Ατομική Διπλωματική Εργασία

ANALYSIS OF COMMUNICATION PROTOCOLS IN INTERENT OF THINGS

Κωνσταντίνος Λουκά

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ιανουάριος 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Analysis of Communication Protocols in Internet of Things

Κωνσταντίνος Λουκά

Επιβλέπων Καθηγητής
Ανδρέας Πιτσιλλίδης

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor, Dr. Andreas Pitsillides, for all the constant support and guidance throughout the course of my graduate studies and thesis at the University of Cyprus, Nicosia. His valuable suggestions and encouragement gave me the motivation to complete my thesis. I am grateful to my academic consultant Dr. Constantinos Pattichis, who guided me in every step of academic life for the past four years.

My deep sense of gratitude to my parents George Louca, Anastacia Louca, my brother Charis Louca, and my sister Maria Louca who are my moral strength and inspiration. I would like to thank all my friends for their constant guidance and encouragement throughout my years of study as well as been my extended family and being there for me whenever I wanted someone to count on. Special thanks to my best friend George A. for his constant guidance and encouragement throughout my years of study.

Finally, I would like to thank the University of Cyprus for offering me the opportunity to make my dream true, which was nothing more than finishing my undergraduate studies in the field of Informatics. In these last years of my studies, I managed to gain experiences and knowledge that will be useful to me throughout my entire life.

Constantinos Louca

University of Cyprus, Nicosia
January 2021

ABSTRACT

ANALYSIS OF COMMUNICATION PROTOCOLS IN INTERNET OF THINGS

Internet of Things (IoT) is a new paradigm that has changed the traditional way of living into a high-tech lifestyle. Smart city, smart homes, pollution control, energy saving, smart transportation, smart industries are such transformations due to IoT. There is no limit to the possibilities as the devices communicate and interact with each other. The devices must communicate with each other, the data from these devices must be collected by the servers, and the data is then analyzed or provided to the people. For all this to happen, there is a need for efficient protocols to ensure that the communication is secure and to avoid loss of data and information. With an ever-growing buzz about IoT and new connected products constantly introduced to the market, it can sometimes be difficult to get a clear overview and understanding of all the wireless connectivity technologies that enable these products. This thesis is about the implementation and analysis of various protocols that can be used for the communication in IoT. Various protocols with various capabilities are required for different environments. The internet today supports hundreds of protocols from which choosing the best would be a great challenge. But each protocol is different in its own way when we have the specifics like security, reliability, range of communication etc. When is it suitable to use Bluetooth vs Narrowband-IoT? What properties does Zigbee provide for a product? How is Thread different from Wi-Fi? This thesis introduces a range of communication protocols used to implementing smart devices currently available on the market and emphasizes on the best available protocols and the environments that suit them the most. It provides an implementation of some of the protocols and analyzes the protocols in depth according to the results obtained. In addition, predictive analysis for performing data analysis will be used to improve the scope of the thesis.

Table of Contents

Chapter 1

1. Introduction

As the need of connectivity increases Internet of things has been evolving nonstop over time. According to the requirements of different systems various architectures of IoT were designed as the main idea was the flow of data between devices and ease of communication across many nodes. At start, most of the devices and technologies were still evolving and limited to wired communications as communication was an obstacle.[1]. Large distance communications were less robust and costly to implement. Years after, wireless technologies like Bluetooth, Wi-Fi made the communication very fast and were easy to implement. As the complexity and size of the systems continued to increase, different aspects of security issues and management issues were noticed. The biggest challenge was that every product must be compatible with other products even in a different environment. Hardware was substantially produced by giant companies like Cisco, Intel, IBM etc. [2] and followed a standardized architecture.

Once the hardware was standardized in terms of standard connectivity, software applications began to follow these developments. The mobile market had widely changed, and an average cellular device could run an application and communicate to any server. This was revolutionary as it made huge impact at the way hardware could interact. Tons of money on hardware and maintenance costs were saved as many hardware functions were replaced by software functions (an application button replaced by a software touch/click).

The architecture was re-designed multiple times along with different considerations for every iteration. A single architecture would not be sufficient to cater the needs of everyone because IoT was evolving for industries of various sizes and domains. A much complex design was needed for large industries because data precision is more crucial, and timing and security are significantly important. On the other hand, for a small industry with hardly half a hundred connected nodes, reliability was more important than high-end security. This led to a wider classification of architecture for IoT [3].

Security stands as a serious issue for big companies since most of the IoT's communication happens over the medium. For example, think of a central server that is connected to a thousand home automation houses in each area with fifty plus nodes in each home to provide relevant data. If each of the home and its sensors are controlled by an application whose user would be the homeowner himself and the main control privileges would lie with the company providing the service, then any issue of security or data breaching [4] into the servers of this company can instantly affect the homes located in its controls.

