PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
Ministry of Higher Education and Scientific Research
Mohamed Khider University - BISKRA
Faculty of Exact Sciences, Natural Sciences and Life

Computer Science department

Order N° :.... RTIC/M2/2020

Memory Thesis

Presented for obtention of master degree in

Computer science

Option: Networks and Technologies of Information and Telecommunications

Secure multipath routing for Low Power and Lossy Networks (LLNs) in IoT contexts

By:

HENNI NABIL

Presented in Date: in front of the jury composed of:

	MCB	President
	MCA	Reporter
	MCB	Examiner

Acknowledgements

First of all, I want to thank my god Allah for giving me the courage and the will to achieve this job.

I would particularly like to thank my supervisor Dr. SAHRAOUI Somia for her motivation, valuable advice and assistance besides the unlimited sharing of her knowledge during the different phases of this thesis.

I sincerely thank the honorable members of the jury who agreed to evaluate my work.

I would not forget to express my appreciation to my dear family for their constant support I would not be here without them.

Finally, special thanks to all my friends and who, in one way or another, contributed to the success of this work and could not be cited here.

Abstract

Routing protocol for low-power and lossy networks (RPL) is the standard IPv6 based routing protocol for low power, lossy Networks (LLNs) proposed by IETF. It is proposed for networks with have special characteristics like small packet size, lossy links, low bandwidth, low data rate and low power resources. RPL is a single path routing protocol and the existing objective functions do not support the creation of multiple routing paths between source and destination. Multipath routing can be adopted to achieve multifold objectives, including higher packet delivery ratio, increased throughput, and fault tolerance. In this work, we highlight the security side of multipath RPL routing over low power, lossy networks. We consider a heterogeneous LLN where packets are routed onto multiple paths through powerful multipath nodes. We evaluate the resiliency of the considered routing scheme against a set of routing attacks. The assessment results show that the solution provides good security levels with the consideration of the multiple constraints of LLNs.

Keyword: LLN, RPL, multipath, security, routing, ipv6, IoT, Cooja, encryption.

ملخص

بروتوكول التوجيه للشبكات منخفضة الطاقة والفاقدية (RPL) هو بروتوكول التوجيه القياسي المستند إلى IPv6 للشبكات منخفضة الطاقة والفاقدية (LLNs) التي اقترحتها IETF. تم اقتراحه للشبكات ذات الخصائص الخاصة مثل حجم الحزمة الصغير ، الروابط المفقودة ، عرض النطاق الترددي المنخفض ، معدل البيانات المنخفض وموارد الطاقة المنخفضة. RPL هو بروتوكول توجيه مسار واحد ولا تدعم وظائف الهدف الحالية إنشاء مسارات توجيه متعددة بين المصدر والوجهة. يمكن اعتماد التوجيه متعدد المسارات لتحقيق أهداف متعددة الجوانب ، بما في ذلك نسبة تسليم حزم أعلى ، وزيادة الإنتاجية ، والتسامح مع الخطأ. في هذا العمل ، نسلط الضوء على الجانب الأمني لتوجيه RPL متعدد المسارات عبر شبكات منخفضة الطاقة وفقدان. نحن نعتبر LLN غير متجانسة حيث يتم توجيه الحزم إلى مسارات متعددة من خلال عقد قوية متعددة المسارات. نقوم بتقييم مرونة مخطط التوجيه المدروس ضد مجموعة من هجمات التوجيه. تظهر نتائج التقييم أن الحل يوفر مستويات أمان جيدة مع مراعاة القيود المتعددة لشبكات LLN.

كلمات البحث :شبكات منخفضة الطاقة والفاقدية ، بروتوكول التوجيه للشبكات منخفضة الطاقة والفاقدية ، متعدد المسارات ، الأمان ، التوجيه ، الإصدار السادس من بروتوكول الإنترنت، انترنت الأشياء ، كوجا ، التشفير.

Table of contents

Chapter 3: Secure routing in IoT-connected LLNs

List of figures

List of tables

Abbreviations

BLE	Bluetooth Low Energy
CoS	Class of Service
CSS	Chirp Spread Spectrum
DAO	Destination Advertisement Object
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DODAG	Destination-Oriented Directed Acyclic Graph Read
EPC	Electronic Product Code
GAF	Geographic Adaptive Fidelity
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
IEEE	The Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
LAN	Local area network
LBR	LLN border routers
LLN	Low Power and Lossy networks
LoRa	Long Range
LR-WPAN	Low-Power Wide-Area Network
LTE	Long-Term Evolution
M2M	Machine to machine
MP2P	Multipoint-to-Point
NFC	Near Field Communication
OF	Objective function
P2MP	Point-to-multipoint
P2P	Point-to-point
PAN	Personal area network
QoS	Quality of service
RFID	Radio Frequency Identification
RPL	Routing protocol for low power and lossy networks
UID	Unique identifier
UWB	Ultra-Wideband
WAN	Wide area network
Wi-Fi	Wireless fidelity
WSN	Wireless sensor networks

General Introduction

Computing and Internet are becoming more and more a necessity for modern life, over time, on a computer integrated into various objects of our daily life. In addition, with the internet, these objects can connect and communicate with each other, developing possibilities for more direct integration of the physical world into computer systems, and resulting in greater efficiency, accuracy, and additional economic benefits, which reduce human intervention. The concept of linking things to the Internet, known today as the "Internet of Things".

Nevertheless, the IOT is still in its infancy, and several progresses remains to be made in the areas of security, optimization of energy consumption, congestion and especially routing where weak connectivity not only leads to loss of data and networks, but also to the emergence of new threats that affect the integrity of objects. This calls for new trends and innovations in terms of routing protocol architectures.

RPL (IPv6 Routing Protocol for Low Power and Lossy Network) is a routing protocol that constructs and maintains DODAGs (Destination Oriented Directed Acyclic Graph) to transmit data from sensors to root over a single path, which cannot be considered as effective techniques due to security vulnerabilities, the unreliability of wireless links besides the resource constraints of sensor nodes. Thus, multipath routing.

This thesis, which aims to provide a secure RPL through multipath, is organized into four chapters:

1. The first chapter will be devoted to the presentation of the IoT, as well as the introduction of some fundamental concepts used in the field of IOT (applications, communication technologies, protocols). Meanwhile, an overview of Low-power and Lossy Network LLNs.

2. In the second chapter, we present one of the most widely used routing protocols in the field of IoT, which is RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks).

3. In the third chapter, we target the issue of routing security by describing a state of the art of the solutions developed to avoid the common vulnerabilities before comparing them.

4.The fourth chapter starts with the overview of our secure RPL by describing our contribution where we define the principle functions of the proposed feature of multipath. Finally, summarizing the results obtained after simulation and discussion of them.

Chapter one:

Presentation of IoT and LLN networks

I. Introduction:

The Internet of things refers to a type of network to connect anything with the Internet based on stipulated protocols through information sensing equipment to conduct information exchange and communications in order to achieve smart recognitions, positioning, tracing, monitoring, and administration. In this chapter, we briefly discussed about what IOT is, how IOT enables different technologies, about its architecture, characteristics & applications, IOT functional view & what are the future challenges for IOT.

Low power and Lossy Networks (LLNs) are networks of embedded devices, such as sensors, that have limited power, memory, and processing capability. These low-cost devices are often battery operated and can only handle limited amounts of data. Due to the embedded nature of these devices, they are subjected to a high variance of environmental factors, interference, and noise. Network protocols must be designed to operate effectively in what is referred to as a "lossy" environment where transmitted messages are often lost.

The growing importance of LLN becomes apparent when you look at how LLN networks will be used. Applications include the Internet of Things (IoT), Machine-to-Machine (M2M) communications, and Smart City. In other words, the number of devices that connect these networks will be in the tens of billions.

II. Internet of things (IoT):

1. Definition:

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

2. Characteristics:

The fundamental characteristics of the IoT are as follows [1, 2]:

Interconnectivity: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

Things-related services: The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

Heterogeneity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

Enormous scale: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet.

Safety: As we gain benefits from the IoT, we must not forget about safety. As both the creators and recipients of the IoT, we must design for safety. This includes the safety of our personal data and the safety of our physical well-being. Securing the endpoints, the networks, and the data moving across all of it means creating a security paradigm that will scale.

Connectivity: Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data.

3. IoT architecture:

IOT architecture consists of different layers of technologies supporting IOT. It serves to illustrate how various technologies relate to each other and to communicate the scalability, modularity and configuration of IOT deployments in different scenarios.

The functionality of each layer is described below [1, 3]:

A. smart device / sensor layer:

The lowest layer is made up of smart objects integrated with sensors. The sensors enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed. There are various types of sensors for different purposes. The sensors have the capacity to take measurements such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity etc. In some cases, they may also have a degree of memory, enabling

them to record a certain number of measurements. A sensor can measure the physical property and convert it into signal that can be understood by an instrument. Sensors are grouped according to their unique purpose such as environmental sensors, body sensors, home appliance sensors and vehicle telematics sensors, etc.

Most sensors require connectivity to the sensor gateways. This can be in the form of a Local Area Network (LAN) such as Ethernet and Wi-Fi connections or Personal Area Network (PAN) such as ZigBee, Bluetooth and Ultra-Wideband (UWB). For sensors that do not require connectivity to sensor aggregators, their connectivity to backend servers/applications can be provided using Wide Area Network (WAN) such as GSM, GPRS and LTE. Sensors that use low power and low data rate connectivity, they typically form networks commonly known as wireless sensor networks (WSNs). WSNs are gaining popularity as they can accommodate far more sensor nodes while retaining adequate battery life and covering large areas.

B. Gateways and Networks

Massive volume of data will be produced by these tiny sensors and this requires a robust and high performance wired or wireless network infrastructure as a transport medium. Current networks, often tied with very different protocols, have been used to support machine-to-machine (M2M) networks and their applications. With demand needed to serve a wider range of IOT services and applications such as high-speed transactional services, context-aware applications, etc., multiple networks with various technologies and access protocols are needed to work with each other in a heterogeneous configuration. These networks can be in the form of a private, public or hybrid models and are built to support the communication requirements for latency, bandwidth or security.

C. Management Service Layer

The management service renders the processing of information possible through analytics, security controls, process modeling and management of devices.

One of the important features of the management service layer is the business and process rule engines. IOT brings connection and interaction of objects and systems together providing information in the form of events or contextual data such as temperature of goods, current location and traffic data. Some of these events require filtering or routing to postprocessing systems such as capturing of periodic sensory data, while others require response to the immediate situations such as reacting to emergencies on patient's health conditions. The rule engines support the formulation of decision logics and trigger interactive and automated processes to enable a more responsive IOT system.

In the area of analytics, various analytics tools are used to extract relevant information from massive amount of raw data and to be processed at a much faster rate. Analytics such as in memory analytics allows large volumes of data to be cached in random access memory (RAM) rather than stored in physical disks. In-memory analytics reduces data query time and augments the speed of decision making. Streaming analytics is another form of analytics where analysis of data, considered as data-in-motion, is required to be carried out in real time so that decisions can be made in a matter of seconds.

Data management is the ability to manage data information flow. With data management in the management service layer, information can be accessed, integrated and controlled. Higher layer applications can be shielded from the need to process unnecessary data and reduce the risk of privacy disclosure of the data source. Data filtering techniques such as data anonymization, data integration and data synchronization, are used to hide the details of the information while providing only essential information that is usable for the relevant applications. With the use of data abstraction, information can be extracted to provide a common business view of data to gain greater agility and reuse across domains. Security must be enforced across the whole dimension of the IOT architecture right from the smart object layer all the way to the application layer. Security of the system prevents system hacking and compromises by unauthorized personnel, thus reducing the possibility of risks.

D. Application Layer

The IoT application covers "smart" environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy.

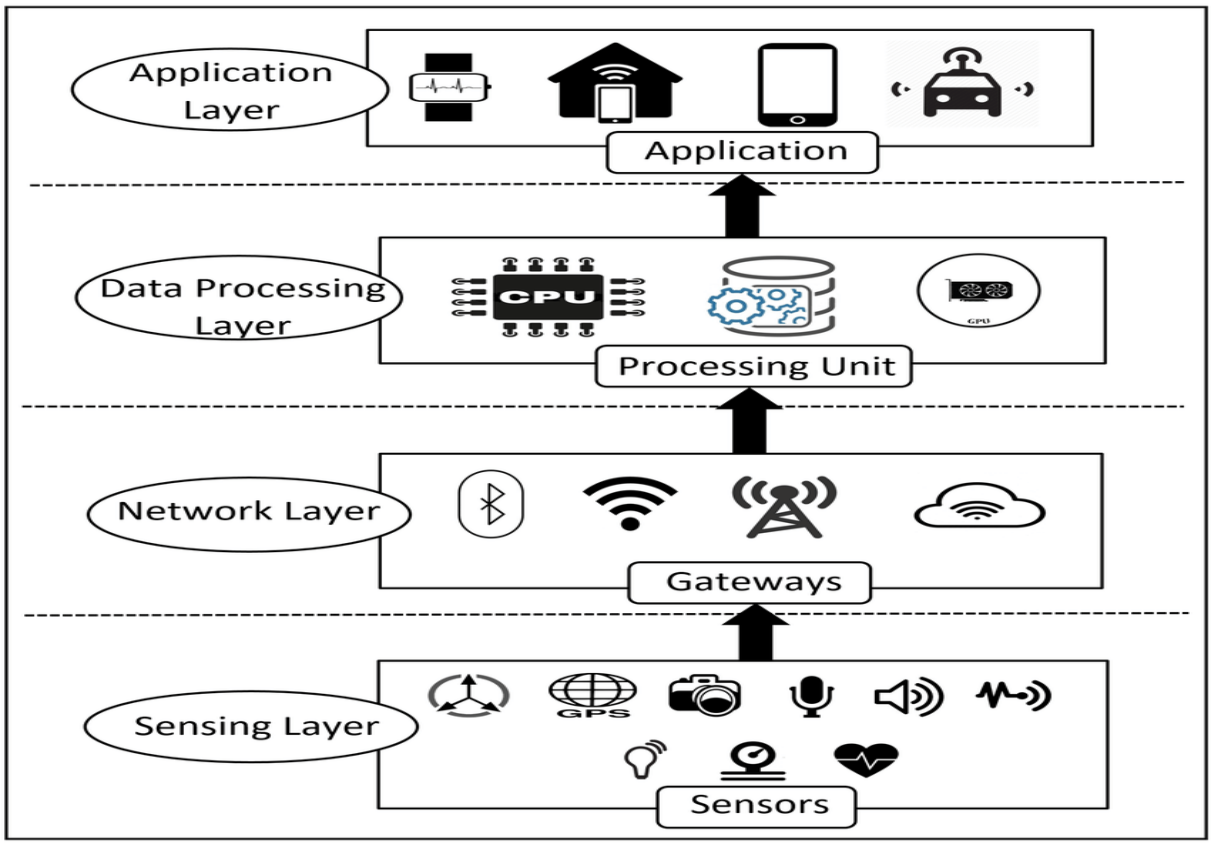

Figure 1. 1 IoT architecture [3]

4. Enabling technologies in IoT:

The term was first mentioned by Kevin Ashton, co-founder of the Auto-ID Center at MIT, with reference to a global standard system for Radio Frequency Identification (RFID) and other sensors were created [7]. Further, the Electronic Product Code (EPC) was developed aiming to spread use of RFID in worldwide networks [8]. Gradual development of wireless communication systems, such as Wi-Fi, Bluetooth, Near Field Communication (NFC), Wireless Sensor Network (WSN), and cellular technologies helped in its evolution. Today, an IoT system consists of a set of smart devices (building blocks), or things, that interact on a collaborative basis to fulfil a common goal [9]. Things collect data from the environment, compute, and integrate seamlessly with the physical world. They must be easily locatable, recognizable, addressable and controllable. Because these things are also interconnected through the internet, an almost endless combination can be devised to create innovative products and services. The evolution of IoT is mainly supported by following technological developments:

● *RFID* tags are intelligent bar codes capable to talk with a networked system to track the objects. Technically speaking, RFID tags are chips with antenna that are typically embedded in objects and containing electronically stored data. For the automatic identification and tracking, RFID uses electromagnetic fields. There are two types of RFID tags, namely passive and active tags. Passive tags transmit data when they collect energy from the

electromagnetic fields of a nearby RFID reader, whereas active tags contain a local power source and can operate at hundreds of meters from RFID readers.

●*Sensor* is a device to convert a physical phenomenon into an electrical signal. It represents part of the interface between the world of electrical devices and the physical world. The other part of this interface is represented by actuators, which convert electrical signals into physical phenomena [10]. For the purposes of IoT, electronic sensors, chemical sensors, and biosensors frequently act as interfaces between the virtual world and the physical world [11]. Sensor data is processed, analyzed, and then provided to the actuators that use this information to influence the physical world environment. The data generated by sensors are transmitted to other electronic devices by a variety of means: wired and wireless, long or short range, high or low power, high or low bandwidth. Ultimately, these collected data are stored in cloud platform for further analysis.

● *NFC*, a Near Field Communication, is a communication technology that enables devices to share information wirelessly by putting them in touch or bringing them into proximity with each other. The NFC is broadly used in applications for sharing personal data (such as contacts, business cards, photos, videos), financial transactions, information access in smart posters, etc. It is considered as an evolution of RFID as it is built upon RFID systems adding the possibility of bidirectional communications. There is still lack of adoption of NFC in M2M communications due to the unwillingness among organizations, such as retailers and public transport companies to provide open access to their respective client base. In such cases, infrastructures are explicitly made incompatible with NFC.

5. Transmission technologies in IOT

There is two type of technology to transmit a data in IOT, which is:

a. Short range technologies:

- **IEEE 802.15.4:** technology specifies physical and media access control (MAC) layers for LR-WPAN (low-rate wireless personal area networks) networks. It is recognized by its low cost and low power consumption which makes it suitable for WSNs. The maximal number of the associated devices may reach 65 000 nodes that can be organized in star, tree, cluster, and mesh network topologies. IEEE 82.15.4 technology allows a maximal throughput of about 250 Kb/s with 127 bytes of MTU (Maximum Transmission Unit). There is also a support for optional security in IEEE 802.15.4 MAC layer using the symmetric block encryption algorithm AES-128 (Advanced Encryption Standard with a 128-bit key).

- **BLE:** Bluetooth Low Energy (BLE), also called smart Bluetooth, is another promising technology that is expected to be an adapted transmission technology for low power networks in IoT contexts. BLE is more efficient than IEEE 802.15.4 in terms of enhanced data throughput and energy reservation. However, the number of connected devices is very limited compared to IEEE 802.15.4. Many research efforts

are actually concentrated around the definition of mesh topology for BLE-operated networks so that to fulfill network scalability requirements.

- **Wi-Fi (IEEE 802.11x) :** is a local wireless networking technology that is largely used by IoT devices in home automation (such as in smart homes), whereas mobile wireless networks are used by IoT for geographically dispersed M2M connectivity. Most commonly, Wi-Fi uses the 2.4 GHz frequency band (UHF) and 5 GHz (ISM radio) band for communication. Recently, the Wi-Fi Alliance introduced Wi-Fi HaLow, an extension for Wi-Fi enabling the low power connectivity required for applications using sensors and wearables, such as Smart homes, connected cars and Smart Cites. Wi-Fi HaLow is based on 802.11ah standard and operates in 900 MHz frequency band.

b. Long range technologies:

New transceiver technologies have emerged which enable power efficient communication over very long distances. Examples of such Low-Power Wide-Area Network (LPWAN) technologies are LoRa, Sigfox.

