EAI Endorsed Transactions
on Internet of Things
Research Article
EAI.EU

IoT Short-range Network protocols: Analytical study and operating models

Sakina Elhadi[1], Abdelaziz Marzak[1] and Nawal Sael[1]

[1]Laboratory of Modelling and Information Technology, Faculty of sciences Ben M'SIK, University Hassan II Casablanca, Morocco

Abstract

Internet of Things (IoT) is a constantly evolving concept. Nonetheless, we can consider that the Internet of Things broadly refers to the trend towards generalized interconnection of all the objects that surround our daily lives, places and physical environments. Among the success keys of Iot there are protocols. However, the lack of a single connectivity protocol causes a lack of interoperability between IoT devices and applications. In this article, we present a detailed comparative study of the Short-range network protocols. Then, we will present the operating models of these protocols. There models facilitates the in-depth understanding of how network protocols work. Subsequently, from our comparative study already established and these proposed models we determine the priority of the criteria of these protocols. Using the projection of these criteria on the proposed operating models. This will help to choose the adaptable protocol for a type of IoT applications.

Keywords: Internet of things, IoT, operating models, Network protocols, the activity diagram.

Received on 11 December 2020, accepted on 28 January 2021, published on 16 February 2021

doi: 10.4108/eai.16-2-2021.168717

1. Introduction

The Internet of Things (IoT) is a new technology developed in recent years where the interconnection between the Internet and physical objects. IoT applications cover a multitude of fields, ranging from large industrial applications to small daily uses. These applications connect in real time and transfer different information. Therefore, there is around us a range of objects capable of collecting, sending and processing data and communicating with each other using several technologies, namely: Big data, cloud computing, protocols, etc. So, One of the main aspects of IoT is the communication between the different components of the global system thanks to a set of network protocols, such that there are a variety of standards and protocols to allow physical objects to interact with each other, thus secure transfer of information from IoT devices. However, the diversity of network protocols offered in the market by organizations and researchers requires a careful study of the operation of the protocols that we will adapt to our applications.

Each protocol must be able to meet a few stringent requirements. It should be able to provide functionality to the right Procedure. There are several requirements that allow us to evaluate a protocol. First, the protocol must therefore have functionality that allows its data format management. Secondly, during the data transmission procedure, it would be necessary to manage address format and data routing. Thirdly, a protocol should be able to detect these errors. Therefore, to manage the loss of information. Finally, the protocol must ensure direction of information flow and Sequence control. Etc.

In this article, we wanted to deepen this question by proposing operating models of three different network protocols at first. This study facilitates the understanding of the function of network protocols by using Uml modelling. This will help to choose the protocol adaptable to a type of IoT application.

The remainder of this document is organize as follows: Section II presents the Network protocols. Section III, presents the comparative study of network protocols IoT. Next, in section IV we propose some models of Operating network protocols. We conclude our study by Section V.

[*]Corresponding author. Email: Elhadi.sakina1993@gmail.com

2. Network protocol

Network protocols and standards is a specification of several rules for a particular type of communication between two or more devices on the network. IoT protocols are one such system that will transfer safely data over the Internet. It will transfer the data when the communication network between the two devices is connected. On the one hand, there are the general protocols used by personal devices that do not reply specific requirements of the IoT application. On the other hand, there are some improved versions of existing protocols and new IoT protocols have evolved to meet the requirements of IoT devices. We classified network protocols into three categories:
Short-range protocols: Bluetooth, Zigbee, NFS.
Medium range protocols: Z-Wave, Wifi .
Long-range protocols: LoRa , Cellular ,Sigfox , Neul.
In this section, we present the most used and important network Short-range protocols for the internet of objects.

2.1. Zigbee

Zigbee is an IEEE radio communication protocol based on 802.14.4, considered an important technology for IoT of home automation applications. In 2005, his birth is to accept for the IoT. December 14, 2004, The IEEE 802.15.4-2003 Zigbee specification ratified. With an average range of 10 meters. It uses low bandwidth, thus it is ideal for transferring data in low volume. It designed to operate in a mesh network: each node receives, sends and relays data [1]. Duty cycle is an important concept for both Zigbee and other low-power protocols. The results of several researches are that the quality of service (QoS) is better with a high duty cycle, but the energy consumption is also better with a low duty cycle [2].

2.1. Bluetooth

Bluetooth invented in 1994 by the Swedish company Ericsson. The Special Interest Group (SIG) is developing it where they have published Bluetooth 5 in order to adapt these protocols to IoT [3]. This technology is part of wireless communications. Bluetooth protocol allows two-way wireless data transfer and exchange at very short distance using UHF radio waves on a 2.4 GHz frequency band. It uses low bandwidth. Consequently, Bluetooth allows the transfer of a small amount of data at short distances. Furthermore, it offers a low energy solution and low cost for UHF radio transmissions at short range. Bluetooth used in many applications and IoT devices: smart watch, automated smart homes, Cell phones, automobiles, etc. Bluetooth is easy to use, install and adapt, but has low security [4] [5].