Some examples of Internet of Things are a thermostat, an animal with biochip transponder, a person with heart monitor implant etc. Security plays a major role in the maintenance of an IoT system. For example, some self-driving cars use IoT systems. If someone could hack into the server even a small change or loss of data could be catastrophic and lead to an accident. IoT is making everything in our lives "smart" [5]. The number of IoT devices is growing around the globe in leaps and bounds. Researchers estimate that the number of IoT connected devices will exceed 21.5 billion by 2025.

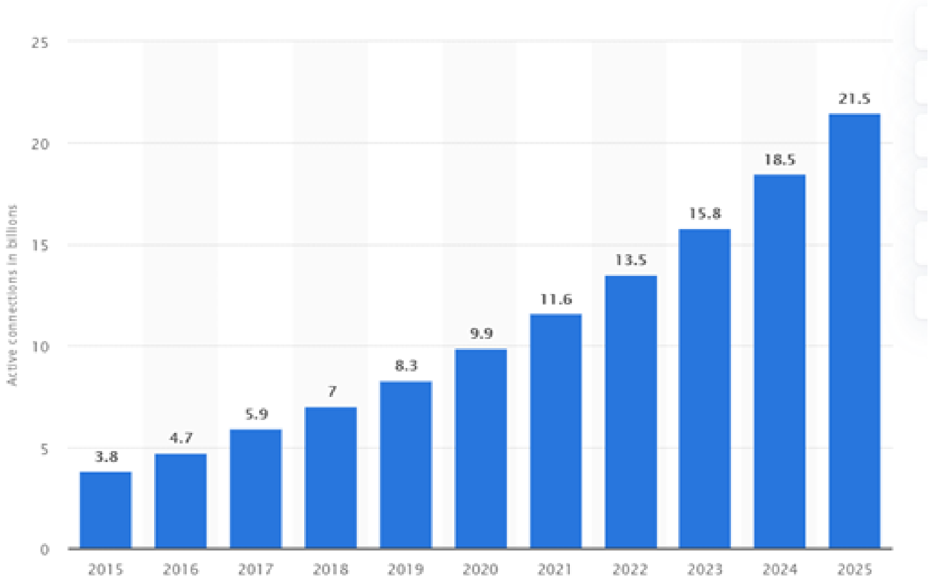


Figure 1.1: Statistics of the number of connected IoT devices

One of the areas in IoT where security can be improved is by choosing the right communication protocols. Communication protocols are important in telecommunications systems and other systems because they create consistency and universality for the sending and receiving of messages. Communications protocols can cover authentication, error detection and correction, and signaling. Communication protocols are a set of digital rules that are required to exchange data among computing devices. The devices on the network must agree upon various aspects of data exchange for successful transmission to happen. Today there are hundreds of protocols that are supported by the internet. Using the right protocol according to the environment and the devices being used has a significant importance. This could improve the security of IoT system by a consistent level.

1.1 Goals

This thesis analyzes various communication protocols in the IoT environment. As there are a huge number of manufacturers for IoT hardware with various levels of standards to meet certain common goals and standards, some protocols have been developed. This thesis extensively focused on protocols, their advantages, their disadvantages, their vulnerabilities, and the type of environments suitable for them. The aim of the thesis is to give a better understanding for anyone who willing to put an IoT device in their life on how to choose which communication protocol is best suited for him whether if it is faster or reliable or less expensive.

Multiple projects were combined to make this thesis more effective. It has been challenging to determine what kind of setup and environment does a given IoT system need. Everything from protocols, hardware selection and modes of communication need to be properly chosen to create an effective IoT system. This work would simplify setting up an IoT system in all aspects. Possible security issues also have been discussed in detail. The main motivation for this work was the interaction with simple systems everyday which had different IoT architectures in the background. This resulted in working more and getting a deeper understanding of how IoT systems are integrated and why not all IoT systems can be same in terms of protocols, communication modes and the hardware's used.

Chapter 2

2. Architecture of Internet of Things

Internet of Things (IoT) provide an interaction medium to transfer data over the network without any human involvement and focusing only on Machine-to-Machine (M2M) [6] communication which is mainly built on cloud computing and an internetwork of sensors that gather data.

Below is an architecture representation for any minimal IoT system. This illustrates different modules within an IoT system and the way they communicate in between. This architecture shows the components involved in an end-to-end IoT system, starting from an application to the final device to be controlled or receive data.