- **LoRa** (Long Range): is a proprietary spread spectrum modulation technique by Semtech. It is a derivative of Chirp Spread Spectrum (CSS). The LoRa physical layer may be used with any MAC layer; however, LoRaWAN is the currently proposed MAC which operates a network in a simple star topology.
  Using a LoRa radio in a sensor network has some interesting aspects. First, since the range is relatively large (hundreds of meters indoors, kilometers outdoors), networks can span large areas without routing over many hops. In many cases one hop from every node to the sink is feasible. Secondly, transmission on the same carrier frequency, but with different spreading factor, are orthogonal. This creates the opportunity of dividing the channel in virtual subchannels. Thirdly, when transmissions occur at the same time with the same parameters, the strongest transmission will be received with high probability, ie. concurrent transmissions are nondestructive even when their contents is different. This feature is exploited by LoRaWAN where all gateways broadcast beacons at the same time (tight clock synchronization via GPS) and an end device is able to demodulate the strongest beacon.

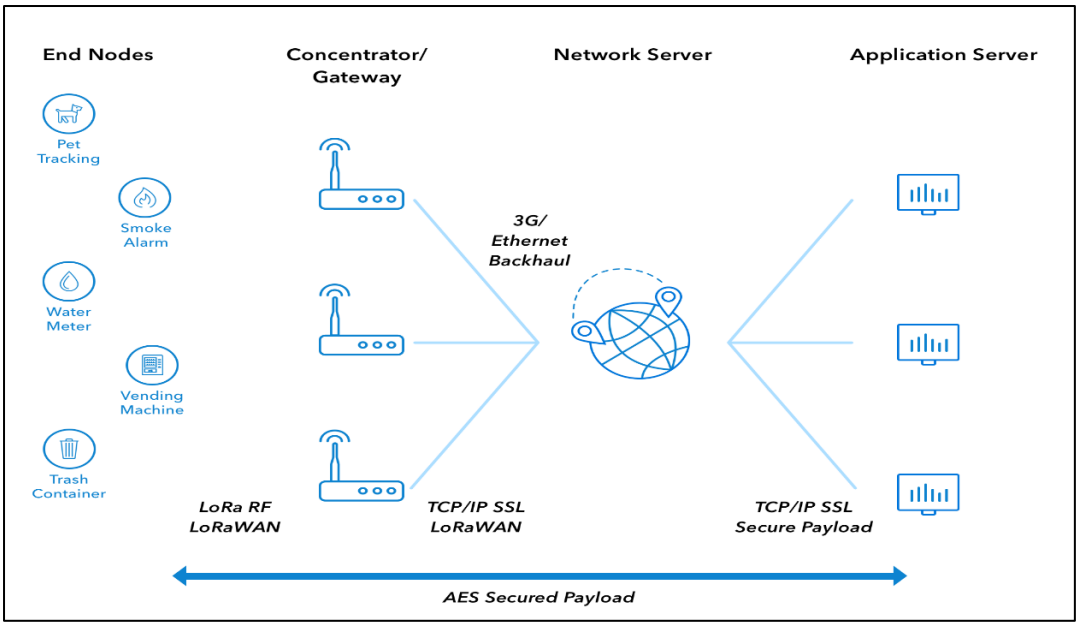

Figure 1.2 LoRaWAN architecture

- **Sigfox:** Sigfox low powered connectivity solutions not only improve existing business cases but also enable a new range of opportunities for businesses across all industries. Sigfox is the first LPWAN Technology ,its physical layer based on an Ultra-Narrow band wireless modulation, it has its proprietary system with low throughput (~100 bps) and low power Extended range (up to 50 km) , 140 messages/day/device ,also it is Subscription-based model , it has its own Cloud platform with and defined API for server access, moreover it offer roaming capability.

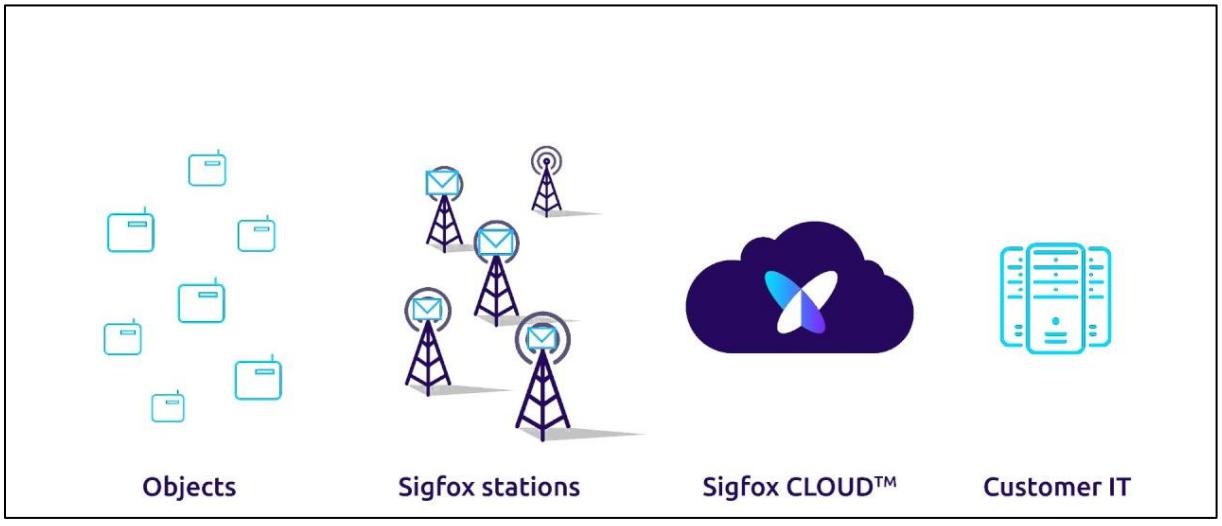

Figure 1. 3 Sigfox network architecture

6. Application domains in IoT:

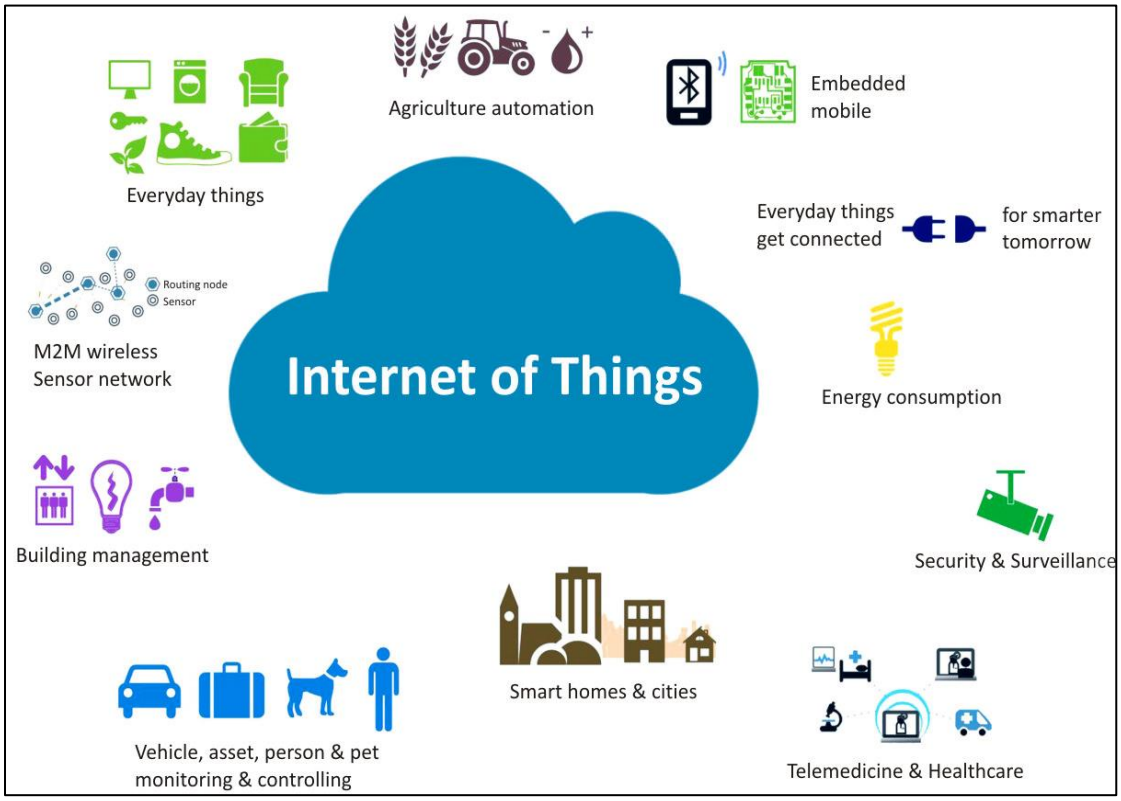

Figure 1. 4 IoT applications

The IoT has huge potential for developing new intelligent applications in nearly every domain, such as personal, social, societal, medical, environmental and logistics aspects [5]. The number of application domains has been also increasing due to its ability to perform contextual sensing. It allows, for instance, to collect information of environment, natural phenomena, medical parameters and user habits and then can offer tailored services based on information received. Such phenomenon should enhance the quality of everyday life, and should have a reflective impact on the society and economy irrespective of the application domain. Globally, various applications domains can be categorized in three major areas: smart city domain, industrial domain, and health and well-being domain. In fact, each domain is partially or completely overlapped but is not isolated from the others since most of the applications are common and share the same resources.

Table 1.1: IoT application domains [5]

Domain	Sub-domain	Examples
Smart Cities	Smart home/ Smart commercial buildings	• Home security system, video surveillance, access management, children protection • Entertainment, comfortable living
	Smart mobility/ transport and smart tourism	• Intelligent transport systems (ITS) - Traffic management, bike/car/ van sharing, multi-modal transport, road condition monitoring, parking system • Connected and automated driving • Automated adaptive traffic control • Payment systems, tour guide services
	Utilities	• Smart grid: power generation, distribution and management • Smart meter, smart water management Sustainable mobility, Storage services
	Public services, safety and environment monitoring	• Public services • Emergency rescue, personal tracking, emergency plan • Video/radar/satellite surveillance • Environmental and territory monitoring
Industrial services	Logistics and product lifetime management	• Smart manufacturing • Identification of material, product, goods or product deterioration • Warehouse, retail and inventory management • Shopping operations and fast payment
	Agriculture and breeding	• Animal tracking, certification, trade control • Farm registration management • Irrigation, monitoring agricultural production and feed
	Industrial processing	• Real-time vehicle diagnostics, assemblage process, assistive driving • Luggage management, boarding operations, mobile tickets • Monitoring industrial plants

Health well-being	Medical and Healthcare	• Medical equipment tracking, secure and access indoor environment management • Smart hospital services, entertainment services • Remote monitoring of medical parameters, diagnostics
	Independent living	• Elderly assistances, disabled assistance • Personal home and mobile assistance, social inclusion • Individual well-being, personal behavior impact on society

7. IoT Use Cases

When devices can sense and communicate via the Internet, they can go beyond local embedded processing to access and take advantage of remote super-computing nodes. This allows a device to run more sophisticated analyses, make complex decisions and respond to local needs quickly, often with no human intervention required. Let's take a look at the most common use cases for the IoT.

- **Asset Tracking:** An extension of these kinds of services is asset tracking, which today is done via barcode and a variety of manual steps, but in the future will leverage smart tags, near-field communication (NFC) and RFID to globally track all kinds of objects, interactively. The word geo-tagged is now being used by some companies to refer to this class of applications. In a future scenario, a user would be able to use Google Earth to track anything with an RFID tag. Alternatively, your refrigerator could keep track of your smart-tagged groceries and tell your cell phone app you are low on a certain item. If your bag of frozen vegetables can have a smart tag, other objects such as valuable cars, jewelry and handbags could too, and they could be tracked via the Internet and also take advantage of a variety of available web-based applications. Some telehealth-related services also belong in this category.

- **Process Control and Optimization** This is when various classes of sensors (with or without actuation capabilities) are used for monitoring and to provide data so a process can be controlled remotely. This could be as simple as the use of cameras (the sensing nodes in this example) to position boxes of various sizes on a conveyer belt so a label machine can properly apply labels to them. This task can be done in real time by sending the data to a remote computer, analyzing it and bringing a command back

to the line so various control actions can be taken to improve the process … without any human intervention.

- **Resource Allocation and Optimization** The smart energy market provides an ideal example of this use case. The term "smart energy" has been used in many ways, but it basically refers to accessing information about energy consumption and reacting to the information to optimize the allocation of resources (energy use). In the case of a household, for example, once the residents know they've been using their washing machine during peak hours when the grid is most constrained and the cost of electricity is at premium, they could adjust their behavior and wash their laundry during nonpeak hours, saving money and helping the utility company cope with the peak demand. Context-aware Automation and Decision Optimization This category is the most fascinating, as it refers to monitoring unknown factors (environmental, interaction between machines and infrastructures, etc.) and having machines make decisions that are as "human-like" as possible.

8. IoT challenges

IoT devices with limited functionality have been around for at least a decade. What has changed recently is the ubiquity of connectivity options (WIFI, 3G, and Bluetooth etc.), cloud services and analytics, which are great enablers for IoT. The Cloud provides a platform for hosting intelligent software, networking a large number of IoT devices and provisioning them with a large amount of data. This enables smart decisions to be made without human intervention.

However, there are still some current challenges limiting the adoption of IoT:

Security vulnerabilities (privacy, sabotage, denial of service): Regular hacking of high-profile targets keeps this danger constantly in the back of our minds. Obviously, the consequences of sabotage and denial of service could be far more serious than a compromise of privacy. Changing the mix ratio of disinfectants at a water treatment plant or stopping the cooling system at a nuclear power plant could potentially place a whole city in immediate danger.

Regulatory and legal issues: This applies mainly to medical devices, banking, insurance, infrastructure equipment, manufacturing equipment, and in particular, pharmaceutical and food related equipment. Today, this mean complying with laws such as CFR 21 part 11, HIPAA, Directive 95/46/EC and GAMP 5. Etc. This adds to the time and cost needed to bring these products onto the market.

Determinism of the network: This is important for almost all areas where IoT can be used, such as in control applications, security, manufacturing, transport, general infrastructure, and medical devices. The use of the cloud currently imposes a delay of about 200 milliseconds or more. This is fine for most applications, but not for security or other applications that require a rapid, almost immediate, response. A trigger from a security monitoring system received five seconds later could be too late.

Lack of a common architecture and standardization: Continuous fragmentation in the implementation of IoT will decrease the value and increase the cost to the end users. Currently, there are also Google's Brillo and Weave, AllJoyn, Higgns, to name but a few. Most of these products target very specific sectors. Some the causes of this fragmentation are security and privacy fears (privacy through obfuscation and the fear of "not invented here"), jostling for market dominance, trying to avoid issues with competitors' intellectual property, and the current lack of clear leadership in this area.

Scalability: This is currently not much of an issue, but it is bound to become an issue mainly in relations to generic consumer cloud as the number of devices in operation rises. This will increase the data bandwidth needed and the time needed for verifying transactions.

Limitations of the available sensors: Fundamental sensor types, such as temperature, light, motion, sound, color, radar, laser scanner, echography and x-ray, are already quite performant. Furthermore, recent advances in microelectronics, coupled with advances in solid state sensors, will make the bare sensors less of an issue in the future. The challenge will be in making them more discriminating in crowded, noisy and more complex environments. The application of algorithms that are similar to fuzzy logic promises to make this less of an issue in the future.

Dense and durable off-grid power sources: While Ethernet, WIFI, 3G and Bluetooth have been able to solve most connectivity issues by accommodating the various devices' form factors, the limitations of battery life still remain. Most smartphones still need to be charged every day, and most sensors still need regular battery changes or connection to the grid. It would make a difference if power could be broadcasted wirelessly to such devices from a distance, or if power sources that can last for at least a year can be integrated into the sensors.

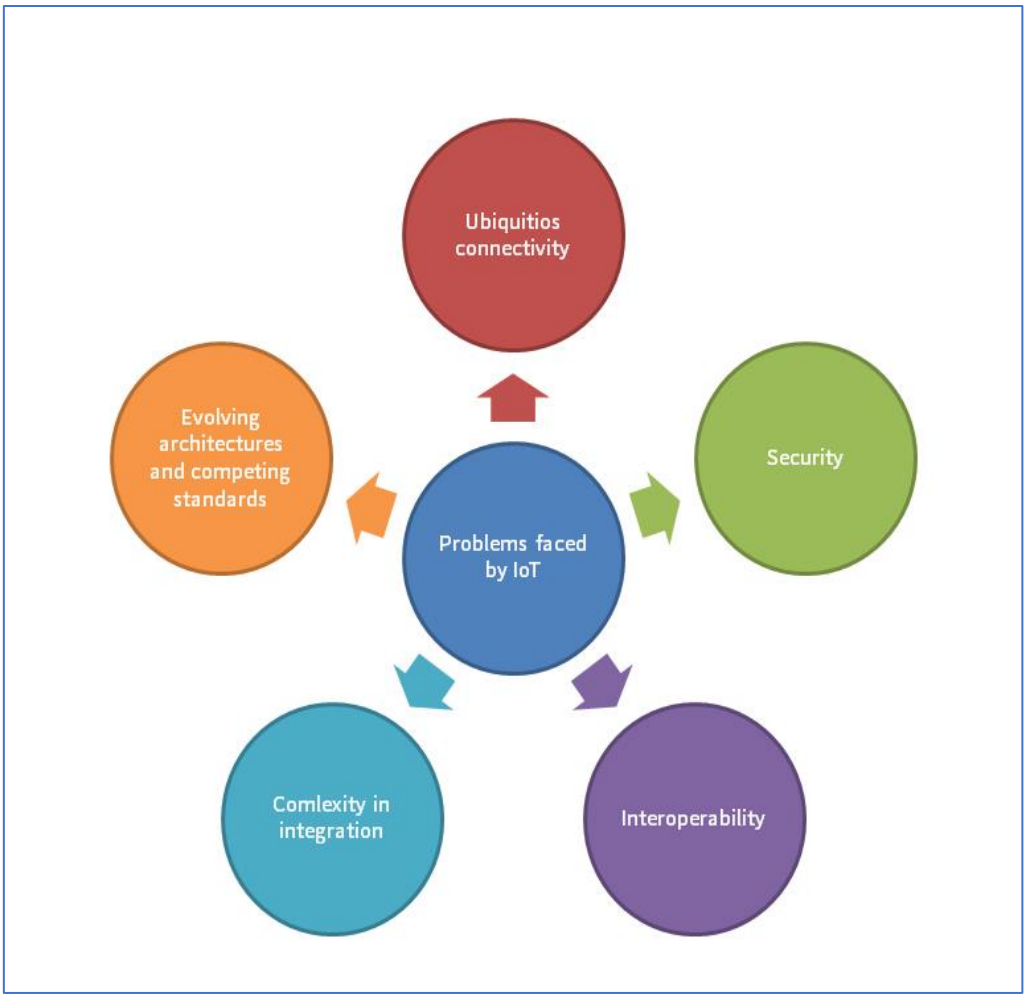

Figure 1.5 Problems faced by IoT

9. Security vulnerabilities in overall IoT system

Having everything connected to the global internet infrastructure and things communicating with each other brings many security and privacy problems in the overall ecosystem [62]. However, many identified challenges could fit in the frame of the original triad for information security, namely confidentiality, integrity and availability.

a) Confidentiality is a fundamental challenge for the IoT system as data are generated from various sources and the system access these data dynamically. Proper management of data sources and a capability to handle the classified data from specific device are the key factors to assure confidentiality of the data in IoT system. Current solutions to guarantee confidentiality may not be applicable [4], mainly due to two reasons: big volumes of generated data sources and lack of effective control over dynamically streamed data. Various encryption schemes can be applied to obtain the confidentiality of the communication channel; however, current systematic and asymmetric algorithms should be updated before implementing in IoT based applications [12].

b) Integrity deals with the first damages or failures of physical devices. Integrity protection includes preservation against sabotage and use of the countermeasure components to protect the device and sent data. Data integrity in IoT system will rely on the robustness and fault tolerance of the entire system. Integrity of the IoT system can be affected by internal and external source as well as by internal process. For example, in sensor networks, many RFIDs remain unattended most of the time. This gives an opportunity to external attackers to either modify data while storing it to the node or while transferring it to the network [4]. Read and write protection using password might be the possible way out to strengthen the integrity of the systems caused by external and internal sources of attacks. Multilevel security (MLS) helps to avoid unauthorized modifications due to internal process, such as malicious running code. A trusted platform module (TPM) is another hardware solution proposed for integrity challenges.

c) Availability of IoT system is highly tied with reliability requirements [13]. To sustain required level of availability, the IoT system should show the levels of performance requested by the application. The adequate level of hardware and software performance used in the IoT network should be able to cope with the requirements of the users. Software availability is the ability of applications to provide the service to everyone at any location simultaneously. Hardware availability refers to the presence of the device all the time. One example of availability challenge could be demonstrated by denial of service (DOS) attack. DOS attacks prevent devices to access resources from the network. Commands for DOS attack can be generated remotely to obstruct the IoT system. DOS attacks in IoT may concern not only the traditional vectors, for instance resources of providers, bandwidth, etc. but also they can affect the data acquisition of wireless communication from IoT node [13]. Moreover, some constrained devices connected in IoT system that may affect the availability in the network, similar to the effect of DOS attacks [14]. Implementation of distributed architecture rather than a centralized one can help to improve the availability of the IoT system [13].