2.3. Near Field Communication (NFC)

The NFC protocol is an extension of ISO / IEC 14443 standardizing proximity cards using RFID [6]. So, it based on Radio frequency identification technology. NFC is a standard for wireless radio frequency communication short range and high frequency with small quantity. As such, it has a read-only tag. This tag contains a small amount of data, which can changed later by the object. It allows the exchange of information between devices up to a distance of approximately 10 cm. Furthermore, NFC provides identification, simple and two-way communication between two electronic objects equipped with an RFID chip. These objects have a label and automatically identified by radio frequency. NFC is widely used to control IoT devices in different environments such as smart home, badges for commercial premises, factory and industrial applications [7] [8].

3. Comparative study

In a previous work, we presented a comparative study of the different networks and network protocols [9]. In particular, it focuses on network Short-range protocol. This study evaluates the capabilities of their main characteristics and behaviours in terms of various metrics of these protocols.
We classify the criteria of the protocols according to three categories are:
Specification of protocols: Specification, Cost, energy consumption.
Network criteria: Network type, Topology, Power, Network size.
Data management evaluation criteria: Data Rate, Bandwidth (designate the maximum bit rate of a transmission channel), Technical Modulation (for adapting the signal to be transmitted to the transmission channel), Spread Spectrum (are signal transmission methods), Range, Security, Risk of data Collision (where data packets can collide with each other).

Table 1. Short-range network protocol

Protocols Criteria		Short range		
		NFC	Bluetooth	Zigbee
Specification of protocols	Specification	ISO/IEC 18000-3	Bluetooth 4.2 core specification	ZigBee 3.0 based on IEEE802.15.4
	Cost	Chip	Low	good
	energy consumption	Low	Low	Low
	Application	Payment Transactions, Business Transactions, Contextual Information	Network for data exchange headset	Senor networks Industrial automation
Network criteria	Network type	P2P	LAN	LAN
	Topology	Mesh	Star	Mesh,Star, Tree
	Power	Very Low	Low	Very Low
	Network size	Small	Small	Very large
Data Management criteria	Data Rate (Gbps)	424 kbits /s	2.1Gbps	250 Gbps
	Frequency band	13.56 MHz	2.4 G Hz	868/915 M Hz, 2.4 G Hz
	Technical Modulation	ASK	GFSK, CPFSK, 8-DPSK, π/4-DQPSK	BPSK, O-QPSK
	Spread Spectrum	FHSS	FHSS	DSSS
	Range	5cm	<100m	10-20m
	Security	Cryptography	Shared secret	CBC-MAC (ext. of CCM)
	Risk of data Collision	Low	High	Medium

4. Operating models

In this section, we will present the modeling of the operation of the following network protocols: Bluetooth, Zigbee, NFS. This model was develop by activity diagram. This diagram represents the triggering of events according to the states of the system, to model parallelizable behaviors, determine a priori sequential treatment. Likewise, it is use to detail the working process of the protocols from a starting point to the finishing point. These models is a continuation of work that we have already done for the application protocols [10] [11].

The activity diagram divided into swimlanes. Each corresponding swimlane is responsible for the creation of a set of activities. The swimlanes present the protocol layers. The pink colour presents the activities. The blue colour shows actions.

4.1. Operating model of Zigbee

ZigBee is structured in four layers are the physical layer (PHY), Medium Access Control layer (MAC), Network layer (NWK), and Application layer (APL).

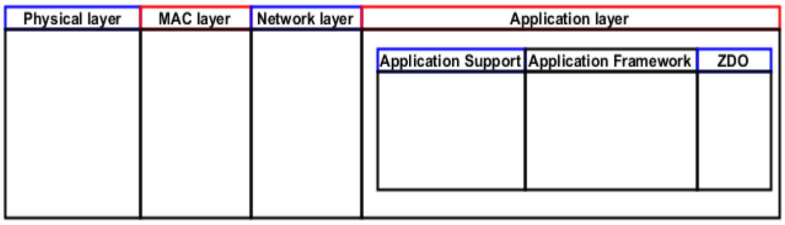

Figure 1. General-operating model of Zigbee

a) Physical and Medium Access Control (MAC) layer

The physical layer supports the management of transmission and reception frequencies, the data rate (sent or received), the type of modulation and the digitization coding of information. The Medium Access Control layer based on physical layer resources. It is main for the software aspects, which defines the way in which a node of the network will be able to dialogue (transmit or receive).

