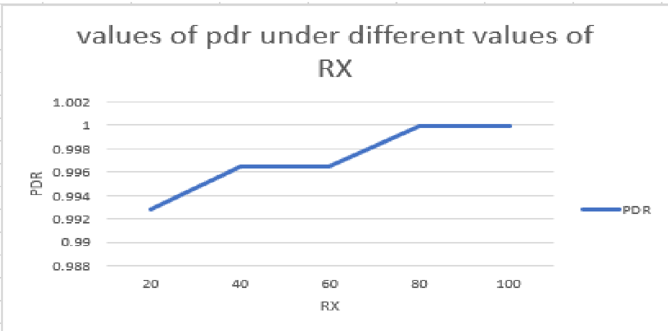


Fig.19:pdr under different values of RX using Random topology when N=40

fig20: pdr under different values of RX using random topology when N=50

Figure 15 pdr under different values of RX using Random topology

- Values of PDR under different values of RX using linear topology:



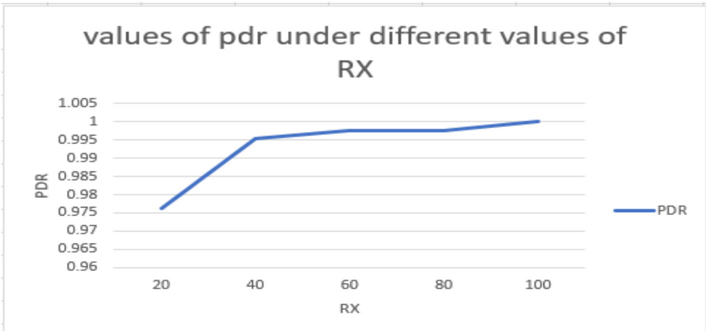
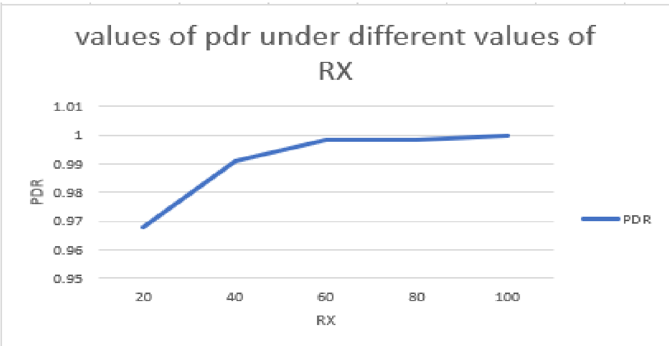


Fig.21:PDR under different values of RX using linear Topology when N=20

Fig.22:PDR under different value of RX using linear topology when N=30



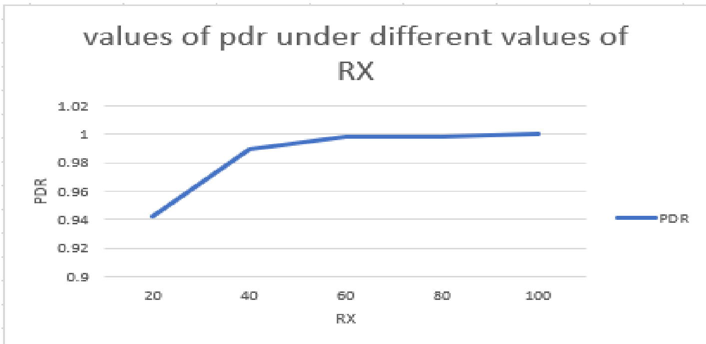


Fig.23 :PDR under different values of RX using linear Topology when N=40

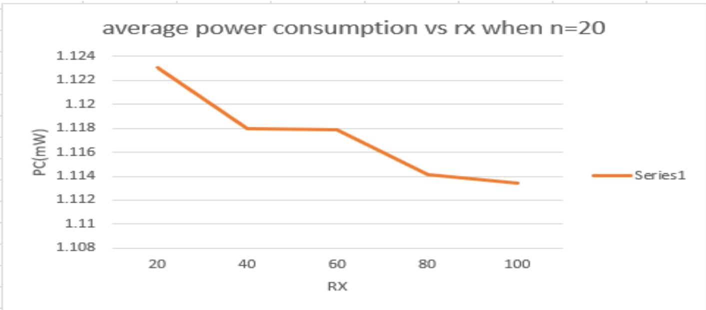
Fig.24:PDR under different values of RX using linear topology when N=50