10. Internet of things future trends

After we have seen the amazing data and made sure that IoT is a very promising path, we are getting acquainted with this innovation a little bit closer and discover what trends are prevailing now on this market and what aspects should be taken into account .

a. IoT and big data

Big data appeared long before the IoT. But the whole concept of the Internet of things is about data gathering and processing. IoT devices are built on the basis of special chips which main purposes are to track users' activity.

As far as the IoT ideas are going to be applied to every sphere of human's lives, like houses, transport, medicine, education and many other things, Big Data gathering opens new opportunities to introduce your customer to great experiences which he or she couldn't even imagine before.

Such a massive data flow requires another level of computing capability to analyze and process data in a real time mode. Along with that, we see that some new generation analytical platforms are offering to use GPU powered databases to process vast data using minimal hardware.

b. IoT and machine learning

As IoT devices collect so much data why not to use it to teach the system? IoT boost brings more and more devices into our lives, and as a result machine to machine, communication has to become more and more advanced. Machine learning is needed to make better predictions about the outcome of different situations. It is a matter of life and death if we apply it to medicine or road traffic safety. Usual analytics are static, whereas Machine Learning algorithms constantly improve. The ability of IoT devices to interact with other appliances makes it even easier because of training one, you train them all.

This fantastic ability of IoT devices to get smarter over time is extremely useful for businesses. The system is able to detect minimal deviations from the norm long before a human eye could detect them. For some companies that use expensive equipment, which breakages lead to millions in expenses, precise maintenance prediction means huge cost savings.

c. IoT and Blockchain

Because data gathering is so essential in IoT work, it means that this data has to be protected throughout its life cycle. Data management under all these conditions is a very difficult task as it will flow across many boundaries with different policies. This complexity shows all the challenges to keep IoT protected.

The IoT approach is new and old security technologies cannot be applied here as they don't guarantee a proper protection of the system. The answer is Blockchain. This method is secure, transparent and efficient.

III. Low power and lossy networks:

1. low power/lossy network:

LLNs 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.

LLNs are a class of network in which both the routers and their interconnect are constrained: LLN routers typically operate with constraints on (any subset of) processing power, memory

and energy (battery), and their interconnects are characterized by (any subset of) high loss rates, low data rates and instability. LLNs are comprised of anything from a few dozen and up to thousands of LLN routers, and support point-to-point traffic (between devices inside the LLN), point-to-multipoint traffic (from a central control point to a subset of devices inside the LLN) and multipoint-to-point traffic (from devices inside the LLN towards a central control point).[6]

The Routing Protocol for Low Power and Lossy Networks feature specifies the IPv6 Routing Protocol for LLNs (RPL), thereby providing a mechanism whereby multipoint-to-point traffic from devices inside the LLN towards a central control point, and point-to-multipoint traffic from the central control point to the devices inside the LLN, is supported. Point-to-point traffic is also supported.

2. Network organization:

There is a lot of topologies in this type of networks, we mention [15]:

a. Point-to-Point Network

A point-to-point network establishes a direct connection between two network nodes. Communication can take place only between these two nodes, or devices. An example of this type of network is a Bluetooth link between a cell phone and an ear piece.

The advantages of point-to-point networking are its simplicity and low cost. The primary limitations spring from the one-to-one relationship that exists between two devices; the network cannot scale beyond these two nodes. The range of the network is therefore limited to one hop, and defined by the transmission range of a single device. One side is generally a gateway to the Internet or another conventional network that allows users to make use of the device.

b. Star Network

A star network consists of one central hub (a.k.a. gateway node), to which all other nodes (e.g., the sensor nodes) in the network are linked. This central hub acts as a common connection point for all other nodes in the network. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central hub only. An example of this topology is the Wi-Fi network hub in your house. The hub is generally also the link to the outside world. There are a few important advantages to a star topology.

First, the performance of the network is consistent, predictable and fast (low latency and high throughput). In a star network, unlike the mesh network described next, a data packet typically only travels one hop to reach its destination (if traveling between the hub and a sensor) or at most two hops (if traveling between two sensors), yielding a very low and predicable network latency.

Second, there is high overall network reliability due to the ease with which faults and devices can be isolated. Each device utilizes its own, single link to the hub. This makes the isolation

of individual devices straightforward and makes it easy to detect faults and to remove failing network components.

The disadvantages of this network type are similar to the point-to-point network. The range is limited to the transmission range of a single device. Additionally, there is no ability to route around RF obstacles should there be a network interference or interruption. Finally, in a star networking there is a single point of failure, the gateway. In a mesh network, if the gateway loses connectivity, the network is cut off from the world but it can still exchange and store data internally. This is important to some applications, such as meter reading or cold chain management.

c. Mesh Network

A mesh network consists of three types of nodes:

- A gateway node as in a star network, provided so data can reach the outside world
- Simple sensors nodes
- Sensor/router nodes, which are sensor nodes with repeater/routing capability

Sensor/router nodes must not only capture and disseminate their own data, but also serve as relays for other nodes. That is, they must collaborate with neighboring nodes to propagate the data through the network.

Mesh network nodes are deployed such that every node is within transmission range of at least one other sensor/router node. Data packets pass through multiple sensor/routers nodes to reach the gateway node.

This networking topology is used for many applications requiring a long range and broad area coverage. Applications include building automation, energy management, industrial automation, and asset management, to name a few. Because the network range is not limited to the transmission range of a single device, the network range can be very broad, covering large areas, such as a building or campus. Mesh networks can scale up to thousands of nodes, providing a high density of coverage with a broad assortment of sensors and actuating devices. The flexibility of network layout allows coverage in environments facing high radio frequency (RF) challenges, such as high RF interference or RF obstacles. Intermittent network interruptions are mitigated by self-healing and packet retransmission capabilities that together provide a high degree of network resilience.

The primary disadvantage is that mesh networks are, by their nature, more complex than point-to-point or star network topologies. A sight survey is typically done followed by installation and commissioning of the network. Also, there is higher network latency in mesh networked due to multiple networks hops typical from the sensor to gateway.

These three networking topologies form the foundation for a deeper evaluation of attributes associated with each established and emerging network standard.

In a follow-up post we'll review several other important network attributes, then drill into a full application requirements characterization and checklist, a critical next step in making a networking technology selection.

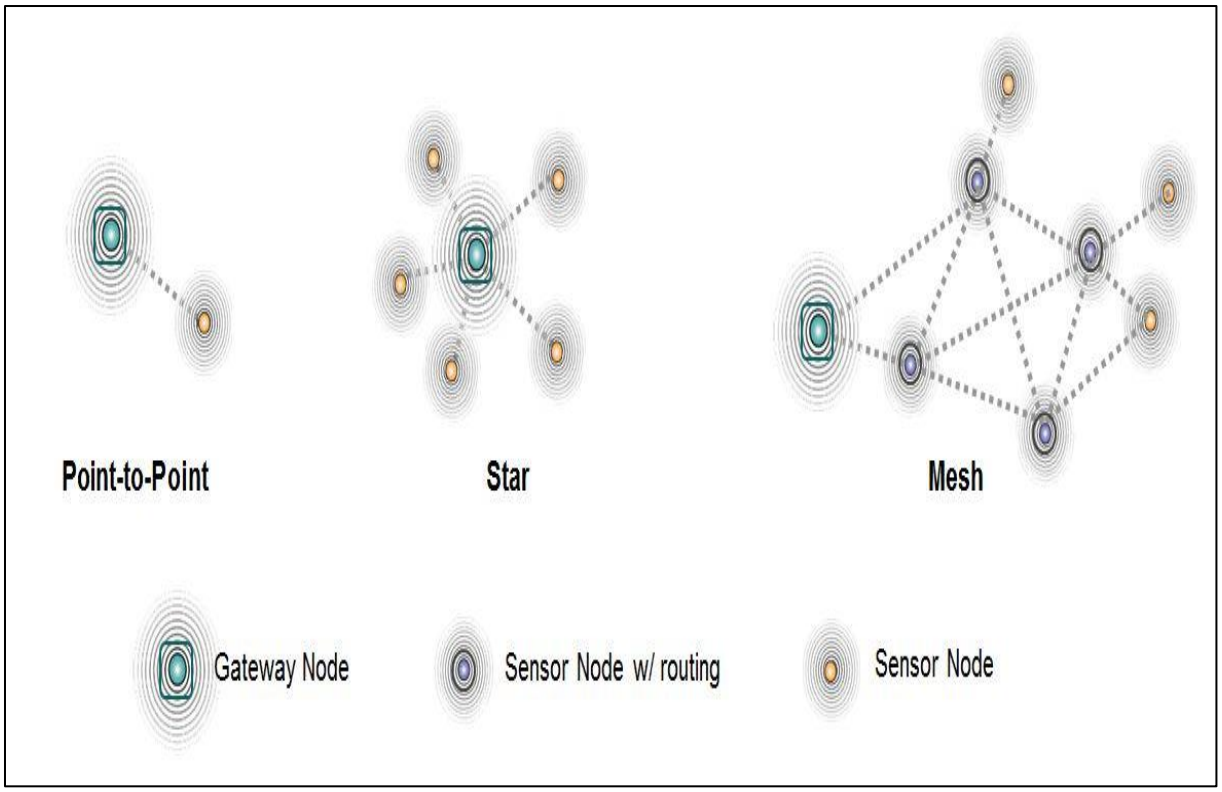

Figure 1.6 Network topologies in LLN

3. Network characteristics:

This type is considered as a network where some of the characteristics pretty much taken for granted with link layers in common use in the Internet at the time of writing are not attainable, we mention [16] some characteristics like:

- low achievable bitrate/throughput (including limits on duty cycle).
- high packet loss and high variability of packet loss (delivery rate).
- highly asymmetric link characteristics.
- severe penalties for using larger packets (e.g., high packet loss due to link-layer fragmentation).
- limits on reachability over time (a substantial number of devices may power off at any point in time but periodically "wake up" and can communicate for brief periods of time).
- lack of (or severe constraints on) advanced services such as IP multicast.

4. 6LoWPAN

a. Definition:

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) is a protocol definition to enable IPv6 packets to be carried on top of low power wireless networks, specifically IEEE 802.15.4. The concept was born from the idea that the Internet Protocol could and should be applied to even the smallest of devices.

b. Architecture:

LoWPANs are stub networks which is:

- Simple LoWPAN with Single Edge Router.
- Extended LoWPAN with Multiple Edge Routers with common backbone link.
- Ad-hoc LoWPAN which has no route outside the LoWPAN.

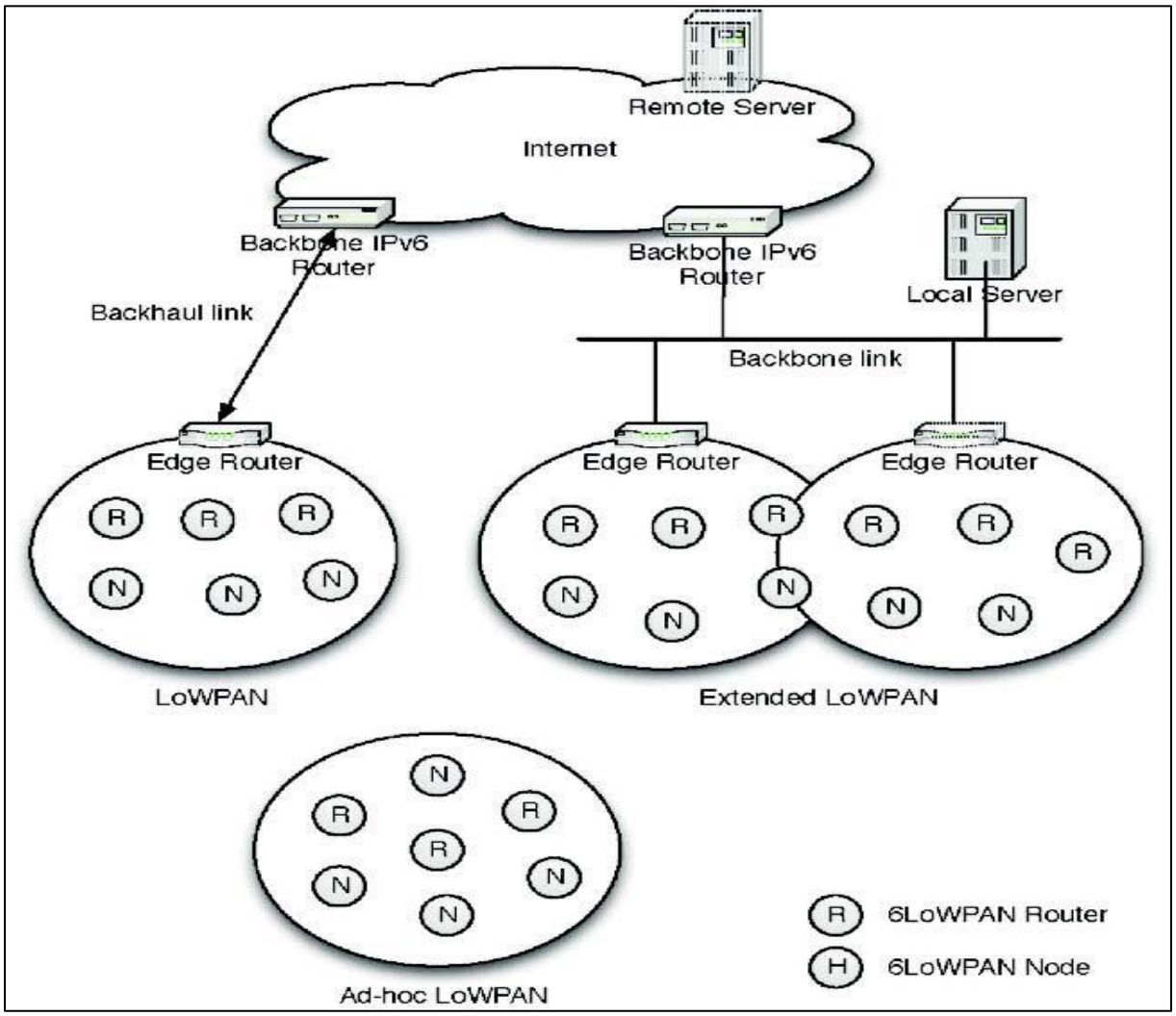

Figure 1.7 6LoWPAN architecture

c. *Benefits of 6LoWPAN Technology*

- Open, long-lived, reliable standards
- Easy learning-curve
- Transparent Internet integration
- Network maintainability
- Global scalability
- Enables a standard socket API
- Minimal use of code and memory
- Direct end-to-end Internet integration

d. *6LoWPAN protocols stack*

Application layer	**Application protocols**	
Transport Layer	**UDP**	**ICMP**
Network Layer	**IPv6, RPL**	
Data Link Layer	**LoWPAN**	
	IEEE 802.15.4 MAC	
Physical Layer	**IEEE 802.15.4 PHY**	

Table 1.2 the 6LoWPAN stack

IV. Conclusion

The Internet has changed drastically the way we live, moving interactions between people at a virtual level in several contexts spanning from the professional life to social relationships. The IoT has the potential to add a new dimension to this process by enabling communications with and among smart objects, thus leading to the vision of "anytime, anywhere, anymedia, anything" communications.

Chapter two:

Routing in IoT-connected LLNs

I. Introduction

One of the fundamental aspects of the Internet of Things is the manner low powered devices self-organize and share information (route and data information) among themselves. Even though these sensory devices are energy constrained, they however, perform storage and computation functions while communicating over lossy channels. These nodes work in unison and can join and leave the network at any time. It is of importance that the wireless routing solution for these sensor networks should be scalable, autonomous while being energy-efficient. The devices utilized in these low power lossy networks (LLN) are basically sensors and actuators but they have routing capabilities. Some of these sensor nodes act as border routers and hence connect the LLNs to the internet or to a closely located Local Area Network (LAN). Such routers are commonly referred to as LLN border routers (LBR).

The Internet Engineering Task Force (IETF) created working groups (WGs) which developed various IoT protocols for IoT devices, these protocols have been developed for the Internet of Things (IoT), such as 6LoWPAN,RPL,AODV, 6TiSCH (IPv6 over the time slotted channel hopping mode of IEEE 802.15.4e) …etc.

In this chapter, we focus on the presentation of the RPL protocol details, which is going to use in our solution later.