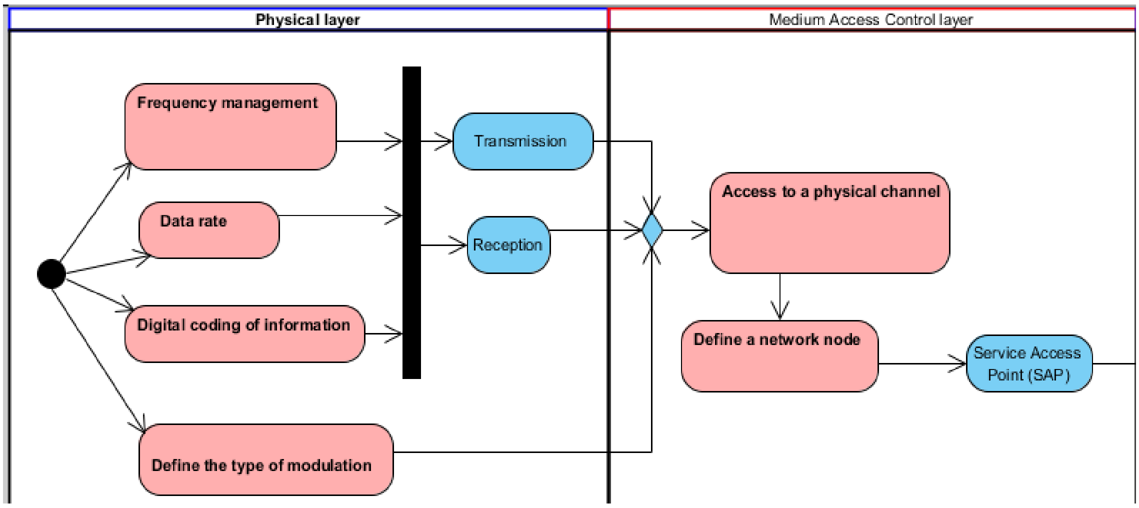
Physical layer
Medium Access Control layer
Frequency management
Data rate
Digital coding of information
Define the type of modulation
Transmission
Reception
Access to a physical channel
Define a network node
Service Access Point (SAP)

Figure 2. Operating model of Physical and MAC layers

b) Network layer

The network layer mainly provides the rules for establishing a network, the association and the interconnection of all nodes in the network, the transfer of information between the entities of this network via a route, as well as the structure of the messages that will be exchange. Moreover, network layer packets can sent in unicast, broadcast or even multicast.

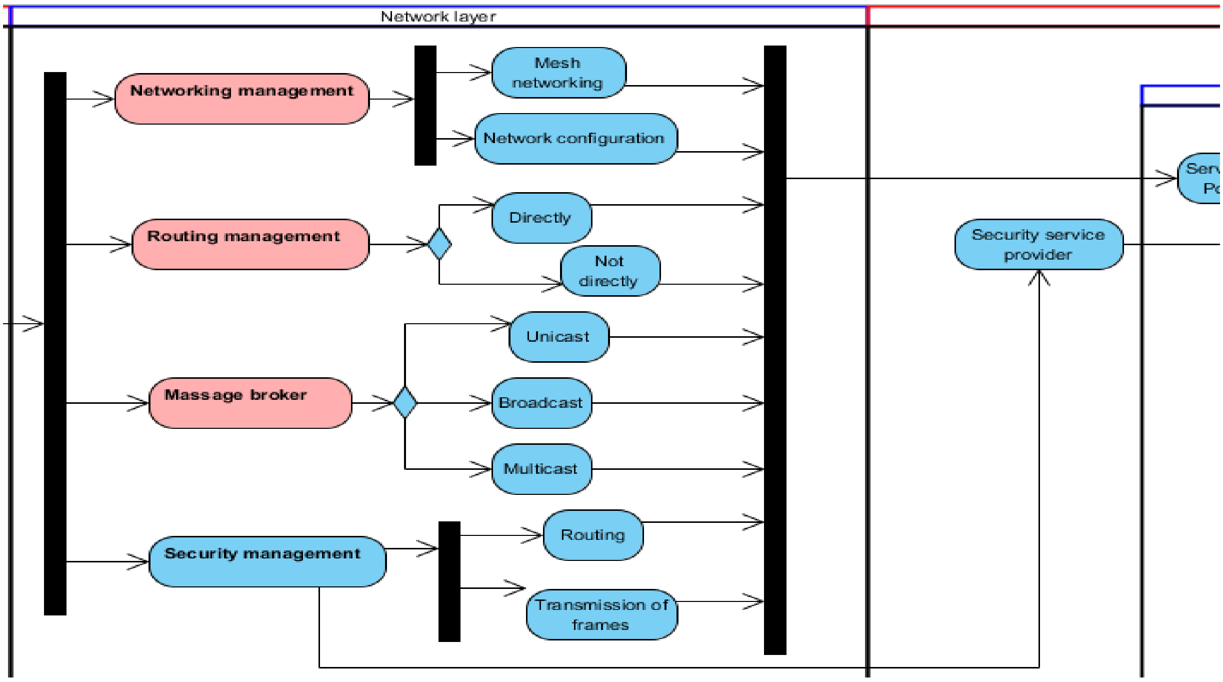

Figure 1. Operating model of Network layer

c) Application layer

The application layer uses the lower layers for a given communicating application. Among other things, it gives meaning to the information exchanged in the network. This layer is associated with four elements: the Application Support Sub-Layer (APS), the Application Framework (AF), the Security Service Provider (SSP) module, and the ZigBee Device Object (ZDO) module. Each layer provides services for the upper layer. Through a Service Access Point (SAP), every service offers an interface to the upper layer. The Application Support Sub-Layer guaranteed several features that cited in figure. The Application Framework admits different application profiles. It therefore offers APIs for developers. We do not forget that each application has an address of the ZigBee node. The ZigBee Device Object module is responsible for equipment management, role definition (ZigBee Coordinator, ZigBee Router, End device). For

Security, the Security Service Provider (SSP) module provides security services to the NWK and APS layers.