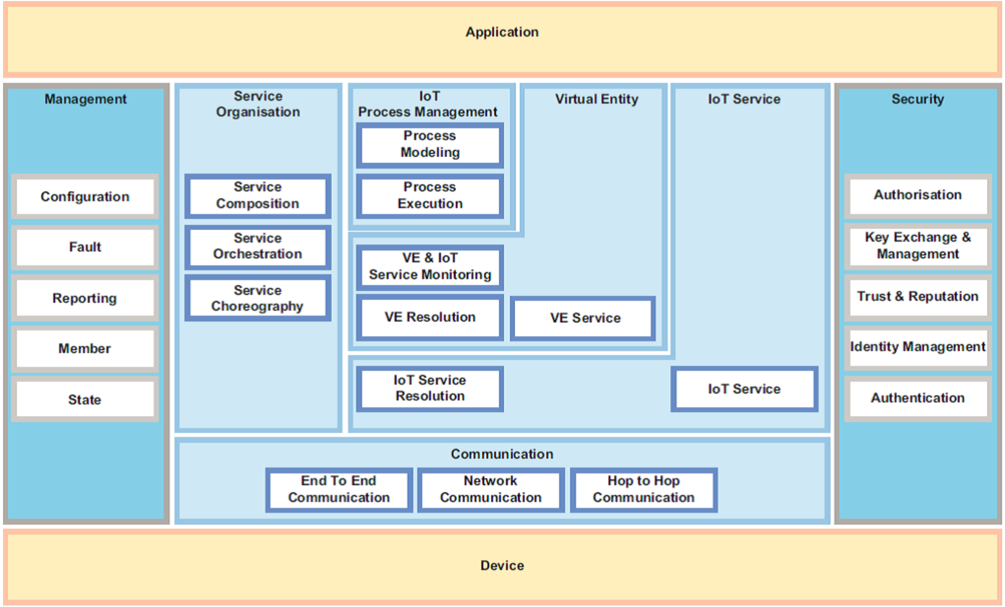


Figure 2.1: Architecture for a minimal IoT system

- Application

Application can be any software application that is used by the user which could be running on any device/platform or on any operating system. This is the first gateway through which the user would like to get or publish data to any service he is referring to. An application will have its own layer of security like user authentication via password or voice reader. Communication can be done via Wi-Fi/Bluetooth or Ethernet depending on the device they are installed and will send/receive from the end device. The application can send and verify data securely using various encryption [7] methods.

- Management

Management makes sure the transactions happen safe at different layers and it can also do error reporting or find malfunctions in a system [8]. His main purpose is to improve the user experience for that specific system.

- Security

The aim of the security is to make the whole application secure, reliable, and dependable. The complexity of this module is dependent on the size and requirement of the system. Security is required at the application layer, transport layer and at the hardware end as well. Any compromise at any layer will be a threat to data and the system itself [9].

- IoT Service

IoT Service is the core of the system operation and it is responsible for providing different services to users. These services can reduce the complexity of an IoT system in user perspective by a lot. Users can buy a compatible IoT module and subscribe to the service provided while using the system right away. This can lead to overall reduction cost for the user since he only needs to buy a part of the system.

- Communication

It coordinates how modules from different manufacturers will communicate and it got the most robust communication protocols to be set. Communication protocols again are widely divided into categories based on the pay load, range, and security.

- Devices

Devices are the end components that are controlled by the entire system. They get upgrades frequently and the system must be on alert to make sure the newly replaced device is compatible.

- Types of IoT Systems

There is no actual classification for different IoT systems, but some types of IoT systems can be:

1. Large Industries: Can use up to a few thousands of sensors to measure and collect data

2. Integrated systems for small areas: Can use up to a few hundreds of sensors

3. Personal systems : Home security, Health Check

4. Wide Area Services : Radio technologies

Chapter 3

3. Communication Protocols

Nowadays, more and more customized protocols are getting standardized for all the devices which work on IoT. The Wireless Sensor Networks are being implemented in large scale to monitor different parameters like temperature humidity etc. The nodes of the wireless sensor network follow the shortest path algorithm to transfer the data from the sensors to the control station. The temperature and the humidity of certain place are sensed and then these data are transmitted by the shortest path available. CoAP features a retransmission mechanism to ensure whether the message/packet is delivered or not. On the other hand, MQTT relies on TCP. When wired connectivity is lacked like in remote areas, we will have significant loss and delay as the only available Internet access is wireless or satellite. With this increase, devices must have low power consumption and a lot of bandwidth. Each device will act as a node collecting data from environment and transmitting over the net to master nodes. For data transfer across the sensor node, we need a light-weight protocol like MQTT to keep the bandwidth low but also to minimize power consumption and extend the sensor node life. In this thesis, we will be discussing the prominent transfer protocols used in the current Internet of Things scenario. The protocols used for such node-to-node communications in IoT are known as M2M (Machine to Machine). Figure 3 shows a simple architecture of M2M.