II. Routing protocols in IOT

1. Routing challenges:

In this section we see some routing challenges:[17]

a. Node deployment:

Unlike conventional networks where network topologies are determined in the beginning of network construction. Node deployment in WSNs is either deterministic or randomized. In deterministic deployment, network topologies are decided in advance and remains nearly the same during their lifetime and thus data can be routed through pre-determined paths. However, in randomized deployment, sensor nodes are randomly scattered creating an unknown and unstable network topology. Data routing in this type of node deployment inherently possesses no prior knowledge of network topology and thus requires processing more routing data.

b. Energy consumption without losing accuracy:

Energy consumption is a big concern in WSNs due to sensor nodes' limited supply of energy. Thus, the routing protocols are required to maximize the energy-conserving form of communications and computations to prolong the battery lifetime. However, these types of communications and computations still provide needed accuracy of routing protocols. The second aspect of energy concern in WSNs is to maintain the accuracy of routing protocols in presence of low power sensor nodes. As sensor nodes can act as either senders, receivers or routers. A malfunctioning of some sensor nodes due to power failures can cause topology changes or miscommunication or miscalculation in constructing routing paths. Thus, routing protocols should be aware of and prepare to handle this possible problem.

c. Network dynamic:

Like conventional networks, most of WSNs consist of stationary sensor nodes. However, there exist dynamic network in WSNs such as WSNs target detection or tracking applications. Routing messages in this type of dynamic networks are more challenging due to quickly changing routing path. In dynamic network, strategy for routing protocols is to simply generating routing path on demand. Due to the instability of the network, pre-calculating routing path is not of importance as the pre-calculated paths maybe of no use when they are needed.

d. Fault tolerance:

WSNs are inherently prone to failure due to for example lack of power, physical damage or environmental interference. Despite of the numerous amounts of sensor nodes in some applications, the failure of certain number of sensor nodes can greatly reduce and affect the performance of the whole network. For example, packets needed to be routed through longer path, a whole network is divided into two parts. Thus, routing protocols should take into consideration some fault tolerance mechanism in case of unexpected failure. For

example, giving more priority to routing path with more remaining energy or quickly detecting the failure of certain nodes to recommend alternative routing paths.

e. Scalability:

WSNs are likely to be expanded in some cases. For example, a company might deploy a network of around a hundred sensor nodes in the beginning and then expand the network to the number of thousands of sensor nodes afterwards. Hence, routing protocols should be designed to work not only in network with small number of sensor nodes but also in network with larger amount of sensor nodes.

2. Routing protocols in Wireless Sensor Networks

Routing protocols for Wireless Sensor Networks can be classified in many ways, depending on different criteria. In this section, routing protocols are classified into two criteria: Network Structure and Protocol Operations.

2.1 Network Structure Utilizing

network structure in routing protocols can reduce usage of many network resources such as bandwidth, traffic load, processing time or energy consumption. Due to variety of network topology, routing protocols are also developed correspondingly.

a) Flat routing protocols are mainly used for networks with flat structure with a large amount of sensor nodes. Each sensor node plays equal role in the network and neighboring nodes can collaborate to gather information or perform sensing task. The large number of sensor nodes results in the impossibility of assigning global unique identifier for each node. This has led to data centric routing mechanism where the receiver node sends queries to a certain group of sensor nodes and wait for reply from the intended sensors. An example of flat routing protocols is SPIN (Sensor Protocols for Information via Negotiation) [18] where each node considers every other node as potential receiver. The protocol utilizes the similar data in the neighboring nodes so as to avoid sending redundant data throughout the network.

b) Hierarchical routing protocols are designed for networks with hierarchical structure like Internet. The idea is to divide the network into cluster and select from each cluster a cluster head. Usually the higher energy nodes are used to process information, send data while the lower energy nodes used to sense in the proximity of the target. This type of routing protocols offers the advantages of scalability and efficient communication at the expense of the overhead of cluster formation and cluster head selection in the beginning. An example of Hierarchical routing protocol is LEACH (Low Energy Adaptive Clustering Hierarchy) [19] which randomly select few sensor nodes as clusterheads. The role of clusterhead rotates among sensor nodes in the same cluster to equally distribute the energy consumption among cluster members. Clusterheads are responsible for gathering data arriving the cluster and sending the aggregated data to the intended receivers. This way can reduce the traffic load among sensor nodes in the network.

c) Location-based routing protocols are protocols that take into consideration the specific location of sensor nodes. The location can be addressed by the signal strength if nodes are close to each other. In case of distant nodes, relative coordinate of nodes can be extracted through information exchanged between neighboring nodes. The protocol tends to save energy consumption by having unnecessary nodes going to sleep mode. Geographic Adaptive Fidelity (GAF) [20] is an example of this type of routing protocols.

2.2 Protocol Operations

Another criteria for routing protocol classification is Protocol Operations. The idea is to classify routing protocols based on their functionalities.

a) Multipath routing protocols

This type of routing protocols constructs many routing paths instead of single path as a fault tolerance mechanism. A single path is selected among several constructed paths usually based on the remaining energy. The sparse paths are kept alive by sending periodic messages. Hence there is the tradeoff between network reliability and traffic load of maintaining the alternate paths.

b) Query-based routing protocols

Data transmission in this type of protocols are carried on through requests and replies. The receiving nodes send requests message through the whole network and only nodes having the required data reply.

c) Negotiation-based routing protocols

This type of protocols is meant to eliminate the redundant data through communication between sending and receiving nodes. Negotiation decisions are taken based on the available resources of each participating nodes.

d) QoS based routing protocols

This type of protocols is used to maintain the balance among network resources such as energy, bandwidth, delay…

3. IOT's routing protocols:

There exist many available protocols for IoT networks. In this section, three examples of such routing protocols are presented.

a. 6LoWPAN - IPv6 over 802.15.4

is meant to extend IPv6 networks to IoT networks. The advantages of this approach are the possibility of re-using existing IPv6 technologies an infrastructure. However, this type of network is originally designed for computing devices with higher processing capability and memory resources which is not suitable for IoT network entities. **[20]**

b. RPL - IPv6 Routing protocols for Low Power and Lossy Network

This protocol types are designed for network comprising of constraint devices in power, computation capability and memory. Thus, the data transmission in this type of networks are unreliable and have low data rate but high loss rate. **[21]**

c. Constrained Application Protocol (CoAP)

The most prominent feature in this type of routing protocols is the ability of translating to HTTP message so as to integrate with web services. The protocol also support multicast with little overhead. **[22]**

III. RPL (Routing protocol for low-power and lossy networks)

1. Definition

RPL was developed by the IETF working group as routing functionalities in 6LoWPAN were very challenging due to the resource constrained nature of the nodes. RPL operates at the network layer making it capable to quickly build up routes and distribute route information among other nodes in an efficient manner. [23]

2. RPL properties overview

RPL demonstrates the following properties:[23]

- RPL is a distance vector routing protocol for LLNs that makes use of IPv6.
- The protocol tries to avoid routing loops by computing a node's position relative to other nodes with respect to the DODAG root.
- The RPL specification defines four types of control messages for topology maintenance and information exchange.
- Another important fact about the protocol's design is the maintenance of the topology.

2.1 IPv6 Architecture

RPL is strictly compliant with layered IPv6 architecture. Further, RPL is designed with consideration to the practical support and implementation of IPv6 architecture on devices which may operate under severe resource constraints, including but not limited to memory, processing power, energy, and communication. The RPL design does not presume high quality reliable links, and operates over lossy links (usually low bandwidth with low packet delivery success rate).

2.2 Typical LLN Traffic Patterns

Multipoint-to-Point (MP2P) and Point-to-multipoint (P2MP) traffic flows from nodes within the LLN from and to egress points are very common in LLNs. Low power and lossy network Border Router (LBR) nodes may typically be at the root of such flows, although such flows are not exclusively rooted at LBRs as determined on an application-specific basis. In particular, several applications such as building or home automation do require P2P (Point-to-Point) communication.

As required by the aforementioned routing requirements documents, RPL supports the installation of multiple paths. The use of multiple paths include sending duplicated traffic along diverse paths, as well as to support advanced features such as Class of Service (CoS) based routing, or simple load balancing among a set of paths (which could be useful for the LLN to spread traffic load and avoid fast energy depletion on some, e.g. battery powered, nodes). Conceptually, multiple instances of RPL can be used to send traffic along different topology instances, the construction of which is governed by different Objective Functions (OF). Details of RPL operation in support of multiple instances are beyond the scope of the present specification.

2.3 Constraint Based Routing

The RPL design supports constraint-based routing, based on a set of routing metrics and constraints. The routing metrics and constraints for links and nodes with capabilities supported by RPL are specified in a companion document to this specification.

RPL signals the metrics, constraints, and related Objective Functions (OFs) in use in a particular implementation by means of an Objective Code Point (OCP). Both the routing metrics, constraints, and the OF help determine the construction of the Directed Acyclic Graphs (DAG) using a distributed path computation algorithm.

3. RPL basics

Some of RPL's basics are:[24]

- A network may run multiple instances of RPL concurrently. Each such instance may serve different and potentially antagonistic constraints or performance criteria.
- In order to be useful in a wide range of LLN application domains, RPL separates packet processing and forwarding from the routing optimization objective like minimizing energy, minimizing latency, or satisfying constraints.
- RPL operations require bidirectional links.
- RPL also expects an external mechanism to access and transport some control information, referred to as the "RPL Packet Information", in data packets.

4. Upward Routing

Upward routing is a standard procedure which enables network devices to send data to a root.

In a typical WSN scenario, nodes periodically generate data packets which have to find their way through the network. [24]

- *DIO Message Structure*

DIO message is the main source of information which is needed during topology construction.

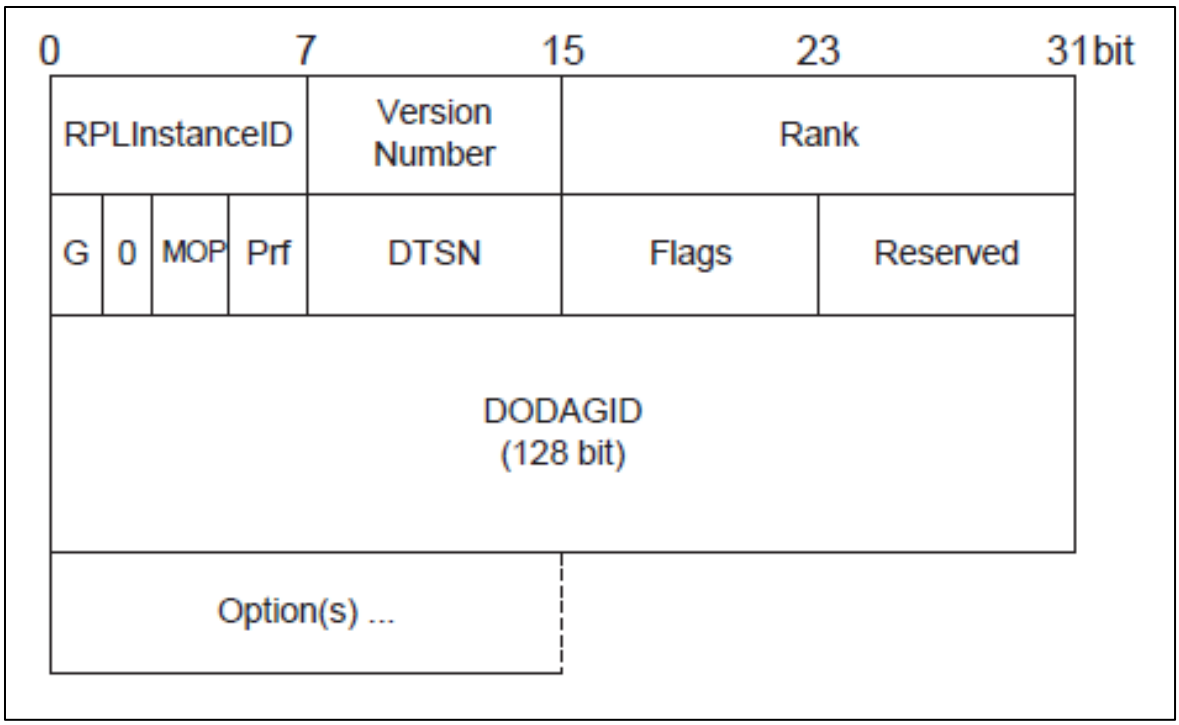

Figure 2. 1 DIO Message Structure

```
0x00 Pad1
0x01 PadN
0x02 DAG Metric Container
0x03 Routing Information
0x04 DODAG Configuration
0x08 Prefix Information
```

Figure 2. 2 DIO Option

- The first field is RPLInstanceID.
- The second and the third field is the sender's DODAG Version and the Rank of the message.
- The 'G' flag which defines whether a DODAG is grounded.

- The MOP(mode of operation) field is set by the DODAG root and defines the used mode of operation for downward routing.
- The Prf(DAGPreference) field defines how preferable the root node is compared to other root nodes.
- DTSN (Destination Advertisement Trigger Sequence Number) field: Such a number is maintained by the node issuing the DIO message and guarantees the freshness of the message.
- The DODAGID field used to identify node.

- *DODAG Configuration Option*

A DIO message may be extended by the use of options.

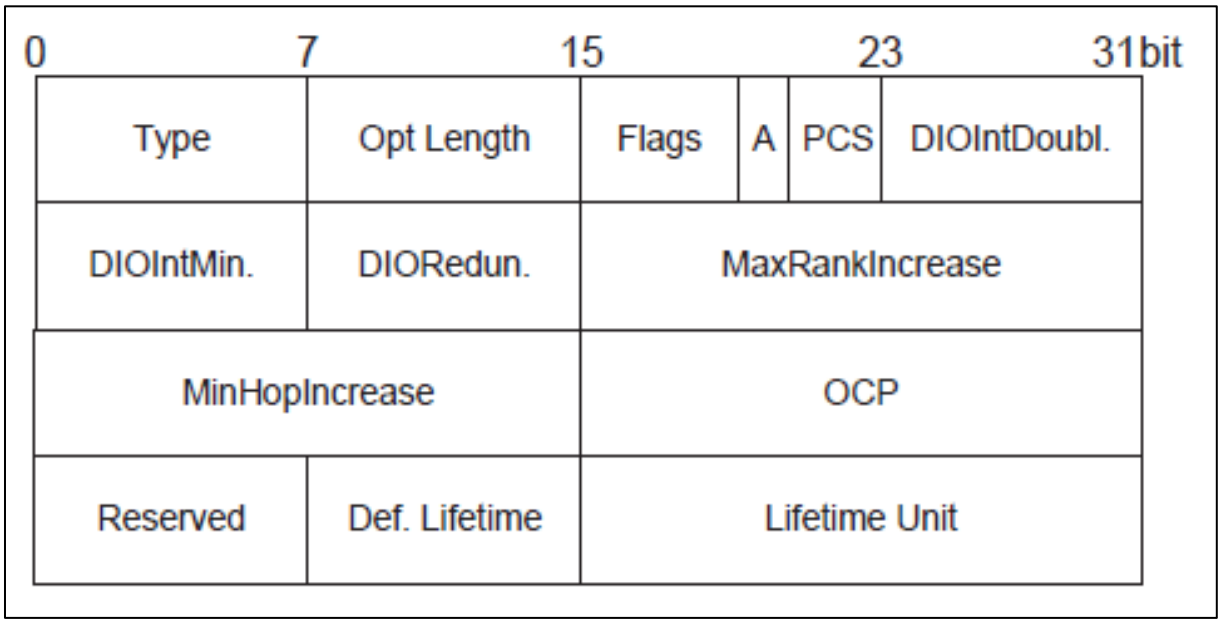

Figure 2. 3 DODAG Configuration Option

- The first two bytes present option type (0x04).
- The option's length (14 bytes).
- DIOIntervalDoublings: used to configure I_{max} of the DIO Trickle timer.
- DIOIntervalMin: used to configure I_{min} of the DIO Trickle timer.
- DIORedundancyConstant: used to configure k of the DIO Trickle timer.
- MaxRankIncrease: defines an upper limit for the Rank.
- MinHopRankIncrease: stores the minimum increase of the Rank between a node and any of its parent nodes.

- OCP (Objective Code Point): The OCP field identifies the OF and is managed by the IANA.
- Default Lifetime: This is the lifetime that is used as default for all RPL routes. It is expressed in units of Lifetime Units
- Lifetime Unit: Provides the unit in seconds that is used to express route lifetimes in RPL.

5. Construction Topologies:

In a RPL network, node have three type:

a) root node
b) routers
c) leaf

and these is the steps to construct topologies in RPL network [24]:

Step1. Construction topology starts at a root node begins to send DIO messages.

Step2. Each node that receives the message runs an algorithm to choose an appropriate parent.

*The choice is based on the used metric and constraints defined by the OF.

Step3. Each of them computes its own Rank and in case a node is a router, it updates the Rank in the DIO message and sends it to all neighboring peers.

Step4. Repeat Step.2 and Step3. the process terminates when a DIO message hits a leaf or when no more nodes are left in range.

Three values have to be considered in order to uniquely identify a DODAG:

a) RPL Instance ID: identification of an independent set of DODAG.
b) DODAG ID: is a routable IPv6 address belonging to the root.
c) DODAG version number: is incremented each time a DODAG reconstruction.

** To achieve RPL dynamically adapts the sending rate of DIO, two values need to be used.

- the minimum sending time interval, T_{min}
- the maximum sending interval, T_{max}

6. Routing Loops

The formation of routing loops is a common problem in all kinds of networks [23].

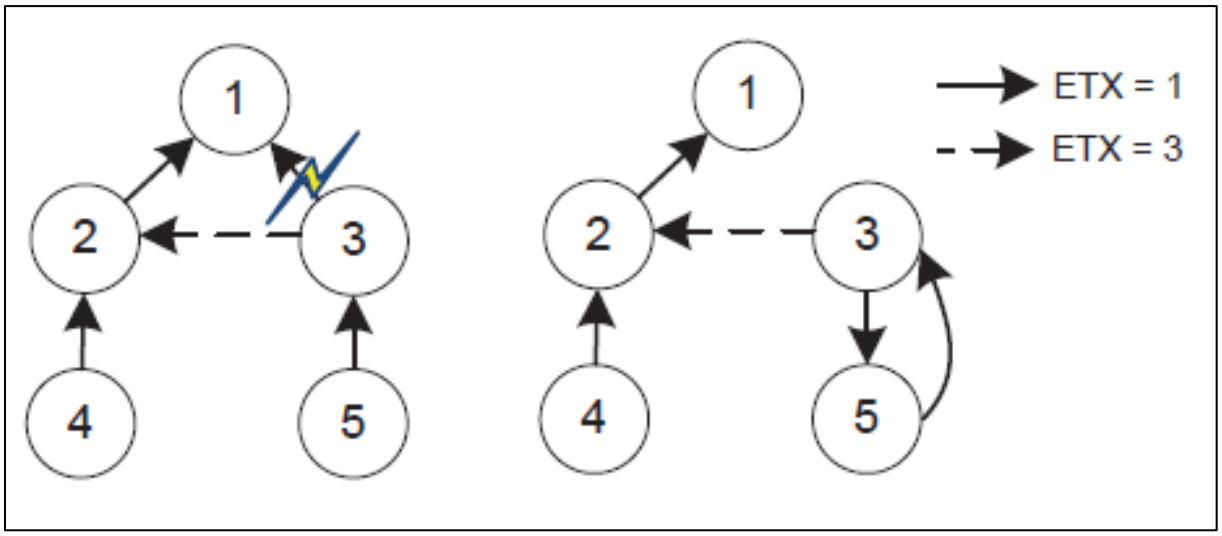

Figure 2. 4 Loop Creation

RPL define two mechanisms to solve this problem.

a) Avoidance Mechanisms
b) Detection Mechanisms

6.a. Avoidance Mechanisms

1. RPL node does not process DIO messages from nodes deeper (higher Rank) than itself.
2. RPL specification suggests that a node must never advertise within a DODAG Version a Rank higher than **RankLowest** + **RankMaxInc**.