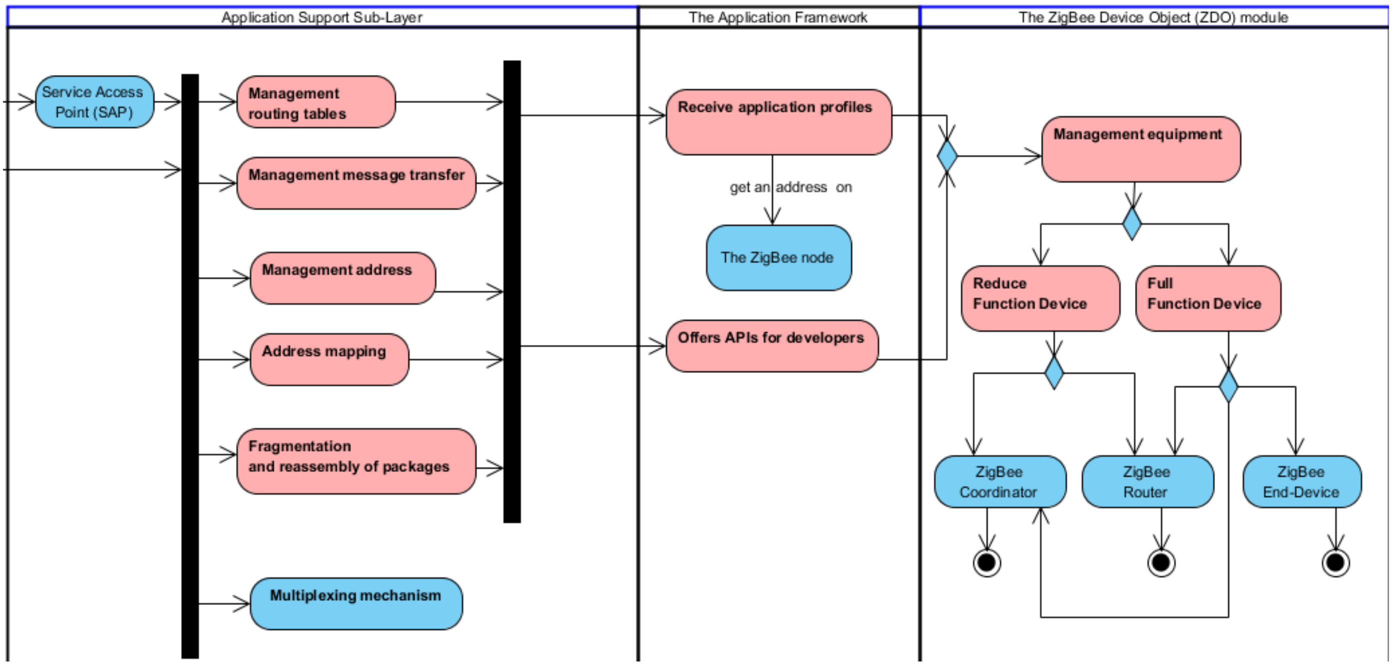
Application Support Sub-Layer
The Application Framework
The ZigBee Device Object (ZDO) module
Service Access Point (SAP)
Management routing tables
Management message transfer
Management address
Address mapping
Fragmentation and reassembly of packages
Multiplexing mechanism
Receive application profiles
get an address on
The ZigBee node
Offers APIs for developers
Management equipment
Reduce Function Device
Full Function Device
ZigBee Coordinator
ZigBee Router
ZigBee End-Device

Figure 2. Operating model of application layer

4.2. Operating model Bluetooth

Bluetooth is structured in two layers are the lower layer materiel and Upper layer software. The Lower layer material consists of three sub-layers are Radio (RF), Baseband link and Link Manager Protocol. The Upper layer software consists of four sup-layers are Logical Link Control, Service Discovery Protocol (SDP), Radio Frontend Component (RFC), application.

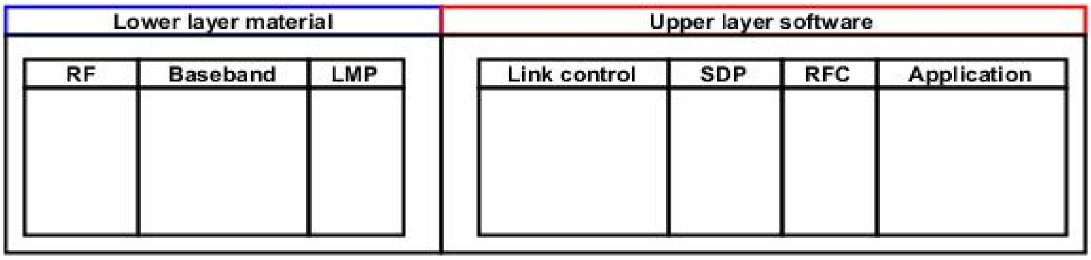

Figure 3. General operating model of Bluetooth

a) The Lower layer material

Radio (RF) sub-layer provides modulation and demodulation of data into RF signals. Therefore, this layer defines the physical characteristics of the Bluetooth transmitter and receiver. In addition, for physical link there are two types are connectionless and connection oriented. Baseband link layer establishes the connection within a piconet. It ensures formatting data for transmission to and from the radio layer. Moreover, Baseband defines the timing, framing and flow control. Link Manager Protocol sub-layer provides several functionality be in the figure, namely: link management, authentication processes and encryption, etc.