Figure 16 pdr under different values of RX using linear topology

- **Performance analysis of packet delivery ratio.**

Fig.17_20 show the performance of the PDR based on varied RX values when using Random topology. The PDR values increased as the RX values increased. also, we have noticed that the PDR value approaching 100% when RX values was greater than or equal to 60%. that means we can use the value of RX= 60% instead of 100% because RPL provides a good Packet Delivery ratio of more than 99% when RX is equal or higher than 60. The main reason for that is the value of RX is not sensed after 60 which is enough to deliver the frequent messages of the LLN. RPL provides a Poor Packet Delivery ratio of around 94% when RX lower than 60% from the nodes installed OF0. Fig.21_24, show similar behavior of the PDR based on varies RX levels when using linear topology.

- **Values of power consumption under different values of RX using random topology:**



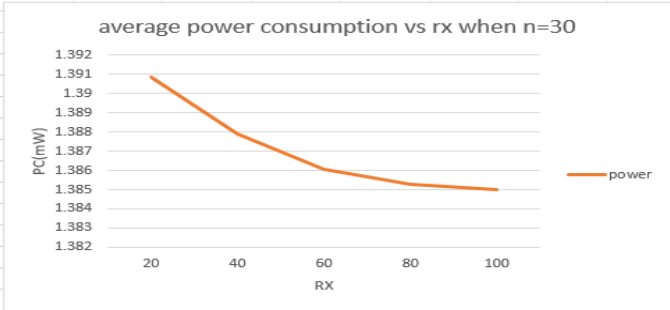
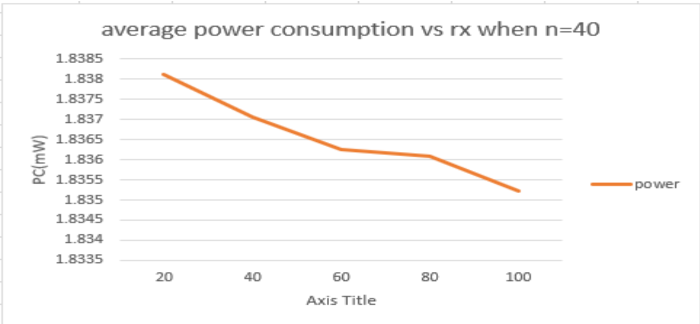


Fig. 25:Power under different RX when N=20

Fig. 26:Power under different RX when N=30



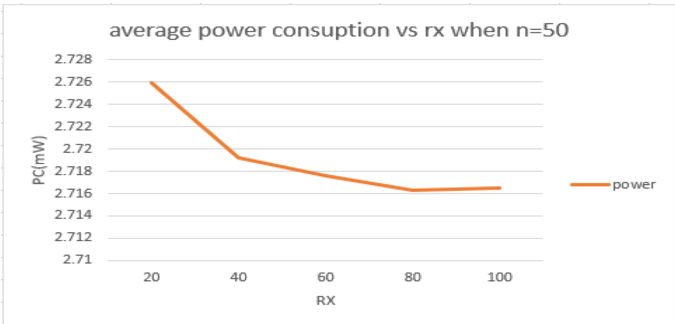
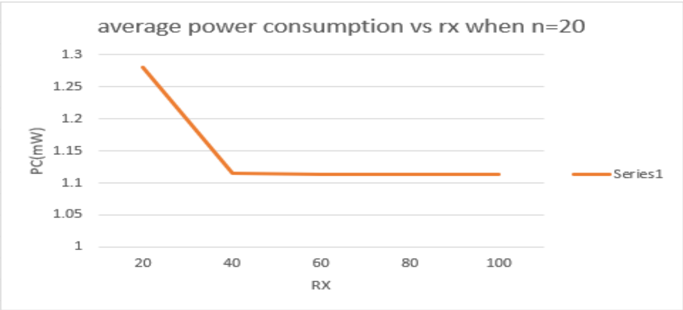