RankLowest is the lowest Rank the node has advertised within a DODAG Version.

RankMaxInc is a predefined constant received via a DIO.

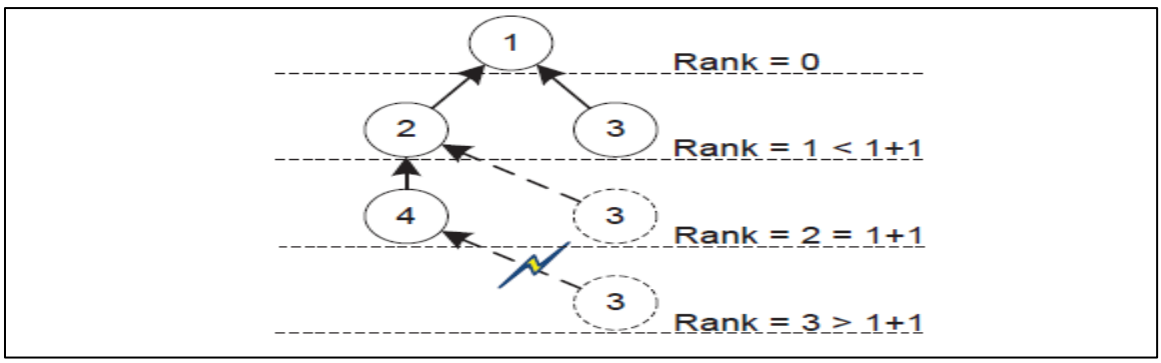

Figure 2. 5 Movement Limitation within a DODAG version

6.b. Detection Mechanisms

RPL loop detection uses additional information that is transported in the data packets.

It places a RPL Packet Information in the IPv6 option field which is updated and examined on each hop.

There are five control fields within the RPL Packet Information.

1. The packet is sent in a upward or downward direction.
2. Reports if a Rank mismatch has been detected.
3. Report a error field by a child node.
4. The Rank of the sender.
5. The RPL Instance ID.

7. RPL Metrics

- ***Node Energy Consumption***

Node energy consumption is the amount of energy or power used; it can be calculated by:

$$EE = \frac{Power_{now}}{Power_{max}} . 100$$

*EE (energy estimation)

- ***PRR (Packet Reception Rate)***

is defined as a percentage of nodes that successfully receive a packet from the tagged node among the receivers that are within transmission range of the sender at the moment that the packet is sent out.

$$PRR = \frac{Number\ of\ received\ packets}{Number\ of sent\ packets}$$

- ***ETX (expected transmission count)***

ETX is a measure of the quality of a path between two nodes in a wireless packet data network.

$$ETX = \frac{1}{PRR_{down} . PRR_{up}}$$

8. Downward Routing

The support of downward routing is another important feature of RPL. [23]

The RPL specification defines two modes of operation for supporting P2MP:

1. Non-storing mode
2. Storing mode

8.1. DAO Message Structure

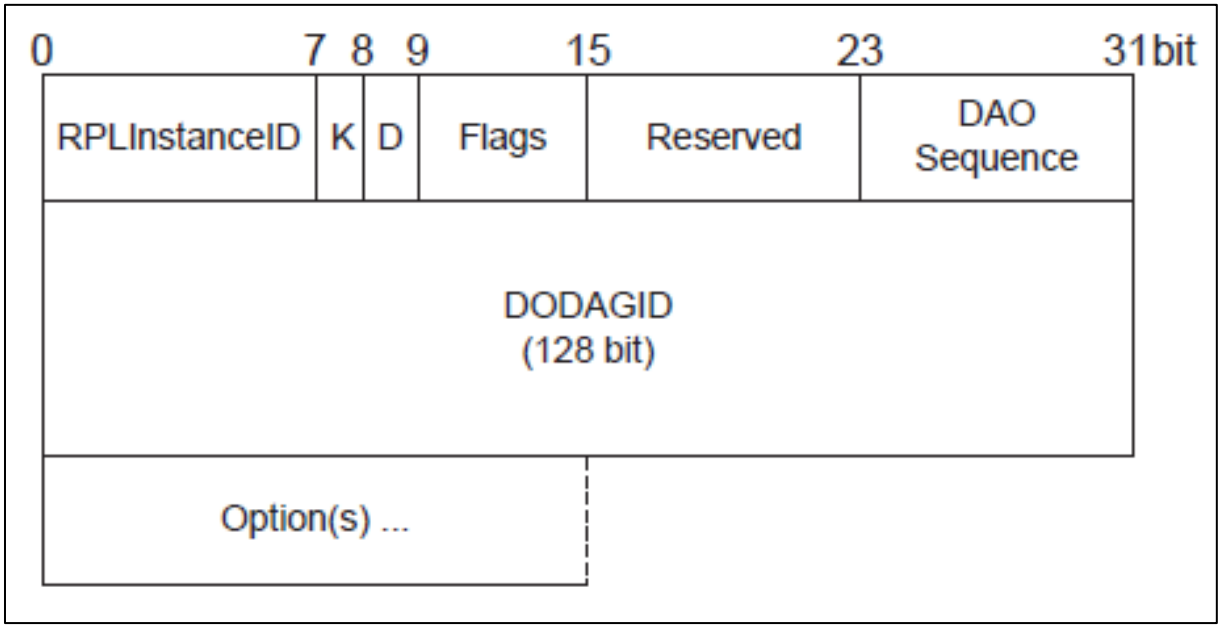

Figure 2. 6 Loop Creation

```
0x00 Pad1
0x01 PadN
0x05 RPL Target
0x06 Transit Information
0x09 RPL Target Descriptor
```

Figure 2. 7 DAO Option

- The 'K' flag which indicates whether the sender of the DAO expects to receive a DAO-ACK in response.
- The 'D' flag indicates if the DODAGID field is present.
- The DAO Sequence field is a sequence number that is incremented for each outgoing DAO message by the sender.

8.2. DAO Target Option

Target Option is used to indicate a target IPv6 address, prefix or multicast group.

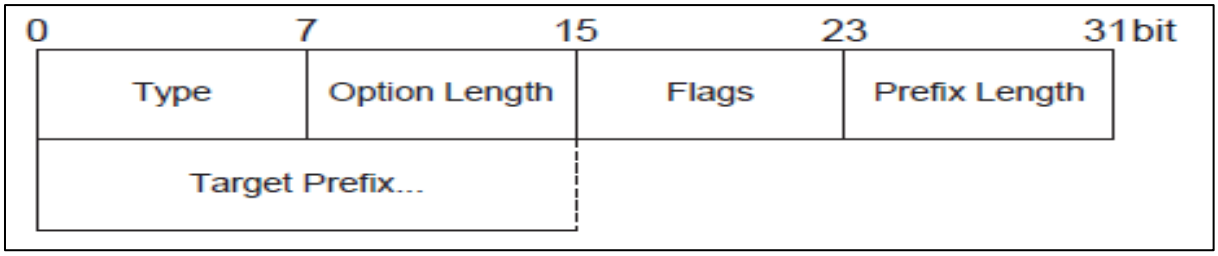

Figure 2. 8 DAO Target Option

- Option Type: 0X05
- Option Length: Variable, length of the option in octets excluding the Type and Length fields.
- Prefix Length: 8-bit unsigned integer. Number of valid leading bits in the IPv6 Prefix.
- Target Prefix: Variable-length field identifying an IPv6 destination address, prefix, or multicast group.

8.3. DAO Transit Information Option

Transit Information Option is used to indicate attributes for a path to one or more destinations.

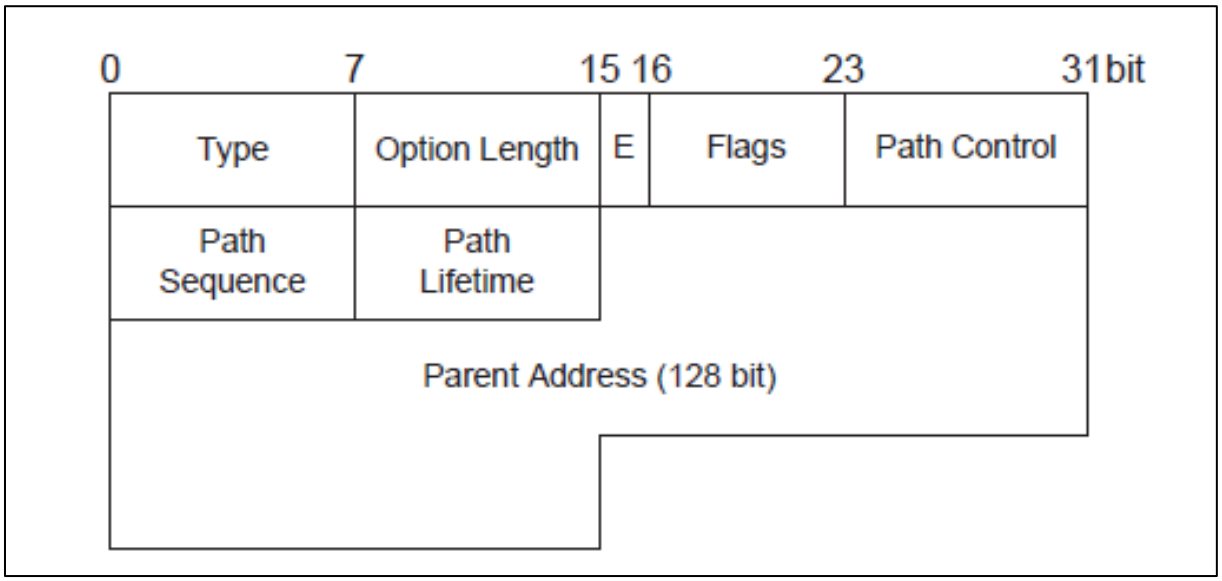

Figure 2. 9 DAO Transit Information Option

- Option Type: 0x06
- Option Length: Variable, depending on whether or not the DODAG Parent Address subfield is present.

- External (E): set to indicate that the parent router redistributes external targets into the RPL network.
- Path Control: limits the number of DAO parents to which a DAO message advertising connectivity to a specific destination may be sent.
- Path Sequence: indicates if a Target option with updated information has been issued.
- Path Lifetime: defines how long a prefix for a destination should be kept valid.
- Parent Address (optional): IPv6 address of the DODAG parent of the node originally issuing the Transit Information option.

8.4. Non-Storing Mode

- In the non-storing mode, each node generates a DAO message and sends it to the DODAG root.
- The RPL specification suggests that the delay between two DAO sending operations may be inversely proportional to the Rank.
- The resulting DAO message is sent directly to the DODAG root along the default route created during parent selection.
- The DODAG root can piece together a Downward route to a node by using DAO parent sets from each node in the route.

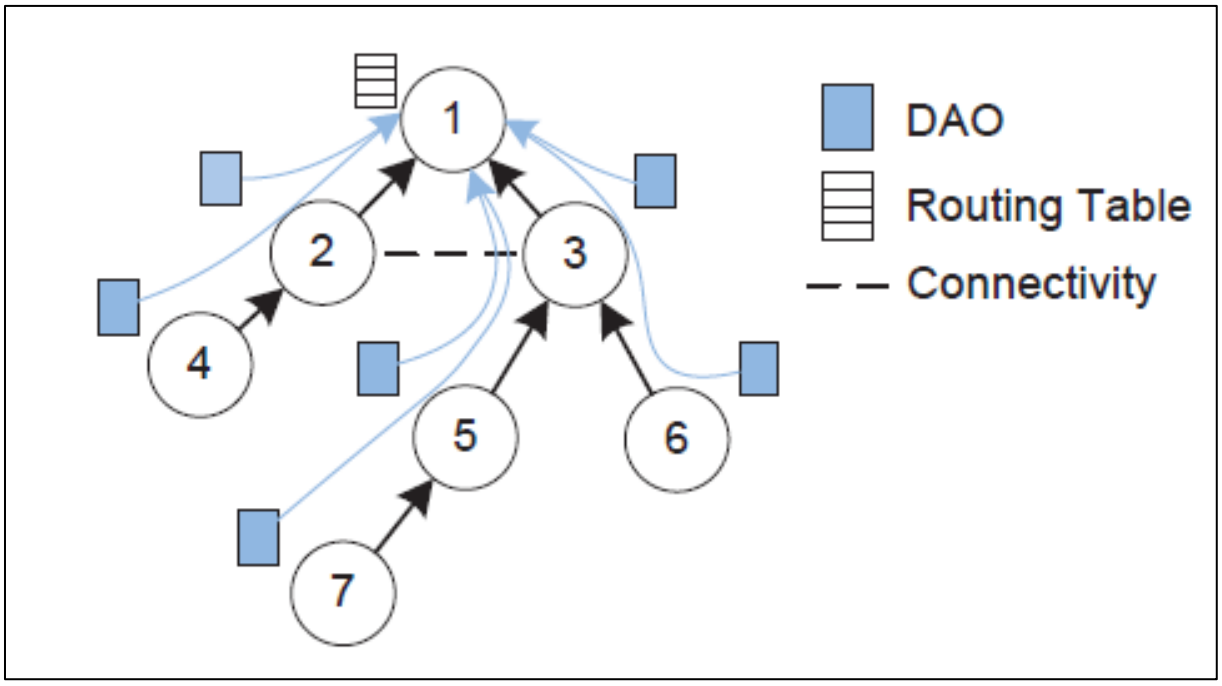

Figure 2. 10 RPL Non-Storing Mode

8.5. Storing Mode

- Similar to the non-storing mode, the storing mode also requires the generation of DAO messages.
- However, a DAO is no longer propagated to the DODAG root.
- Instead, it is sent as unicast to all parent nodes which maintain additional downward outing tables.

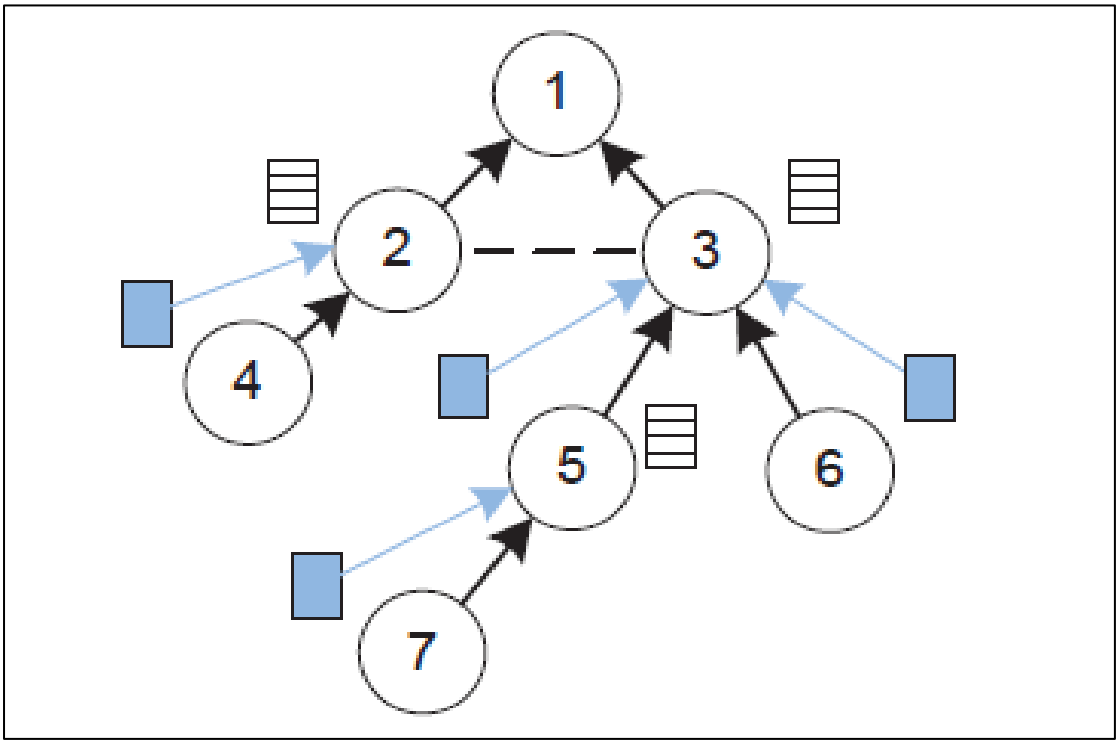

Figure 2. 11 RPL Storing Mode

IV. Conclusion

In this chapter we have presented the most important elements of RPL's operation, we should mention that there is a lot of routing mechanism for networks of low power and limited computation capability devices. Still there are many possible research directions in this area.

Chapter three:

Secure routing in IoT-connected LLNs

I. Introduction:

Many LLN routing protocols have been proposed, but none of them have been designed with security as a goal. When the defender has the liabilities of insecure wireless communication, limited node capabilities, and possible insider threats, and the adversaries can use powerful laptops with high energy and long-range communication to attack the network, designing a secure routing protocol is non-trivial.

In more conventional networks, a secure routing protocol is typically only required to guarantee message availability. Message integrity, authenticity, and confidentiality are handled at a higher layer by an end-to-end security mechanism such as SSH or SSL. End-to-end security is possible in networks that are more conventional because it is neither necessary nor desirable for intermediate routers to have access to the content of messages.

However, in LLN, in-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the content of the messages. Link layer security mechanisms it is not enough.

Therefore, in this chapter, we are going to talk about these attacks and see some works which tries to resolve this kind of vulnerabilities.

II. Routing attacks in IOT-connected LLNs:

Many LLN routing protocols are quite simple, and for this reason are sometimes susceptible to attacks.

These attacks categorize into:

- spoofed, altered, or replayed routing information,
- selective forwarding,
- sinkhole attacks,
- Sybil attacks,
- wormholes,
- HELLO flood attacks,
- acknowledgement spoofing.

1. Spoofed, altered, or replayed routing information

The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.

2. Selective forwarding

Multihop networks are often based on the assumption that participating nodes will faithfully forward received messages. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet she sees. However, such an attacker runs the risk that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a select few nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing.

Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest. The mechanics of such an effort are tricky at best, and may border on impossible.

Thus, we believe an adversary launching a selective forwarding attack will likely follow the path of least resistance and attempt to include herself on the actual path of the data flow. In the next two sections, we discuss sinkhole attacks and the Sybil attack, two mechanisms by which an adversary can efficiently include herself on the path of the targeted data flow.

3. Sinkhole attacks

In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example). Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high-quality route to a base station.

Some protocols might actually try to verify the quality of route with end-to-end acknowledgements containing reliability or latency information. In this case, a laptop-class adversary with a powerful transmitter can actually provide a high-quality route by transmitting with enough power to reach the base station in a single hop, or by using a wormhole attack.