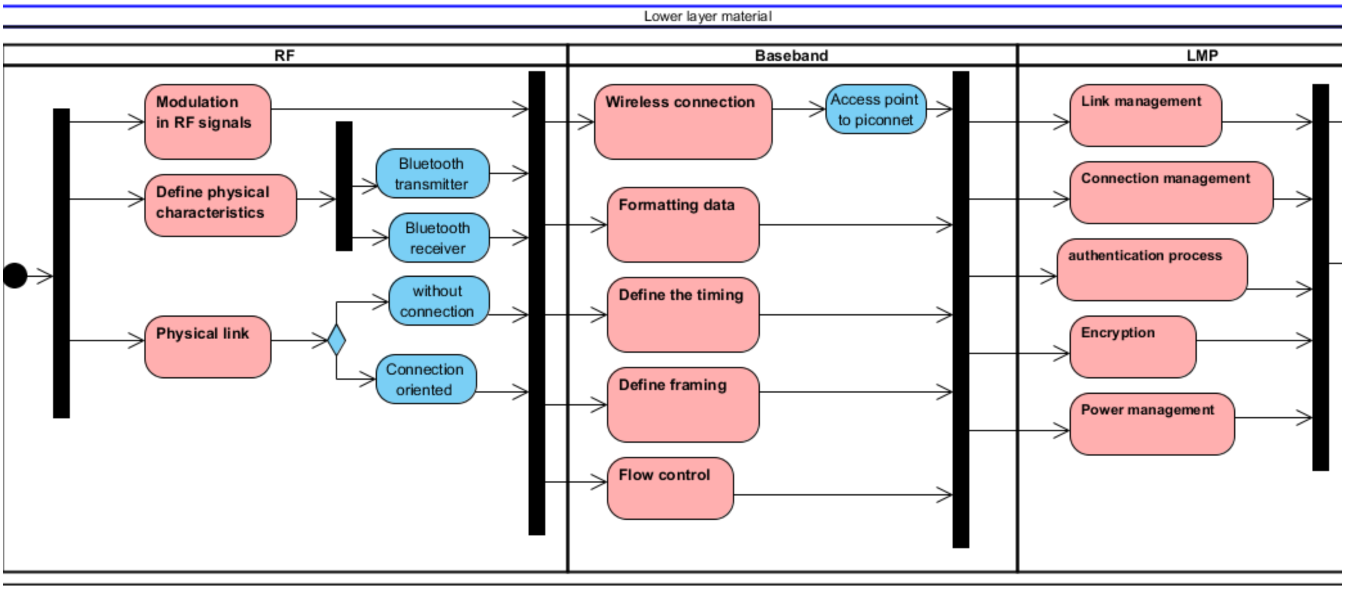

Figure 4. Operating model material layer

b) The Upper layer software

Logical Link Control sub- layer is the most important layer. This sub-layer allows communication between the upper and lower layers through the host controller interface (HCI). In addition, she ensures the management of packages. Service Discovery Protocol (SDP) allows you to discover the available and compatible devices. Adding that SDP allows interoperability between Bluetooth devices. Radio Frontend Component (RFC) provides an interface with Wireless Access Protocol (WAP) and Object Exchange (OBEX). OBEX is a communication protocol. It allows the exchange of objects between two devices. WAP provides Internet access. Sub-layer application allows the user to interact.