Fig.27 :Power under different RX when N=40

Fig. 28:Power under different RX when N=50

Figure 17 ***Values of power consumption under different values of RX using random topology***

- Values of power consumption under different values of RX using linear topology:



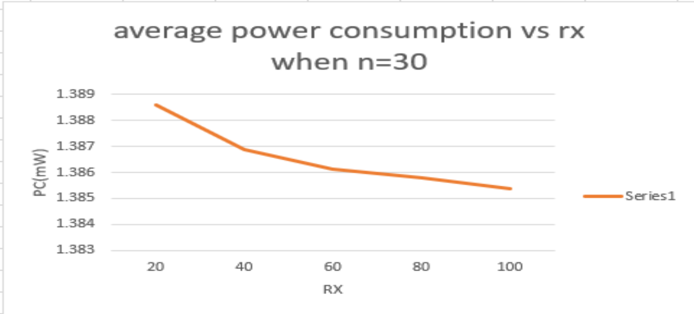
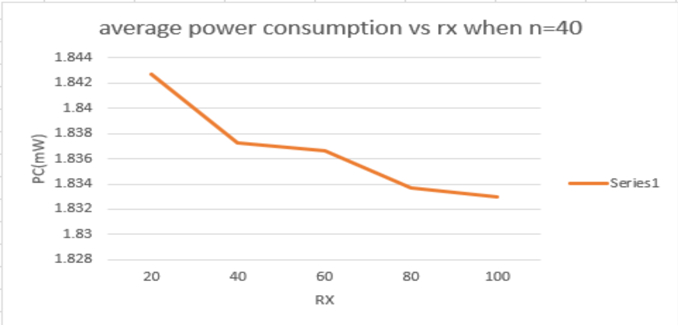


Fig. 29:Power under different RX when N=20

Fig. 30:Power under different RX when N=30



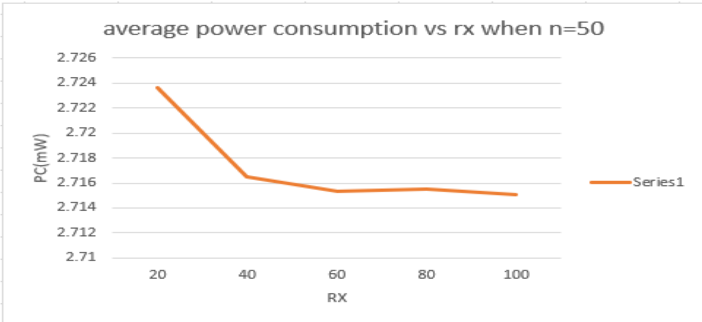


Fig. 31:Power under different RX when N=40

Fig. 32:Power under different RX when N=50

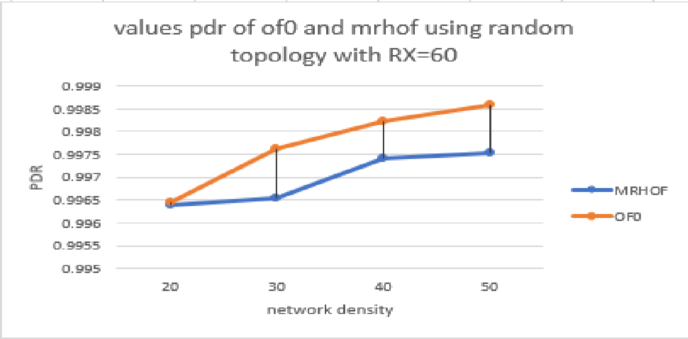
Figure 18 Values of power consumption under different values of RX using linear topology