Due to either the real or imagined high-quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a base station through the adversary, and also propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large "sphere of influence", attracting all traffic destined for a base station from nodes several (or more) hops away from the compromised node.

One motivation for mounting a sinkhole attack is that it makes selective forwarding trivial. By ensuring that all traffic in the targeted area flows through a compromised node, an adversary can selectively suppress or modify packets originating from any node in the area. It should be noted that the reason sensor networks are particularly susceptible to sinkhole attacks is due to their specialized communication pattern. Since all packets share the same ultimate destination (in networks with only one base station), a compromised node needs only to provide a single high-quality route to the base station in order to influence a potentially large number of nodes.

4. The Sybil attacks

In a Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, dispersity and multipath routing, and topology maintenance. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities. Sybil attacks also pose a significant threat to

geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. It is only reasonable to expect a node to accept but a single set of coordinates from each of its neighbors, but by using the Sybil attack an adversary can "be in more than one place at once".

5. Wormholes

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low-latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker.

An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. This will most likely always be the case when the endpoint of the wormhole is relatively far from a base station. More generally, wormholes can be used to exploit routing race conditions.

A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. In this case, an adversary may be able to exert some influence on the resulting topology if it can cause a node to receive certain routing information before it would normally reach them though multihop routing. Wormholes are a way to do this, and are effective even if routing information is authenticated or encrypted.

Wormholes can also be used simply to convince two distant nodes that they are neighbors by relaying packets between the two of them. Wormhole attacks would likely be used in combination with selective forwarding or eavesdropping. Detection is potentially difficult when used in conjunction with the Sybil attack.

6. HELLO flood attack

We introduce a novel attack against sensor networks: the HELLO flood. Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network

that the adversary is its neighbor. For example, an adversary advertising a very high-quality route to the base station to every node in the network could cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into oblivion.

The network is left in a state of confusion. A node realizing the link to the adversary is false could be left with few options: all its neighbors might be attempting to forward packets to the adversary as well. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to this attack. An adversary does not necessarily need to be able to construct legitimate traffic in order to use the HELLO flood attack. She can simply rebroadcast overhead packets with enough power to be received by every node in the network. HELLO floods can also be thought of as one-way, broadcast wormholes.

7. Acknowledgement spoofing

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for "overheard" packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive. For example, a routing protocol may select the next hop in a path using link reliability. Artificially reinforcing a weak or dead link is a subtle way of manipulating such a scheme. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links.

III. Related works:

Solution 1:(M-RPL1)

In this work [25], the author tries to Adapt the cluster-tree of IEEE 802.15.4 so that it can efficiently work coupled with rpl, by integration RPL and IEEE 802.15.4 to enable QoS multipath routing and improve packet delivery before a deadline, while minimizing overhead and energy consumption. The authors compared their opportunistic version of RPL to its basic version in terms of packet delivery ratio, incurred delay, and overhead through detailed simulations. Both protocols generate the same fixed amount of application data packets and none of them is destroyed before the end of the simulation. His Opportunistic solution results

in a slightly greater number of transmitted packets (9%), with a larger overhead comes from the forwarding rule.

Finally, this work allows the coexistence of two structures in emerging IP enabled wireless sensor networks: rpl routing and IEEE 802.15.4 MAC, this solution achieves slightly better results with respect to end-to-end packet reliability (PDR) and delay while keeping almost the same amount of generated traffic.

Solution 2: (M-RPL2)

In this work [26] the authors propose a solution as extension of RPL to provide temporary multipath routing during congestion over a path, which named M-RPL.

Operation of M-RPL is divided into two main parts, congestion detection and congestion mitigation. In M-RPL congestion is detected on any forwarding node whereas mitigation of congestion is performed by introducing multipath routing at nodes prior to the congested node. In Congestion detection the authors use the packet delivery ratio to detect the congestion at any node, and this is the algorithm used:

```
1. FOR EACH packet received DO
2.   IF  pkt_dest_address  NOT  EQUAL  TO
current_node
3.    Pkt_counter++
4.    END IF
5.    IF CI Expired THEN
6.      PDR= C_Pkt_counter /C_expected-packets)
7.      C_Pkt_counter =0;(reset variables)
8.    IF PDR < Cong_TH THEN
9.         Send PDR to child nodes
10.    END IF
11.   END IF
12. END
```

Pkt_counter: to count the pkts received

Cong_TH: congestion threshold

Figure 3. 1 Congestion detection algorithm

Moreover, the congestion mitigation is done by splitting of information over two routing paths is performed on the immediate child of the congested node. Moreover, it is triggered once a child node receives a DIO message containing congestion notification.

From his mentioned results, the throughput of M-RPL is significantly better than RPL, It is evident that as the data rate is decreased (1 pkts per two sec) the performance of RPL gets better because congestion is not severe. In addition, the latency of both the protocol is high. Also, it is noticeable that the delay of M-RPL is similar to RPL initially.

As a conclusion, from this work multiple paths are created by splitting forwarding rate on both preferred parent (congested node) and alternate parent available in RPL also, M-RPL is capable of supporting higher data rates, and this RPL extension does require significant changes in the original protocol.

Solution 3: (M-RPL3)

In the case of heavy network load, RPL network suffer from network congestion, rapid consumption of key node energy and high packet loss rate.

The authors in [27] propose a multipath routing optimization strategy for RPL, which is named M-RPL, it provides redundant links to improve the reliability of data transmission in the network, and increase network stability, all of this with a load balancing algorithm.

Simulation results show that this optimization can handle well the situation of unstable links and network congestion, reduce the packet loss ratio and average time delay of the network, and improve the performance of LLNs.

Solution 4: (SRPL)

RPL is vulnerable to a number of attacks related to exchanged control messages such as hello flooding, blackhole attack, … for that the authors propose in [28] a new secure routing protocol based on RPL referred to as Secure-RPL (SRPL). The main aim of SRPL is to prevent misbehaving nodes from maliciously changing control message values such as the rank of a node that may disturb a network by creating a fake topology.

The goal of this protocol is to build a secure communication overlay encompassing the majority of internal rank attacks while bounding the rate rank change, based on the rank threshold concept that will be assigned to each node through strict authentication measures

The results mention in this work show that SRPL is very effective in protecting the network against attacks based on rank but it cannot resist against some type of attacks that brings the authors to highlight other types of settings, other than rank, which means that every protocol has its vulnerabilities.

IV. Comparison:

In this part we compare the related solutions with the ordinary RPL according to many metrics, so we can see the advantages and inconvenient of every solution.

Table 3.1 Comparison between related works

Solution	Energy consumption	Packet delivery ratio	Generated traffic	Number of routes per traffic
Ordinary RPL	normal	normal	normal	1
[25]	Below normal	Above normal	normal	N >2
[26]	Above normal	Good	Big with delay	2
[27]	Near critical	Good	Normal with reduced delay	2
[28]	Above normal	Very good	Normal with large delay	1

V. Conclusion:

In this chapter we have presented some routing attacks in IoT, and we see some related solutions of secure routing in this context, also we compare those solutions according to some criteria, we conclude that each one of them is good in some points, and bad in some points.

Chapter four:

Scope of our solution and evaluation

I. Introduction:

Routing is one of the most important operations in LLN as it deals with data delivery to base stations. Routing attacks can cripple it easily and degrade the operation of LLNs significantly. Traditional security mechanisms such as cryptography and authentication alone cannot cope with some of the routing attacks as they come from compromised nodes mostly.

Many routing protocols are proposed to secure routing, in which they consider different routing attacks. In this chapter, we see how we secure multipath routing basing on RPL protocol and we see how it is the efficiency of multipath in routing.

II. Multipath routing:

1. Definition:

Multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other. Extensive research has been done on multipath routing techniques, but multipath routing is not yet widely deployed in practice. [29]

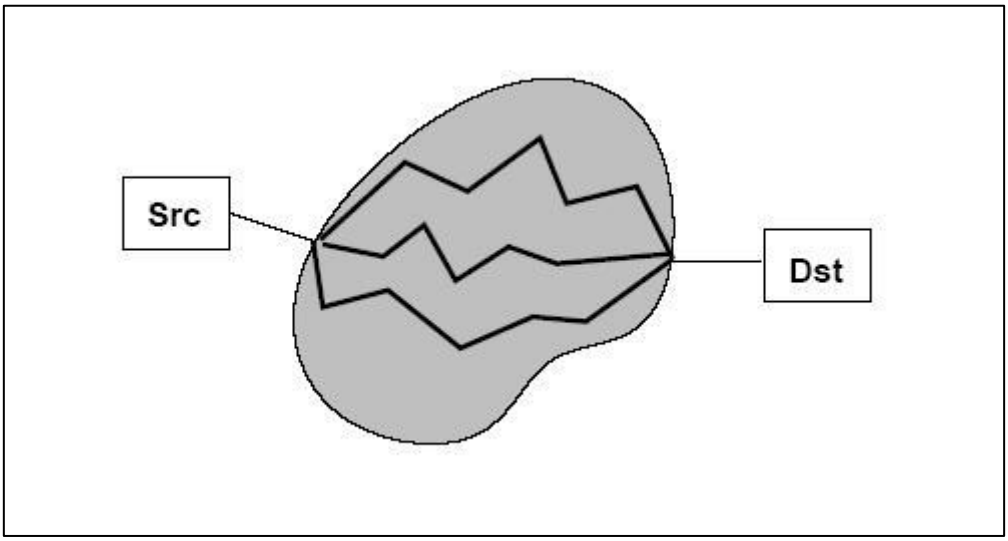

Figure 4. 1 Multipath Routing Model Diagram.[29]

2. Importance of multipath routing:

- QoS, throughput, and delay are difficult problems with current single-path routing architecture.
- From queuing theory, we know that through increased sharing, overall utilization of the entire network is improved.
- Multipath routing provides much better overall network performance by allowing better sharing of the available network resources.
- The use of the Internet is growing at an incredible rate.

3. Multipath Components:

There is three multipath's components:[29]

a) A Multipath Calculation algorithm to compute multiple paths.
b) A Multipath Forwarding algorithm to ensure that packets travel on their specified paths.
c) An End-Host_Protocol that effectively uses the determined multiple paths.

III. Secure multipath routing in IOT

1. Description of our solution:

RPL is a single path routing protocol and the existing objective functions do not support creation of multiple routing paths between source and destination. Multipath routing can be used to achieve multifold objectives, including higher reliability, increased throughput, fault tolerance, congestion mitigation and hole avoidance.

So, we propose to use a node that are specifically for forwarding packets in multiple paths, those nodes called "intermediate nodes" its situated generally in the middle of route, between the source nodes and the destination node.

These nodes forward their received packets into multiple paths, so if there is an attacker in one of these paths the packet will find a way to the destination by the other route. The following figure shows an example of these scenarios:

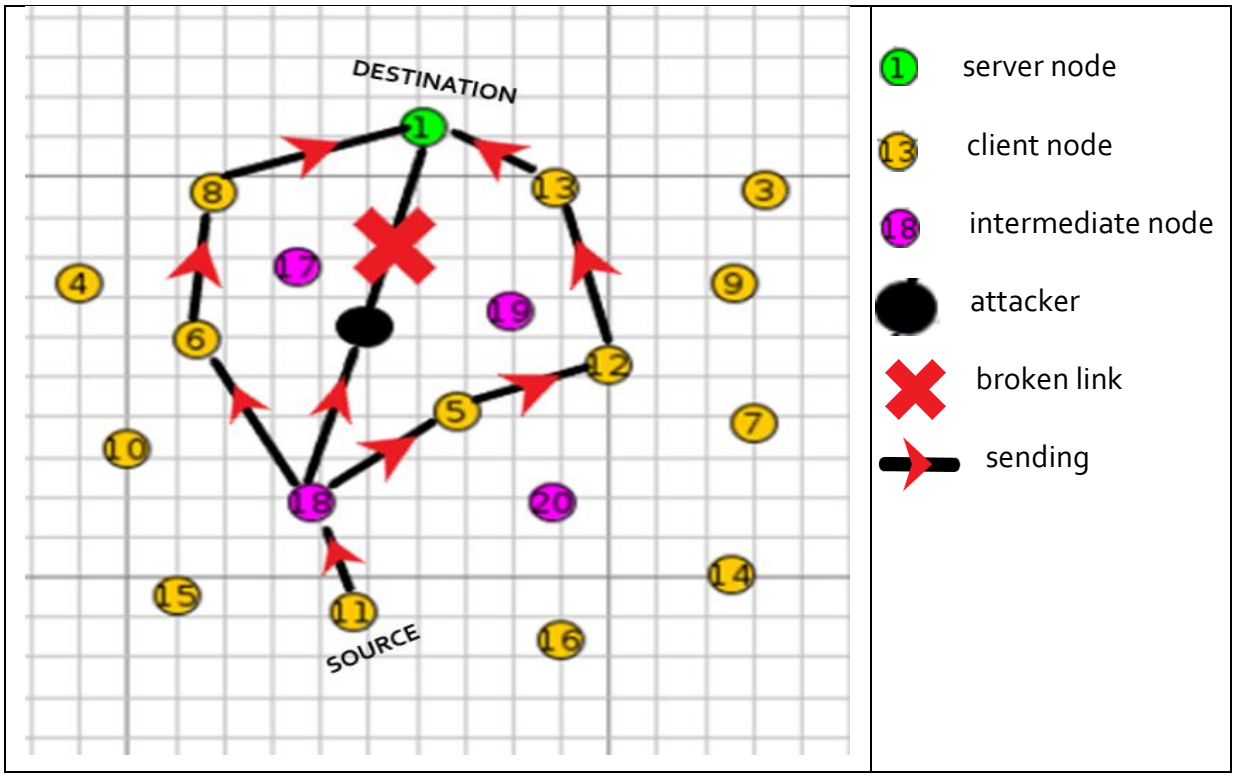

Figure 4. 2 Overview of proposed solution

2. Network model:

Source node

This type of nodes generally is client node send packets to server node, these nodes use RPL as a routing protocol, and it forwards packets.

Destination node

These nodes may be clients or server; may receive data, or rpl messages.

Multipath Intermediate node

The main purpose of these nodes is forwarding randomly received packet to a group of neighbors' nodes.

3. Security context of our solution:

In our solution we used a symmetric encryption algorithm, which is AES, because it uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence, it makes AES algorithm more robust against hacking also for 128 bits, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.

Advanced Encryption Standard (AES):

The AES algorithm is a symmetric-key block cipher in which both the sender and receiver use a single key to encrypt and decrypt the information.[30]

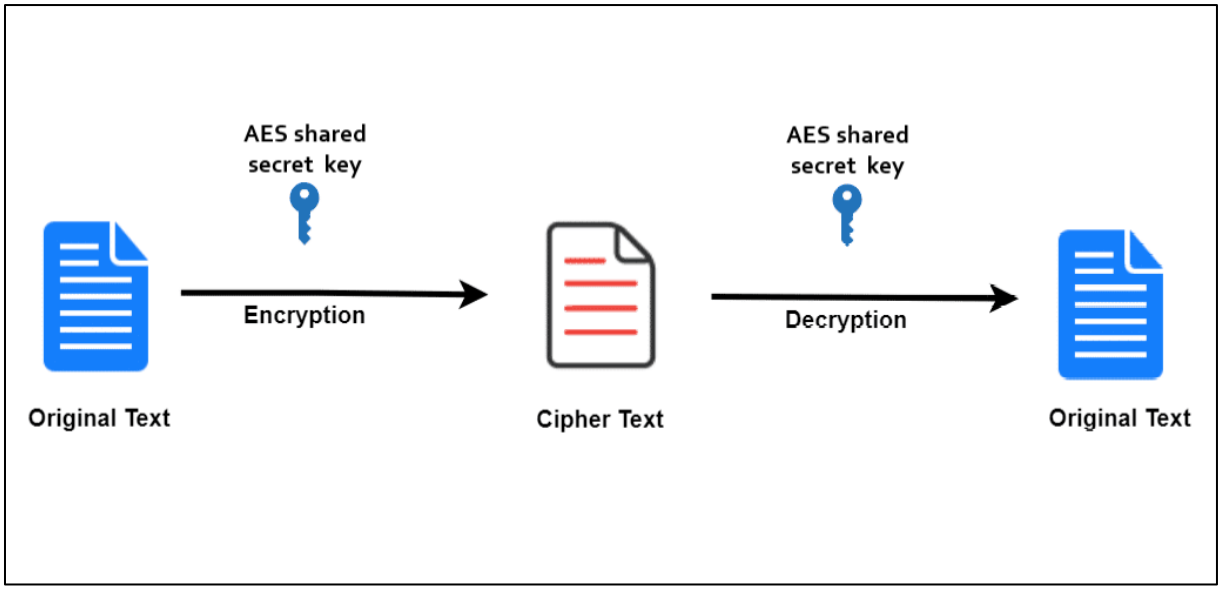

Figure 4. 3. AES algorithm design

How we use AES:

Each node of our network shares a secret key with the 6BR (ipv6 border router) so every communication going to encrypted by this key, so it is End-to-End encryption.

4. Modeling of our solution:

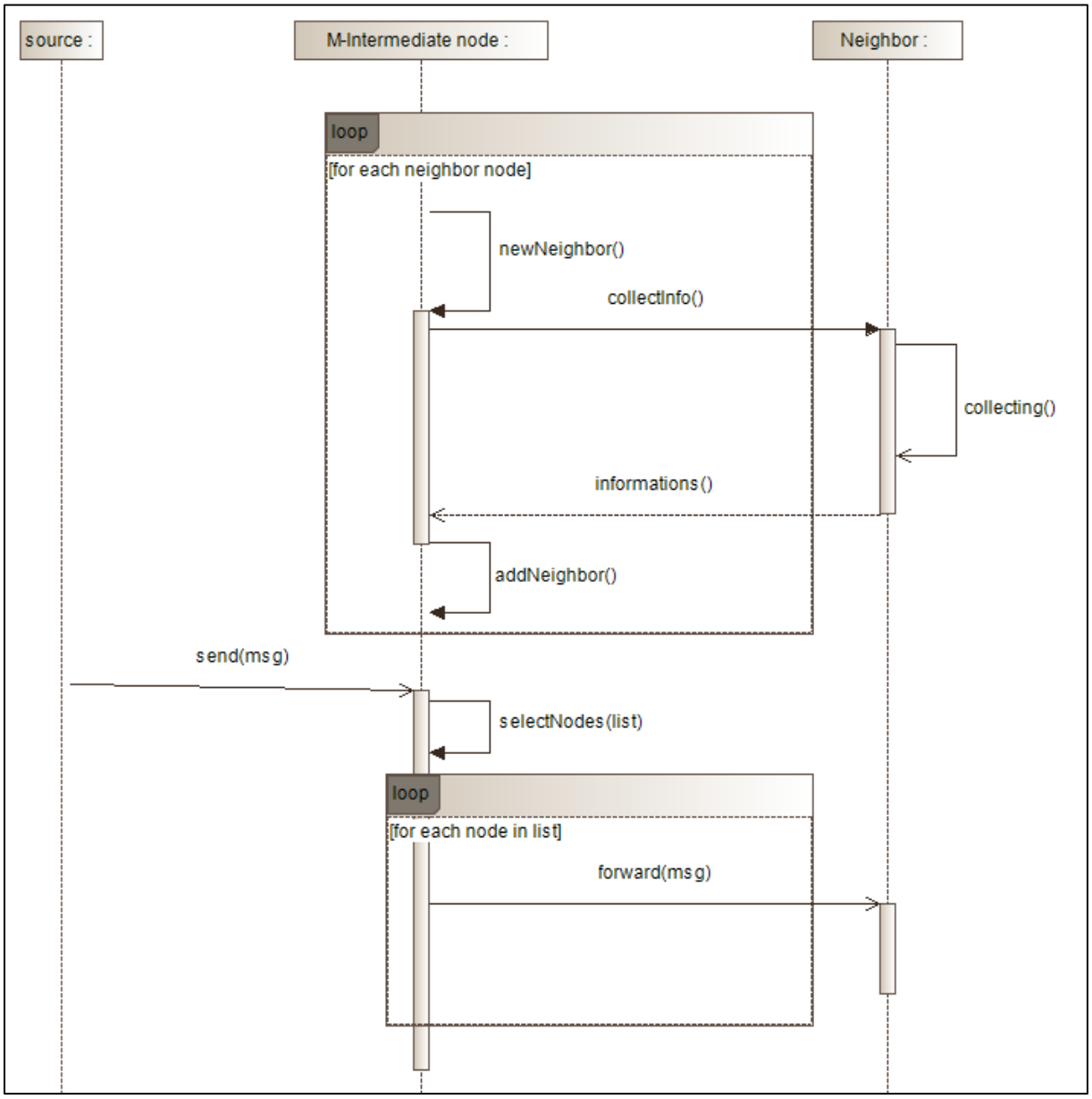

Figure 4. 4 Sequence diagram of multipath intermediate node behaviors

In Fig 4.4 the M-Intermediate node initiate himself by gathering information from them, then it creates a list with this information, this operation done while the construction of the network.