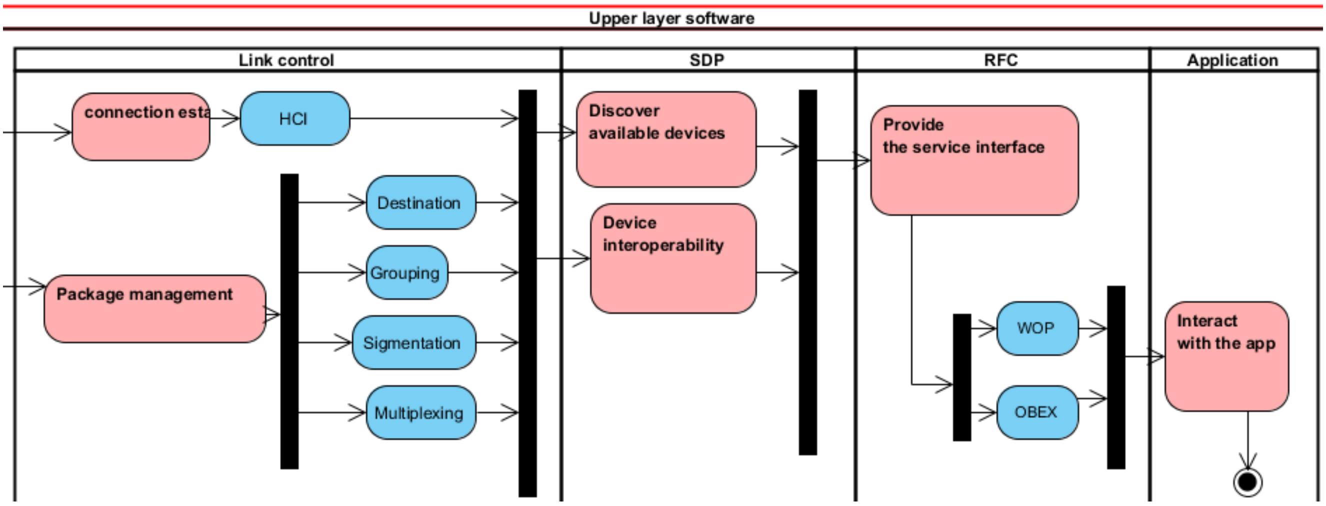

Figure 5. Operating Model Upper layer software

4.3. Operating model of NFC

NFC consists of two layers are Initiator and target. Therefore, NFC communication is between three sub-layers are alimentation, transmission, then a reception. There are three modes of communication reader mode (active mode), card emulation (passive mode), and peer-to-peer mode. This proposed model afterwards is for passive mode. In passive communication, there are two successful steps.

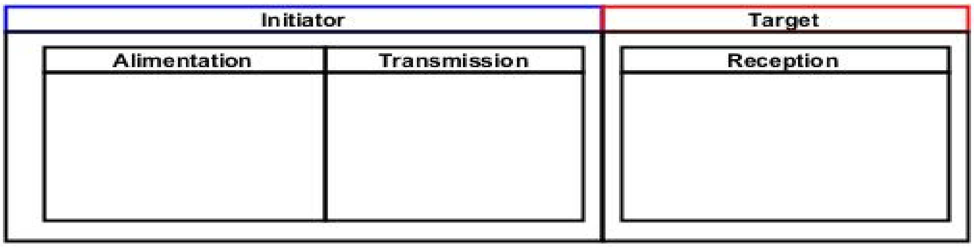

Figure 6. General Operating model of NFC

a) Initiator

Initiator carries the tag and energizes it through the magnetic field 13.56 MHz. The tag is populated. He can send messages regularly and wait for the one where a nearby tag will respond. The NFC reader continues to send the magnetic field just to power the tag.

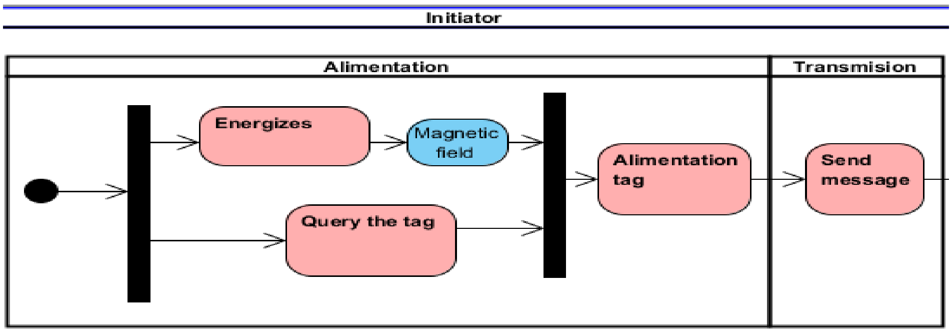

Figure 7. Operating model of Initiator layer

b) Target

The tag then has time to respond. During passive communication, the initiator generates an electromagnetic field from which the target will supplied with energy. To respond, the target will retro-modulate the electromagnetic field by modifying its impedance.

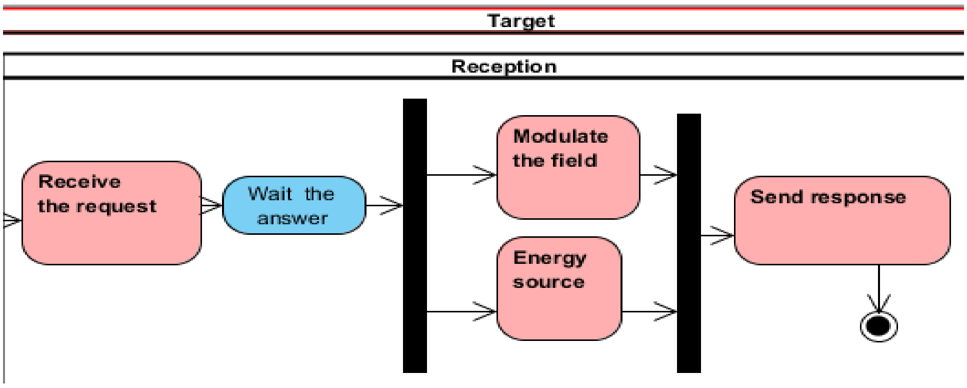

Figure 8. Operating model of Target

On the other hand, during active communication, the target and the initiator have their own energy source and communicate by alternating the electromagnetic field that they generate.

5. Projections of protocol criteria on operating models

In this section we project the protocols criteria of the on the proposed operating models. This projection proposed after a detailed study of the protocols criteria in the section of the comparative study and the analysis of the operating models. We classify the criteria into three categories, namely: Specification, Network criteria, Data management evaluation. We cannot project the specification criteria on the models. Either these criteria allow the user to choose the protocol according to the cost of purchases or according to the type of application in a light way, we neglect the other criteria. Thus, the specification criteria are not relate to the operation of the protocols.