- **Performance analysis of power consumption**

Fig.25_28 show the behavior of the power consumption based on varied RX values first for random topology, we noticed that The power consumption values decreased as the RX values increased. Moreover, we observed that the average power consumption value is fair when RX is greater than or equal to 60%. So that its ranging from 1.2mW to 2.7mW. However, in Fig.29_32, RPL provides a similar average power consumption ratio for linear topology. The reason for this is that the value of RX is not sensed after 60% which is sufficient to reduce the power consumption while deliver the required frequent messages of the LLN

4.10. IMPACT OF RX ON RPL PERFORMANCE RELIANCE ON OF0 AND MRHOF.

By keeping the node packet reception ratio constant under RX=60, we have come out with a useful result of this simulation which is achieved from the nodes that have installed OF0 or MRHOF by using a different number of nodes, we can obtain deferent topologies that have given us the chance to observe the OFs under multiple network densities. Therefore, we have thoroughly compared the main effects of using OF0 and MRHOF to evaluate the performance of RPL through computing the PDR and Power consumption for each of those topologies and different scenarios.



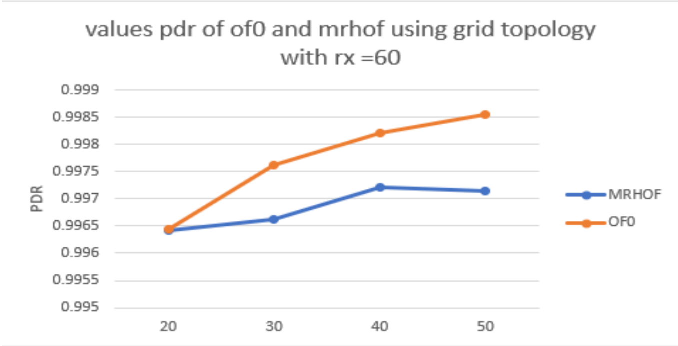


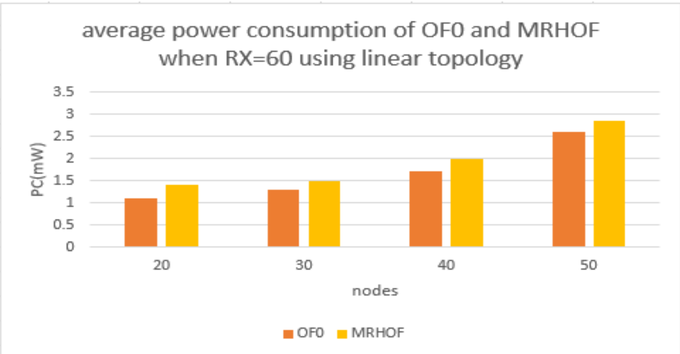
Fig.33:PDR of OF0 and MRHOF using random topology

Fig.34:PDR of OF0 and MRHOF using linear topology

Figure 19 pdr of0 and mrhof using random topology

- **Performance analysis of packet deliver ratio reliance on OF0 and MRHOF.**

In Fig.33a random topology was used and found that the average packet deliver ratio of OF0 is almost 0.98%, and that the average packet deliver ratio of MRHOF is almost 0.97%. In Fig.34 we have used linear topology to represent the average packet deliver ratio, and the results show similar behaviour, where average packet deliver ratio of OF0 is close to 0.98% and the average packet deliver ratio of MRHOF is close to 0.97%. the PDR simulation results observed that both oh the OFs (OF0 and MRHOF) have given a good PDR where OF0 outperforms MRHOF. This is due to a simple difference in the light density network that we used. In these results, we observed in the network configured by 20-50 nodes that the average PDR is best when the network density is between 30- 40 nodes for RX= 60 using Random or linear topology. and we found that the RPL produces similar behaviour of PDR for both OFs in this network density.