After that, when it receives a message, it will choose a list of nodes where the message will be forwarded, this message continues his path to the destination using multihop by RPL.

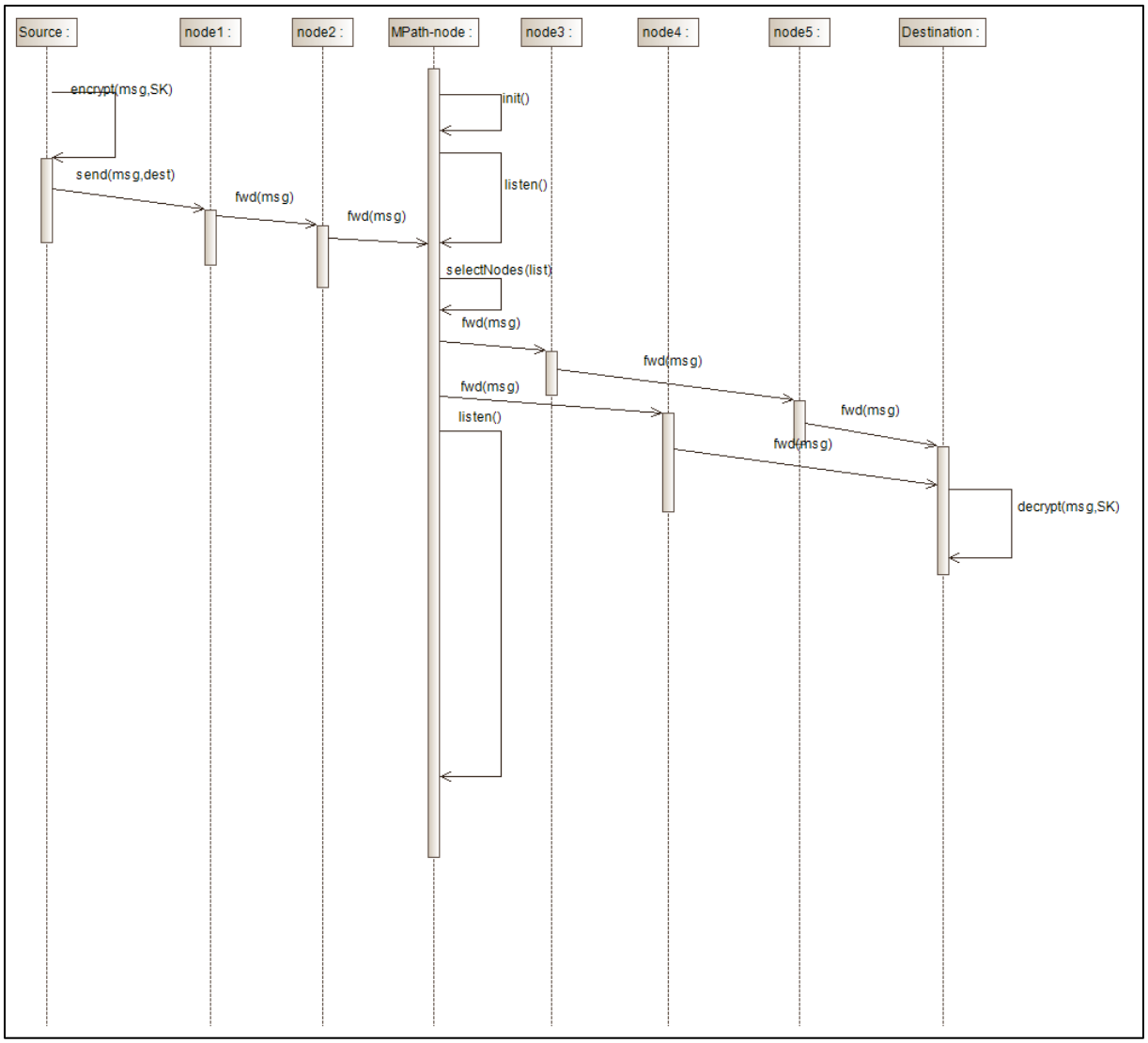

Figure 4. 5 Routing scenario example

In Fig 4.5 we see a scenario of routing from the source to the destination .First, the source encrypt his message using the secret key(SK) between him and destination ,then it send ,this message following his route on multihop using rpl, when it reach an Multipath intermediate node(MPath-node) it will be forwarded into multiple routes, finally the message reach the destination ,it will be decrypted using (SK).

IV. Simulation

1. COOJA simulator:

COOJA is a flexible Java-based simulator designed for simulating networks of sensors running the Contiki operating system, COOJA simulates networks of sensor nodes where each node can be of a different type; differing not only in on-board software, but also in the simulated hardware.

2. COOJA setup:

First need to visit the Contiki website [31] in order to download Instant Contiki. Once the Instant Contiki image has been downloaded and unzipped, it can be opened using VMware. Instant Contiki is an Ubuntu based operating system with Cooja already built in and ready to use.

To start the simulation software, open a terminal window and enter the following commands:

> cd contiki/tools/Cooja

> ant run

3. Why we choose COOJA:

- COOJA network simulator enables the emulation of different kinds of nodes and how the routing matrices are computed.
- Cooja has the advantage that the simulated source code can be downloaded and run into real nodes.
- RPL protocol is well implemented in COOJA with large details.
- COOJA simulator has a library of useful examples for each type of WSN.

4. Simulation parameters:

Table 4. 1 Simulation parameters

Parameter	Value
Network Layer	RPL/ M-Path-RPL
MAC layer	802.15.4
Topology	Random
Simulation time	10min
Objective function	RPL-mrhof
TX range	20m
Interference range	25m

5. Performance metrics:

- Energy consumption.
- Packet delivery ratio (PDR).
- resilience against routing attacks (estimation of overall PDR over increasing amounts of attackers).

V. Results and evaluation

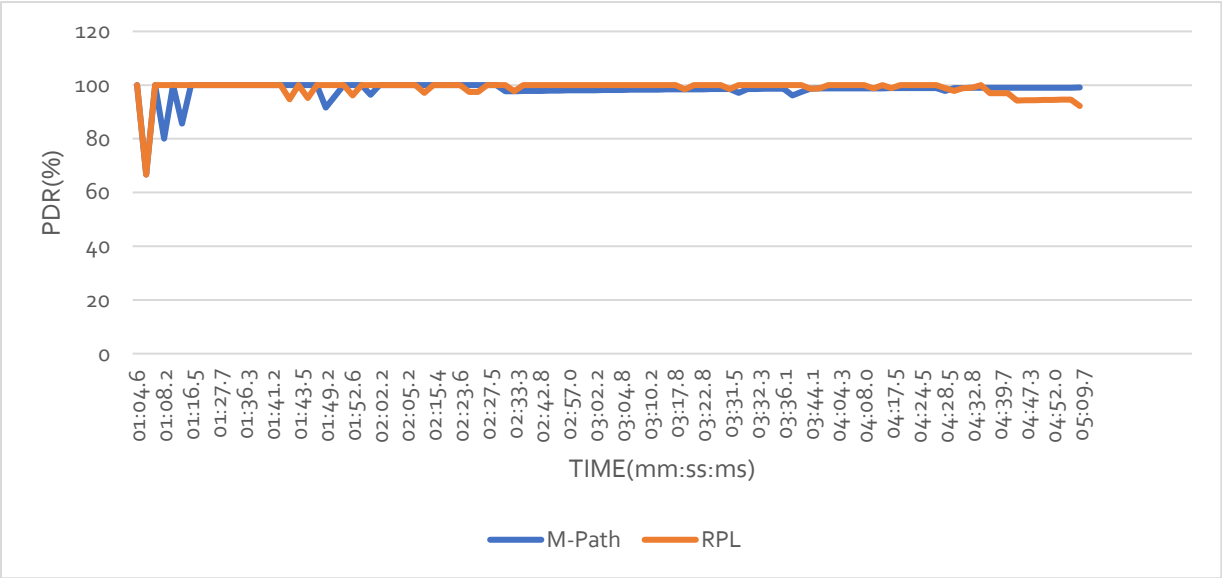

Figure 4. 6 PDR overall network without attack

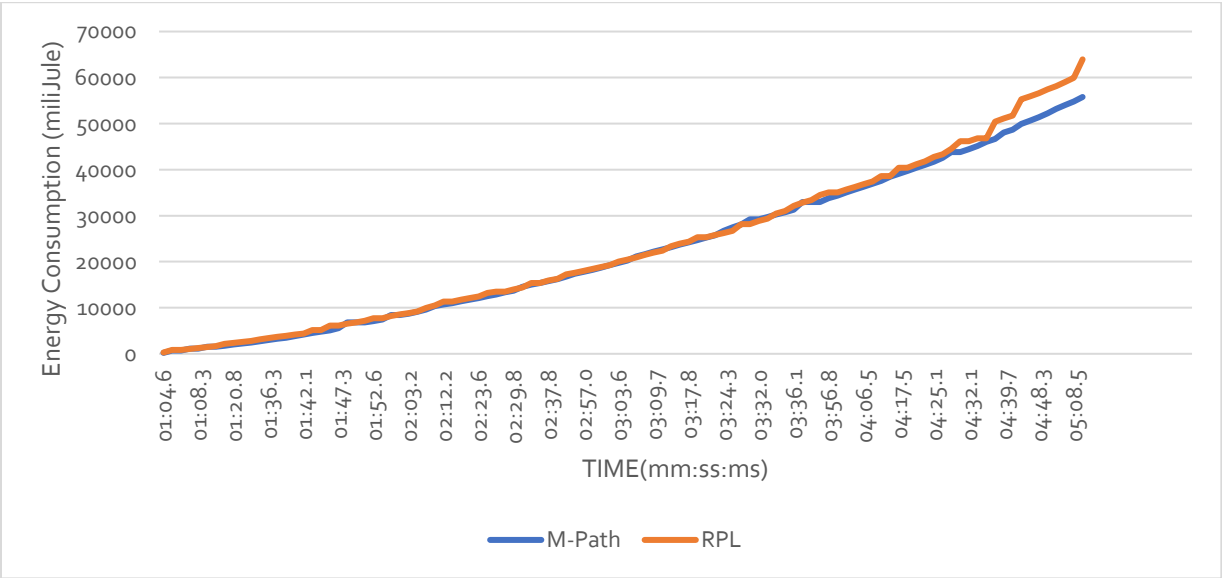

Figure 4. 7 Energy consumption overall network without attack

From Fig4.6 it shows that's the PDR it's the same in our solution and RPL, also the energy consumption it near for both which is showed in Fig4.7.

Note: we didn't estimate energy for M-Path intermediate nodes, we suppose that they have enough energy to do their role.

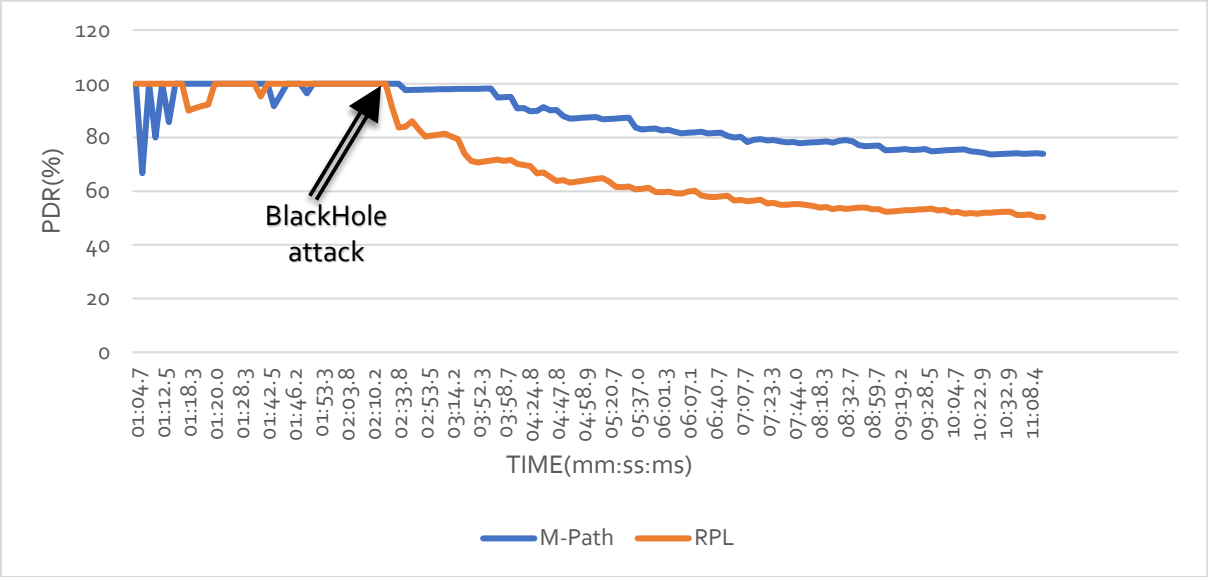

Figure 4. 8 PDR overall network in case of Blackhole attack

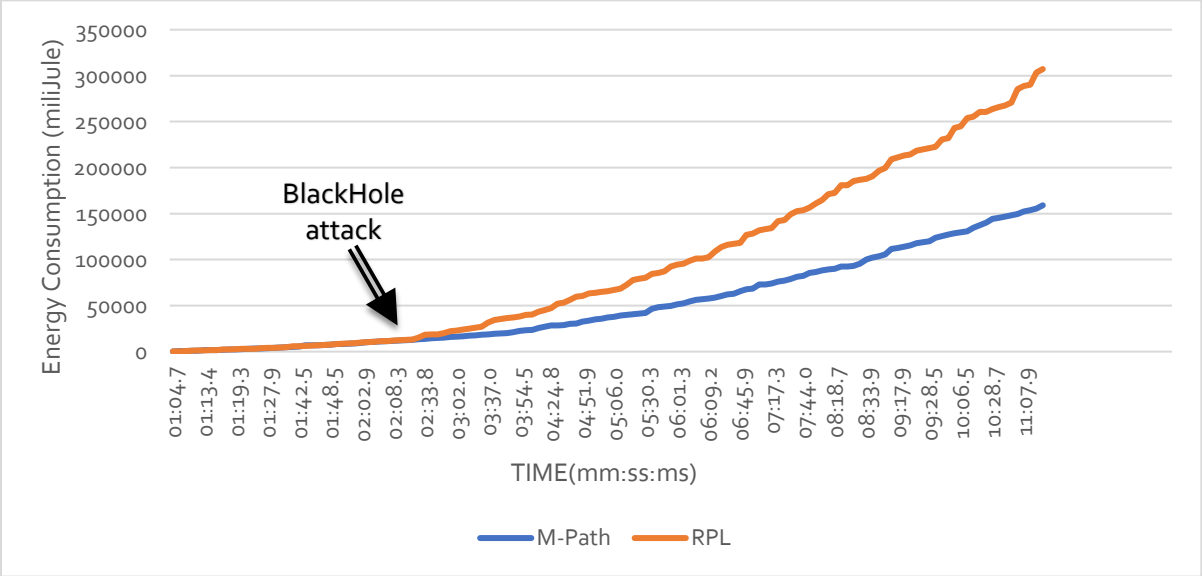

Figure 4. 9 Energy consumption overall network in case of Blackhole attack

Moreover, Fig4.9 we see that in case of blackhole attack, our protocol reaches 78% of PDR overall network, however RPL get the 55%, in the other hand, the energy consumed by RPL is so bigger than in our solution.