5.1. Zigbee

In the figure above, we project the network and data criteria on the general functioning model of Zigbee. We find that the physical and mac layer manages the data criteria, while the network layer manages the network criteria. The application support sub-layer manages routing, risk of collusion and the type of security. This projection shows us that the priority to the data criteria since if the first layer does not work correctly the protocol same thing.

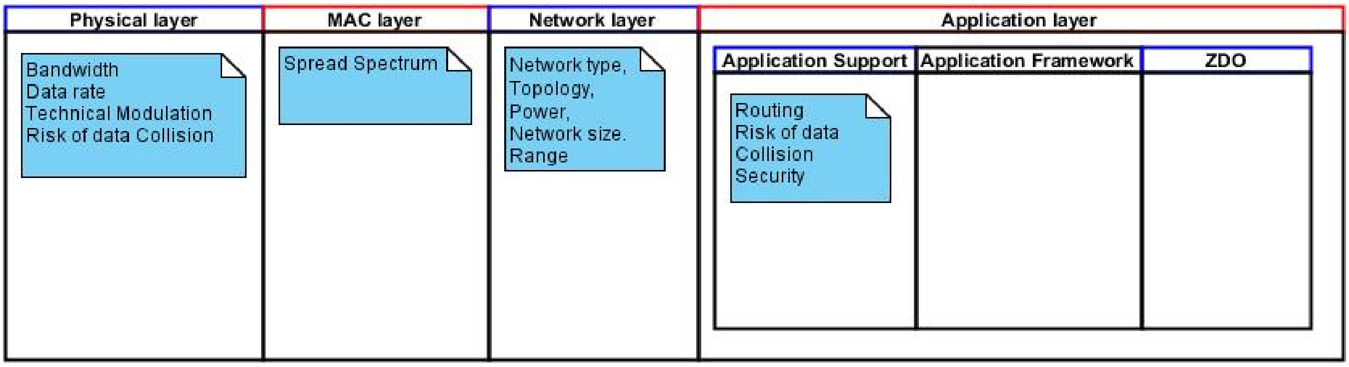

Figure 9. The projection of the criteria on the Zigbee operating models

5.2. Bluetooth

In the following figure, we project the network criteria and data on the general Bluetooth operating model. RF sub-layer and Baseband manage the data criteria. As long as the LMP sub-layer manages network and security criteria, the link data sub-layer manages the data. The projection shows that the priority given to the criteria.

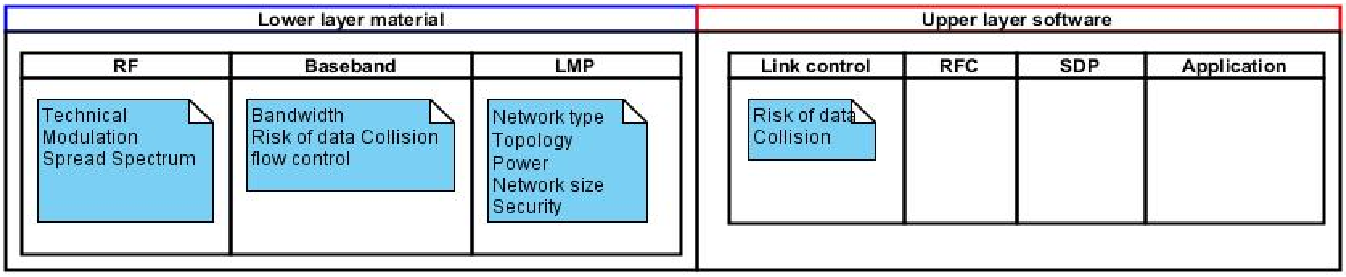

Figure 10. The projection of the criteria on the Bluetooth operating models

5.3. NFC

In the latter figure, we project the network criteria and data on the general NFC operating model. We find that the alimentation layer manages the technical modulation. The reception sub-layer manages the network criteria. This projection shows that the priority to the network criteria on the other hand the other protocols.