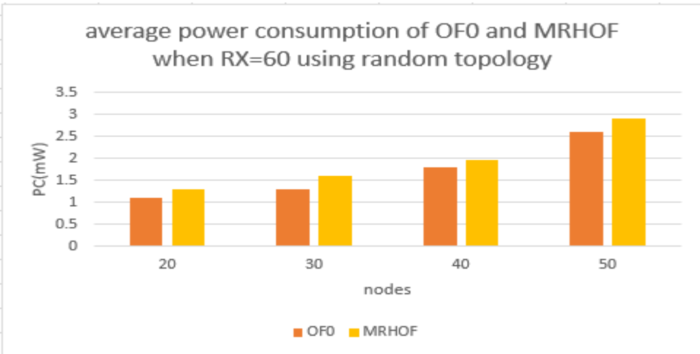


Fig.35:Power of OF0 and MRHOF using linear topology

Fig.36:Power of OF0 and MRHOF using random topology

Figure 20 21 pdr of0 and mrhof using linear topology

- **Performance analysis of power consumption reliance on OF0 and MRHOF.**

according to Fig.35_36 , we can observe that both topologies, OF0 perform better than MRHOF in term of power consumption and the reason for that the MRHOF prefer long paths with more stable link qualities than short paths with poor link qualities which leads more nodes in the routing of a packet and results of higher power consumption for transmission radio. in addition to that OF0 is based on minimizing the number of hops to the root which leads to less retransmition of packets hop by hop and less usage of radio.

and we notice that when the power consumption increases, Because of the increase in the transmission and reception of packets, that is, the increase in traffic, and therefore, a large number of nodes will run out of energy and the remaining energy for them will become less than the threshold, and this requires For the network to perform a repair mechanism in order to re-select the appropriate father and broadcast control messages again to build the network, which increases power consumption.

GENERAL CONCLUSION

GENERAL CONCLUSION

Wireless sensor Networks have crucial constraints like low computing performance, memory and energy in these devices which make the routing in these kinds of networks more rigid, that's why the routing protocol must have the best performances.

In our work, we evaluated the two objectives functions MRHOF and OF0 of RPL in two topologies under different parameters and constraints which allowed us to see that OF0 perform better than MRHOF in term of packet deliver ratio and power consumption. Also, we have shown that the RPL performance for both OFs is best in relation to PDR and power consumption when the values of RX range between 60% and 100% for the majority of circumstances. Where the PDR average when using RX 60% is quite similar to that when using RX 100%. We have also observed that the RPL performance is best for both OFs when the network density is between 30-40 nodes for RX 60% using random or linear topology.

Finally, we can conclude that for applications that monitor a small area, we must choose OF0 as an objective function for RPL.

So as a future work, we prospect to design a new objective function to minimize more the power consumption of the network thus extend the lifetime of the network.

Bibliography

1. **[En ligne] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.**

2. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjFr4C31ZrxAhWwzIUKHQ1QDHwQFjAAegQIBBAD&url=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F339703110_The_Internet_of_Things_IoT_Routing_Security-A_Study&usg=AOvVaw.

3. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjujMf81ZrxAhUQrxoKHRIDCEoQFjAAegQICBAD&url=https%3A%2F%2Fwww.ietf.org%2F&usg=AOvVaw0mIp56XXWfZx5c4RqY7a4I.

4. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjerLuv1prxAhUmzYUKHR_tCzcQFjABegQIAxAD&url=http%3A%2F%2Fwww.cse.chalmers.se%2Fedu%2Fcourse%2FDAT300%2FPAPERS%2Frpl.pdf&usg=AOvVaw2DAfe3gKHuzv2QBl_N9zb8.

5. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi0-cfe1prxAhVQz4UKHZ9kD_0QFjAAegQIAhAD&url=https%3A%2F%2Ftools.ietf.org%2Fhtml%2Frfc6550&usg=AOvVaw1WY6vuNYFfOz0rrPw3Ta9z.

6. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiH3_PX0prxAhUR2BoKHaSaA1wQFjAKegQIFBAD&url=https%3A%2F%2Fwww.zdnet.com%2Farticle%2Fwhat-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now%.

7. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj9iaHb2JrxAhWOzIUKHfHkBPgQFjABegQIBBAD&url=https%3A%2F%2Flink.springer.com%2Fcontent%2Fpdf%2F10.1007%2Fs11390-011-1189-5.pdf&usg=AOvVaw1-LWGKbHtaI_dTA8o_ZqoU.

8. [En ligne] https://www.google.com/imgres?imgurl=https%3A%2F%2Fd3i71xaburhd42.cloudfront.net%2Ff087d32d895b8d54c0458a887f7dc569c4d4c86f%2F4-Figure3-1.png&imgrefurl=https%3A%2F%2Fwww.semanticscholar.org%2Fpaper%2FIoT-Elements%252C-Layered-Architectures-and-Security-A-.

9. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiwseGc2prxAhXyxoUKHTmhBIcQFjACegQIAxAD&url=https%3A%2F%2Fwww.scnsoft.com%2Fservices%2Fiot&usg=AOvVaw2gTrVc9puE4M_6fOXGHGO9.

10. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwigoenG2prxAhUuz4UKHX8lBb4QFjAHegQIAxAD&url=https%3A%2F%2Fwww.digi.com%2Fblog%2Fpost%2Fthe-4-stages-of-iot-architecture&usg=AOvVaw3c0Jwt09mtlqfXZ-cJVP7N.

11. [En ligne] https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQ0vBjAA3oO5Os8LERQqlfzCHZQdJVNCCJAMg&usqp=CAU.

12. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiVlJj-

2prxAhVixoUKHeTjAvkQgQN6BAgBEAE&url=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3D.%2509Wireless%2Bsensor%2Bnetworks%2B(WSN)%26hl%3Den%26as_sdt%3D0%26as_vis%3.

13. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwia9aqf25rxAhUP14UKHbboCeAQgQN6BAgBEAE&url=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3DWireless%2Bmesh%2Bnetworks%2B(wmn)%26hl%3Den%26as_sdt%3D0%26as_vis%3D1%26oi%.

14. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjr_eDD25rxAhXxx4UKHeIYCYYQFjAJegQICxAD&url=https%3A%2F%2Finternetofthingswiki.com%2Fiot-applications-examples%2F541%2F&usg=AOvVaw00bBsxPbpdPQ42gaOaajIR.

15. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi_05_r25rxAhVBVhoKHWDzCqAQFjAAegQIAhAD&url=https%3A%2F%2Fsymfony.com%2Fdoc%2F2.2%2Fbook%2Frouting.html&usg=AOvVaw3KIQJth-2M4C4y5BwzhGrm.

16. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiY_v6J3JrxAhUGCRoKHSg8Di4QgQN6BAgBEAE&url=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3DRouting%2BProtocol%2BMetrics%26hl%3Den%26as_sdt%3D0%26as_vis%3D1%26oi%3Dscho.

17. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwip_cil3JrxAhWK3YUKHRQlDA4QgQN6BAgBEAE&url=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3DProactive%2BRouting%2Bprotocols%26hl%3Den%26as_sdt%3D0%26as_vis%3D1%26oi%3Ds.

18. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwibkcW73JrxAhUM1xoKHZYYC7EQgQN6BAgBEAE&url=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3DReactive%2BRouting%2BProtocol%26hl%3Den%26as_sdt%3D0%26as_vis%3D1%26oi%3Dsch.

19. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiJmo_w3JrxAhUBz4UKHWdEBvwQgQN6BAgBEAE&url=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3Drouting%2Bprotocol%2Blow%2Bpower%2Blossy%2Bnetworks%26hl%3Den%26as_sdt%3D0%2.

20. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiMp72J3ZrxAhXIzoUKHTsdD8QQgQN6BAgBEAE&url=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3Drouting%2Bprotocol%2Blow%2Bpower%2Blossy%2Bnetworks%2BEnhancements%26hl%3Den.

21. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi21Lee3ZrxAhUJ3hoKHQHLBZoQFjABegQIAxAE&url=http%3A%2F%2Fieeexplore.ieee.org%2Fabstract%2Fdocument%2F6857431%2F&usg=AOvVaw2EkPXWUJB4ujr5ypcVJFUe.

22. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjlgpy33ZrxAhVN14UKHcyLCoIQgQN6BAgBEAE&url=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fq%3DChannel-Aware%2BRouting%2BProtocol%26hl%3Den%26as_sdt%3D0%26as_vis%3D1%26oi%.

23. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiylIDM3Z

rxAhUK8BoKHaQuACwQFjABegQIAhAD&url=https%3A%2F%2Fhal.archives-ouvertes.fr%2Fhal-02263388%2Ffile%2F2013-ICWiSE-Evaluation-of-Routing-Protocol-for-Low-Power-and.

24. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjHsNHz3ZrxAhWnyoUKHcJMArwQFjAAegQIAhAD&url=https%3A%2F%2Ftools.ietf.org%2Fid%2Fdraft-ietf-roll-rpl-13.html&usg=AOvVaw2NwrVUrNZN8-L407zDqtPf.

25. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjXydeM3prxAhUkzIUKHaYmD_kQFjABegQIAhAD&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FRPL_(IPv6_Routing_Protocol_for_LLNs)&usg=AOvVaw0-ir5waChvuan7uxmIyoeq.

26. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjogp_I3prxAhUPrxoKHXTICV0QFjABegQIAhAD&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FControl_message&usg=AOvVaw11qDIiQrhhtVorWa2MbBtJ.

27. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiMpZL93prxAhUuyYUKHeZfAH4QFjAAegQIAhAD&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FMetrics_(networking)&usg=AOvVaw0QPZYy_3C-IwrlIi2GSnXg.

28. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjxgI-f35rxAhWsxIUKHYRwDuQQFjAOegQIHBAD&url=https%3A%2F%2Fdotnettutorials.net%2Flesson%2Froute-constraint-asp-dot-net-mvc%2F&usg=AOvVaw1-UXHAdYyBypx-4qcv9pK9.

29. [En ligne] https://www.google.com/imgres?imgurl=https%3A%2F%2Fmedia.springernature.com%2Flw685%2Fspringer-static%2Fimage%2Fart%253A10.1007%252Fs11276-020-02347-7%2FMediaObjects%2F11276_2020_2347_Fig1_HTML.png&imgrefurl=https%3A%2F%2Flink.springer.com%2Farticle%2F10..

30. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjItLTb4JrxAhUN1xoKHVWND3EQFjAHegQIBBAE&url=https%3A%2F%2Ftools.ietf.org%2Fhtml%2Frfc6550&usg=AOvVaw1WY6vuNYFfOz0rrPw3Ta9z.

31. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjijfL_4JrxAhUO2BoKHYdkBWYQFjAAegQIAhAD&url=https%3A%2F%2Flink.springer.com%2Fcontent%2Fpdf%2F10.1007%252F978-3-642-30633-4_8.pdf&usg=AOvVaw1CoZx3hxvQOKvxBhIdKLIU.

32. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjoyKig4ZrxAhWlz4UKHctxBn8QFjAAegQIBBAD&url=http%3A%2F%2Fwww.contiki-os.org%2F&usg=AOvVaw1kQf_ZYjADt420x-dTueF2.

33. [En ligne] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwihjKC_4ZrxAhURx4UKHU1GAwYQFjAAegQIAhAD&url=https%3A%2F%2Fanrg.usc.edu%2Fcontiki%2Findex.php%2FCooja_Simulator&usg=AOvVaw3TdlX-lDSzLsFFkdMpnHkF.

34. [En ligne] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.