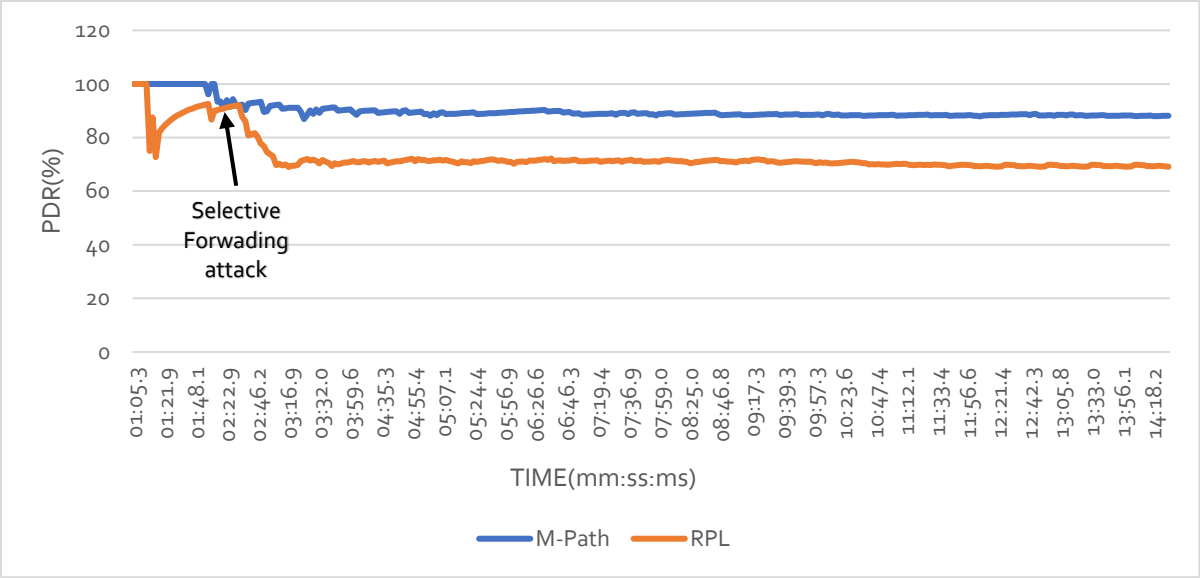

Figure 4. 10 PDR overall network in case of Selective forwarding attack

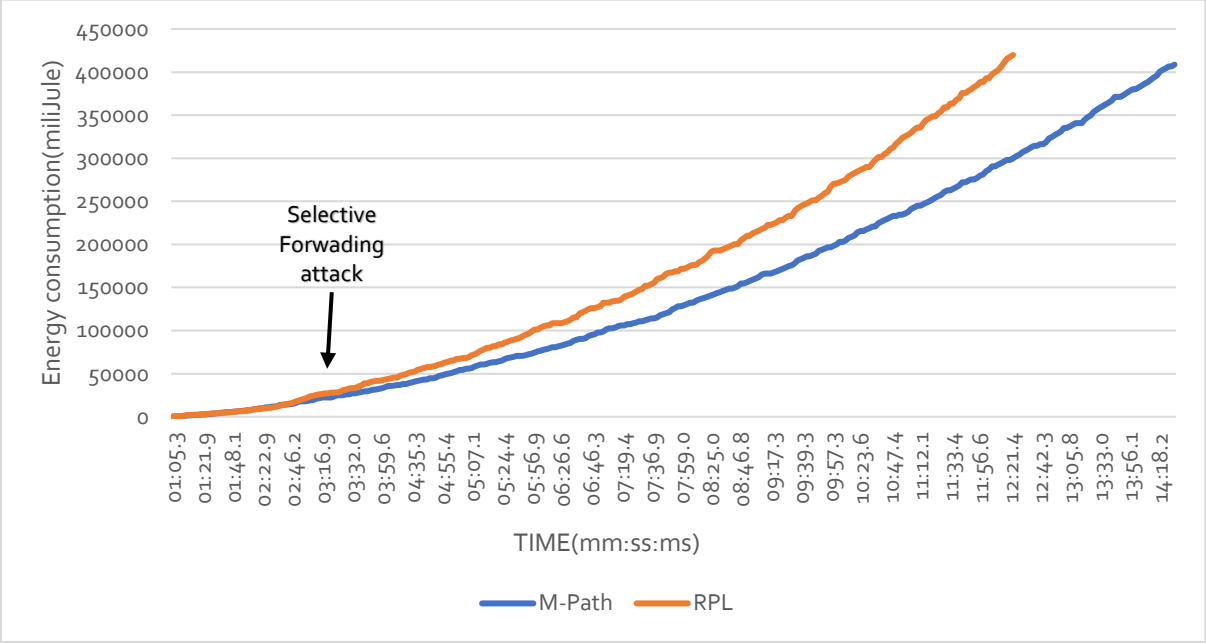

Figure 4. 11 Energy consumption overall network in case of Selective forwarding attack

Also, it mentioned in Fig4.10 that because of selective forwarding attack we have 85% PDR in our solution but in RPL it is only 75%, in side of energy consumption both protocols consume massive amount energy.

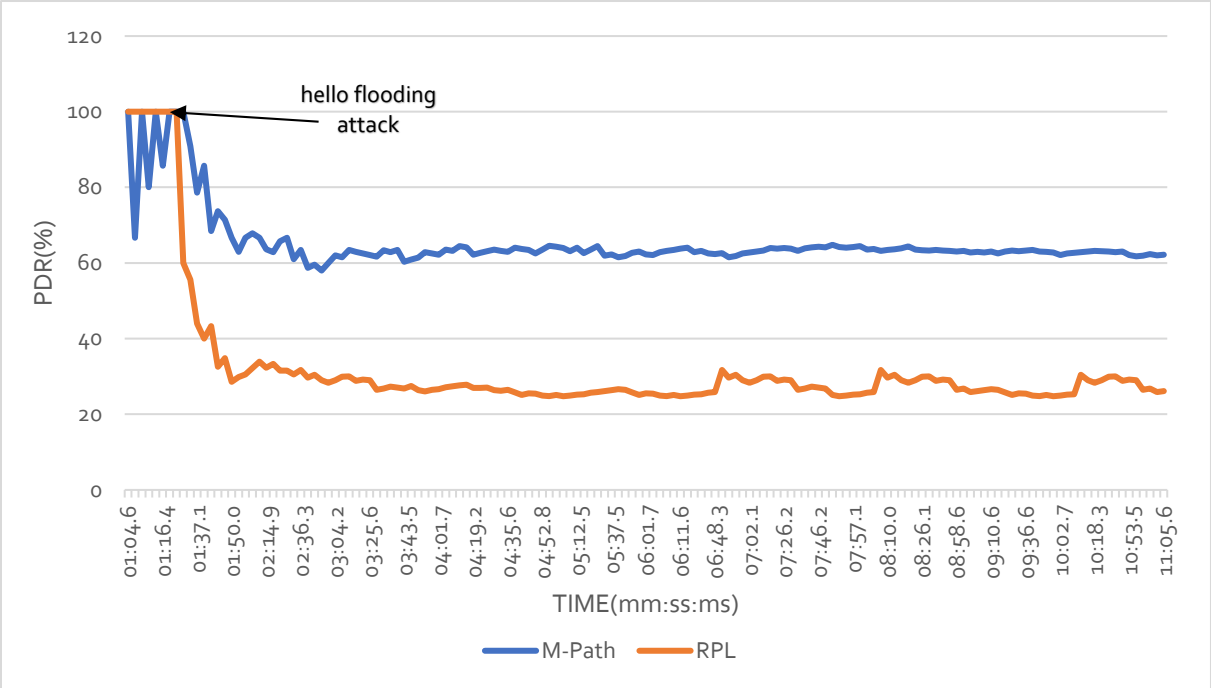

Figure 4. 12 PDR overall network in case of Hello flooding attack

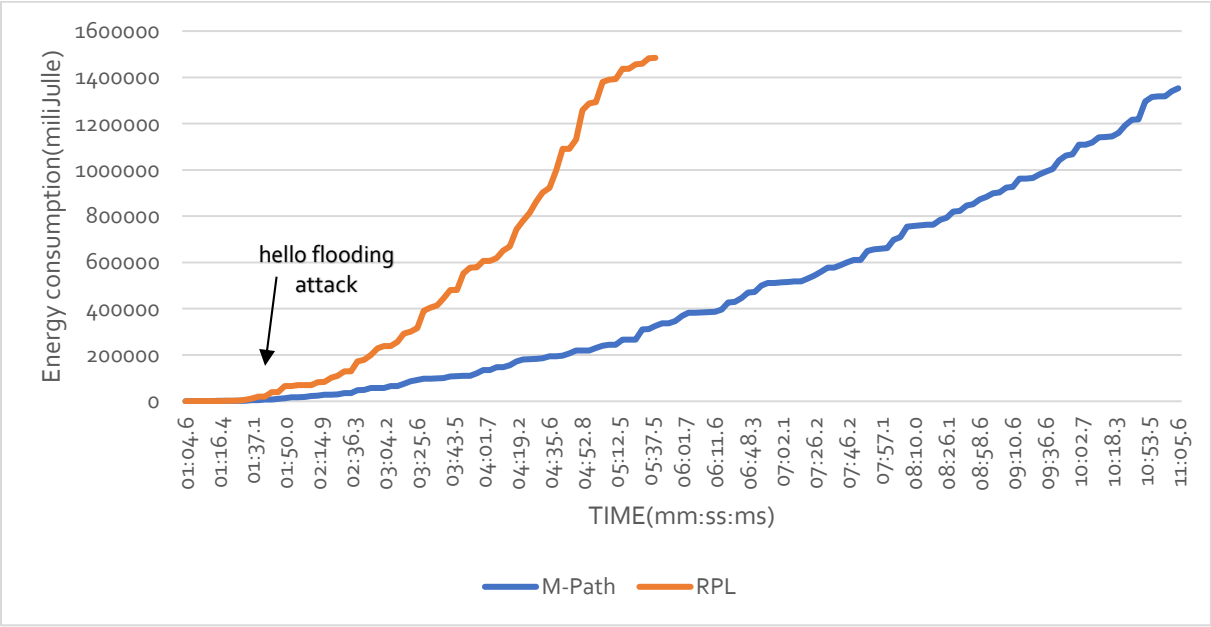

Figure 4. 13 Energy consumption overall network in case of Hello flooding attack

For the last attack, from Fig4.13 hello flooding attack is the most harmful attack it provides a huge amount of energy consumption for nodes for both protocols. Moreover, our solution stack at 60% of PDR, however RPL only decreases to 32% of PDR.

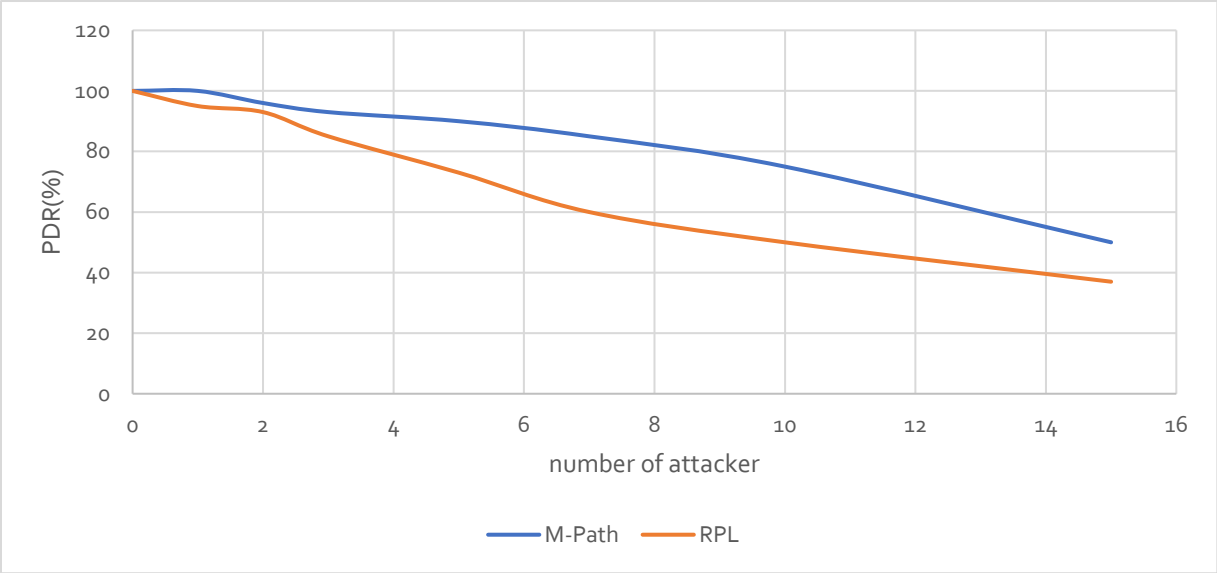

Figure 4. 14 Resilience against blackhole attack

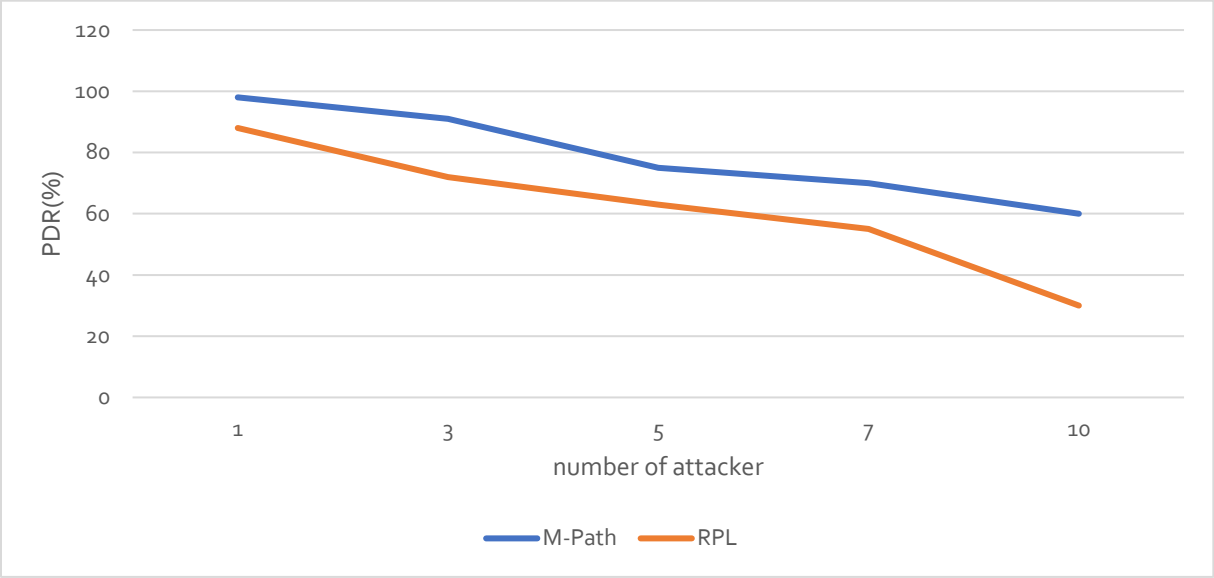

Figure 4. 15 Resilience against hello flooding attack

Fig4.14 and Fig4.15 show that increasing the number of attackers provides a falling in PDR, also our solutions resist more than RPL in the two cases (blackhole and hello flooding attack), in addition, we should mention that hello flooding has the bigger impact of reducing PDR and increasing energy consumption overall network.

VI. Conclusion

In this last chapter, we have seen how to use multipath RPL for security, and we presented an overview about our solution. Additionally, we introduced Cooja simulator, as well as the evaluation context. The obtained results show that our designed multipath RPL performs better than ordinary RPL against last used attacks.

General Conclusion

Throughout this work, we have introduced internet of things by focusing on its characteristics, architecture, enabling technologies, protocols, application domains as well as its main challenges.

LLN is a network composed of embedded devices that are limited of resources as power, storage space, processing capacity, energy storage and so on. For this reason, the working group researched and formulated the RPL (Routing Protocol for LLN) which proved its worth through its flexibility and extensibility via a single path. However, it is exposed to security vulnerabilities as HELLO flood attacks, spoofed attacks…

Finally, we were able to carry out an adaptation of a RPL protocol aiming to guarantee the security of the network by integrating a symmetric encryption (AES) besides the multipath approach. The resulting protocol has shown its performance in reducing power consumption while keeping data transmission within agreed limits.

As future work, we think that with a probabilistic multipath routing for RPL, we could achieve better performance, especially those related to energy consumption.

Bibliography

[1] O. V. SINTEF, N. Peter Friesseu, "Internet of Things–From Research and Innovation to Market Deployment", river publishers' series in communications, 2014.

[2] [http://www.reloade.com/blog/2013/12/6characteristicswithin-internet-things-iot.php].

[3] [https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf] [Accessed 11 2019].

[4] D. Mendez, I. Papapanagiotou and B. Yang, "Internet of Things: Survey on Security and Privacy," Cornell University Library, 2017.

[5] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Computer Communications, vol. 54, pp. 1-31, 2014.

[6] Routing Protocol for LLN (RPL) Configuration Guide, Cisco IOS Release 15M&T Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/rpl/configuration/15-mt/rpl-15-mt-book.html#concept_442C4259376346D5958C3A812412967D [Accessed 13 December 2019]

[7] K. Ashton, "RFID Journal," June 2009. [Online]. Available: http://www.rfidjournal.com. [Accessed 23 November 2019].

[8] GS1 EPC Tag Data Standard 1.6, 2011. [Online]. Available: https://www.gs1.org/sites/default/files/docs/epc/tds_1_6-RatifiedStd-20110922.pdf. [Accessed 11 2019].

[9] "ILNAS White paper Digital Trust for smart ICT," October 2016. [Online]. Available: https://portail-qualite.public.lu/fr/publications/confiance-numerique/etudes/white-paper-digital-trust-october-2016.html.

[10] J. S. Wilson, "Chapter 1 - Sensor Fundamentals, In Sensor Technology Handbook," in In Sensor Technology Handbook, www.sciencedirect.com, 2005, pp. 1-20.

[11] J. S. Wilson, "Sensors Fundamentals," in Sensor technology Handbook, Elsevier, 2014.

[12] S. Alam, M. M. Chowdhury and J. Noll, "Interoperability of security enabled internet of things," Wireless Personal Communications, vol. 61, no. 3, p. 567–586, 2011.

[13] R. Roman, J. Zhou and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, p. 2266–2279, 2013.

[14] 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," Wireless Communications, IEEE, vol. 20, no. 6, p. 91–98, 2013

[15] Topologies in IoT , Available: http://radar.oreilly.com/2014/04/3-topologies-driving-iot-networking-standards.html [Accessed 13 December 2019]

[16] Constrained Networks [Online], Available: https://ldapwiki.com/wiki/Constrained%20Networks ,[Accessed 14 December 2019]

[17] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," Wireless Communications, IEEE, vol. 11, no. 6, pp. 6–28, 2004.

[18] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, vol. 8, no. 2/3, pp. 169–185, 2002.

[19] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application specific protocol architecture for wireless microsensor networks," Wireless Communications, IEEE Transactions on, vol. 1, no. 4, pp. 660–670, 2002.

[20] Z. Shelby and C. Bormann, 6LoWPAN: the wireless embedded internet. Wiley, 2010, vol. 33.

[21] T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, and J. Vasseur, "RPL: IPv6 routing protocol for low power and lossy networks," Work In Progress), http://tools. ietf. org/html/draft-ietf-roll-rpl-11, 2010.

[22] Z. Shelby, C. Bormann, and D. Sturek, "Constrained application protocol CoAP," orgiddraftietfcorecoap01 txt 0807, pp. 1–81, 2011.

[23] RFC4101, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks draft-ietf-roll-rpl-04"

[24] RFC6550," RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks"

[25] Bogdan Pavkovic, Fabrice Theoleyre, Andrzej Duda, "Multipath Opportunistic RPL Routing over IEEE 802.15.4" MSWiM'11, October 31–November 4, 2011, Miami, Florida, USA.

[26] M Ali Lodhi , Abdul Rehman , Meer M Khan , Faisal Bashir Hussain, "Multiple Path RPL for Low Power Lossy Networks" , 2015 IEEE Asia Pacific Conference on Wireless and Mobile

[27] Weisheng Tang , Zhi Wei , Zongjie Zhang and Bo Zhang "Analysis and Optimization Strategy of Multipath RPL Based on the COOJA Simulator " IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 5, No 1, September 2014

[28] Ghada Glissa , Abderrezak Rachedi , Aref Meddeb , "A secure routing protocol based on RPL for Internet of Things (SRPL)" , 2016 IEEE Global Communications Conference (GLOBECOM) , 4-8 Dec. 2016

[29] S.-J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," Proc. ICC 2001, vol. 10, pp. 3201–3205, June 2001.

[30] "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, November 26, 2001.

[31] Contiki, "Contiki: The Open Source Operating System for the Internet of Things," 2020. [Online]. Available: http://www.contiki-os.org/. [Accessed: 09-Dec-2019].