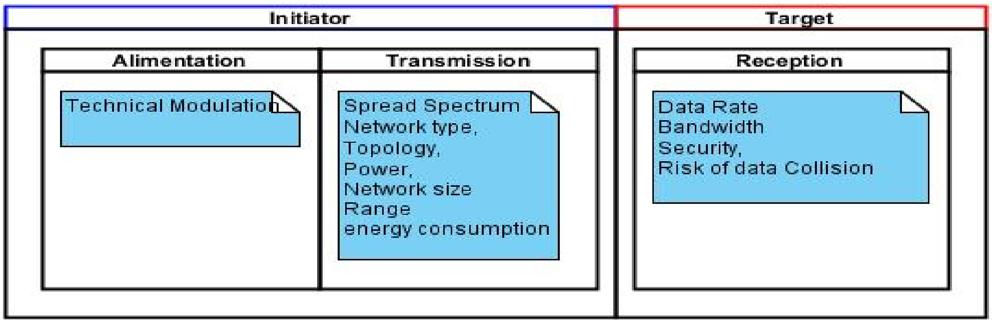

Figure 11. The projection of the criteria on the NFC operating model

6. Discussion and conclusion

Zigbee, Bluetooth and NFC wireless protocols are widely used for local communications in Internet of Things (IoT) applications. There are very different technologies used for the same job as near field data transfer. Each protocol has unique characteristics. The operating models define how the protocols work and how it should use to accomplish specific tasks. They are a set of layered programs. Each layer of a protocol speaks to the layer above it and to the layer below. At the distance level, Bluetooth allows data transmission up to 30 feet, while NFC can operate up to 20 cm away. Zigbee can operate over long distances through a mesh network of intermediate nodes. This makes it possible to reach distant nodes. At energy level, ZigBee is low consumption. It allows the interconnection of devices as well to pass requests in both directions. Power consumption for NFC is much lower than that of Bluetooth. When you make an NFC transfer, this consumes a certain amount of battery compared to Bluetooth transfer. NFC is actually faster than Bluetooth. At the data level, Zigbee has much greater range than any radio. The technology used in NFC is radio waves and in Bluetooth is RFID with a smart card infrastructure. ZigBee and Bluetooth operate in the same frequency range. The frequency range of Zigbee is 2.4 GHz from Zigbee. NFC needs that the devices must kept almost close to each other in order to complete the transfer. At the data level, Zigbee has much greater range than any radio. The technology used in NFC is radio waves and in Bluetooth is RFID with a smart card infrastructure. ZigBee and Bluetooth operate in the same frequency range. The frequency range of Zigbee is 2.4 GHz from Zigbee. NFC needs that the devices must kept almost close to each other in order to complete the transfer. At the connection level, the NFC connection may take a few seconds or sometimes it will not connect due to technical problems or faults. For data transfer speed, NFC is better than Bluetooth, NFC is 10 times faster than Bluetooth. At the security level, the security of using NFC and Bluetooth, the conclusive result would be that NFC is more secure than Bluetooth. Because NFC requires a range very close to that of Bluetooth. At the application level, Bluetooth and NFC is mainly use as a means of connecting consumer electronic devices. ZigBee used in equipment intended to automate and to operate largely without user intervention. These models will then allow us to give priority to the criteria of the protocols to make the choice of protocol adaptable to an IoT application.

The NFC model is the simplest also the interaction between swimlanes. It consists of two main layers and three sub-layers. The Bluethoot model is more complex at NFC so the interactions inside the swimlanes. It consists of two main layers and seven sub-layers. The Zigbee model consists of four main layers and three sub-layers.

According to the projections, that we have established there is one which gives priority to the network protocols other gives priority to the given protocols. These models and these projections allow us to have the knowledge to choose a network protocol for short-range applications.

As well, the operating models that we have realized allowing us to understand the requirements of each protocol in an in-depth manner. These models facilitate the implementation of choice of protocols according to the conditions of each type of application.

References

[1] S. Al-Sarawi, M. Anbar, K. Alieyan, et M. Alzubaidi, « Internet of Things (IoT) communication protocols: Review », in 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, mai 2017, p. 685‑690, doi: 10.1109/ICITECH.2017.8079928.

[2] P. Barker et M. Hammoudeh, « A Survey on Low Power Network Protocols for the Internet of Things and Wireless Sensor Networks », in Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, United Kingdom, juill. 2017, p. 1–8, doi: 10.1145/3102304.3102348.

[3] « Bluetooth 5: A Concrete Step Forward toward the IoT - IEEE Journals & Magazine ». https://ieeexplore.ieee.org/abstract/document/8419192/ (consulté le juin 16, 2020).

[4] « Building the Internet of Things with bluetooth smart - ScienceDirect ». https://www.sciencedirect.com/science/article/abs/pii/S1570870516302050 (consulté le juin 16, 2020).

[5] « JSAN | Free Full-Text | Security Vulnerabilities in Bluetooth Technology as Used in IoT ». https://www.mdpi.com/2224-2708/7/3/28 (consulté le juin 16, 2020).

[6] G. Memmi et U. Blanke, Mobile Computing, Applications, and Services: 5th International Conference, MobiCase 2013, Paris, France, November 7-8, 2013, Revised Selected Papers. Springer, 2014.

[7] « Internet of Things (IoT) communication protocols: Review - IEEE Conference Publication ». https://ieeexplore.ieee.org/abstract/document/8079928 (consulté le juin 20, 2020).

[8] P. Sethi et S. R. Sarangi, « Internet of Things: Architectures, Protocols, and Applications », Journal of Electrical and Computer Engineering, janv. 26, 2017. https://www.hindawi.com/journals/jece/2017/9324035/ (consulté le juin 20, 2020).

[9] S. Elhadi, A. Marzak, N. Sael, et S. Merzouk, « Comparative Study of IoT Protocols », SSRN Electron. J., 2018, doi: 10.2139/ssrn.3186315.

[10] S. ELhadi, A. Marzak, et N. Sael, « Operating models of application protocols », in Proceedings of the 4th International Conference on Smart City Applications, Casablanca, Morocco, oct. 2019, p. 1–7, doi: 10.1145/3368756.3369073.

[11] Elhadi S., Marzak A., Sael N. (2020) Functional Modeling of IoT Protocols. In: Ben Ahmed M., Boudhir A., Santos D., El Aroussi M., Karas İ. (eds) Innovations in Smart Cities Applications Edition 3. SCA 2019. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham. https://doi.org/10.1007/978-3-030-37629-1_45