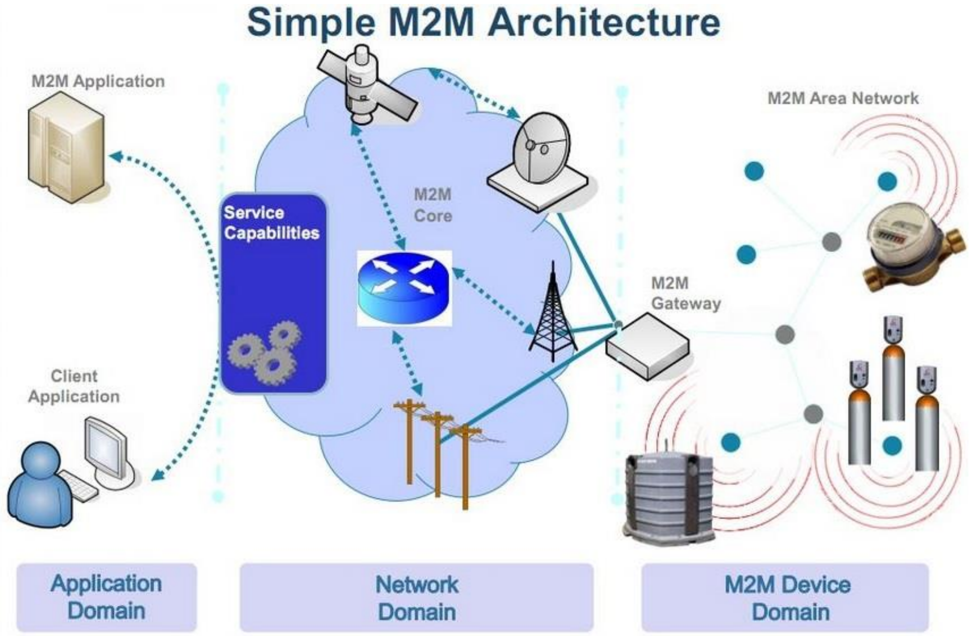
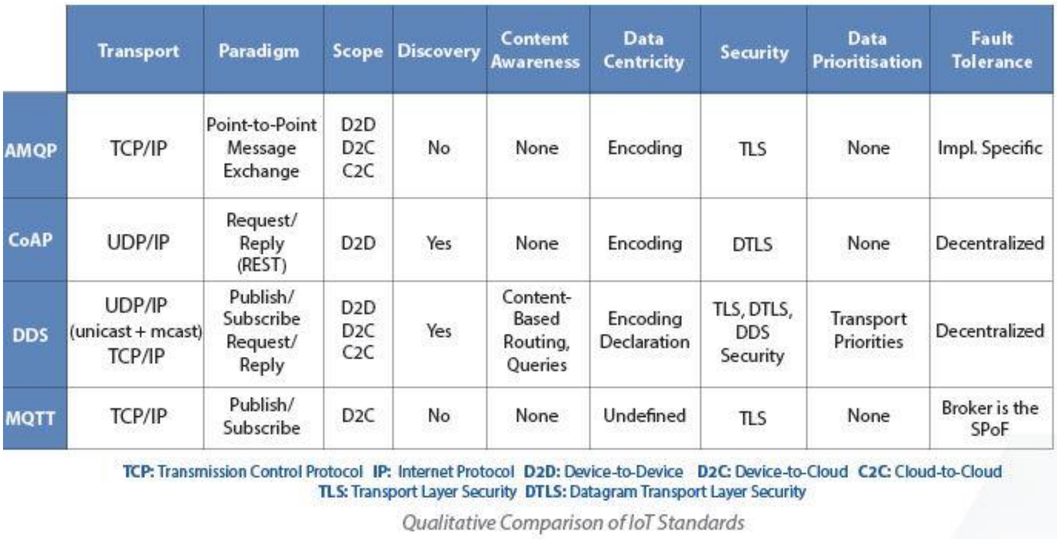


Figure 3.1: Simple M2M Architecture

M2M designates any system where machines communicate without human input, regardless of the device or communication medium while also providing connectivity for variety of devices like sensors, mobile devices, health monitoring systems, utility meters [10] etc. All everyday devices that are getting updated and addressed can be recognized and controlled via networks. The two most evident protocols that will be analyzed in this research are MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol). Both above-mentioned protocols are open standards and are better suited to constrained environments. These protocols have wide range of implementations for different requirements in the IoT field as they both run on IP and provide mechanisms for asynchronous communication. Other major protocols that will be analyzed are used in a smaller environment like Wi-Fi, Bluetooth, Z-Wave, Zigbee [11] etc.



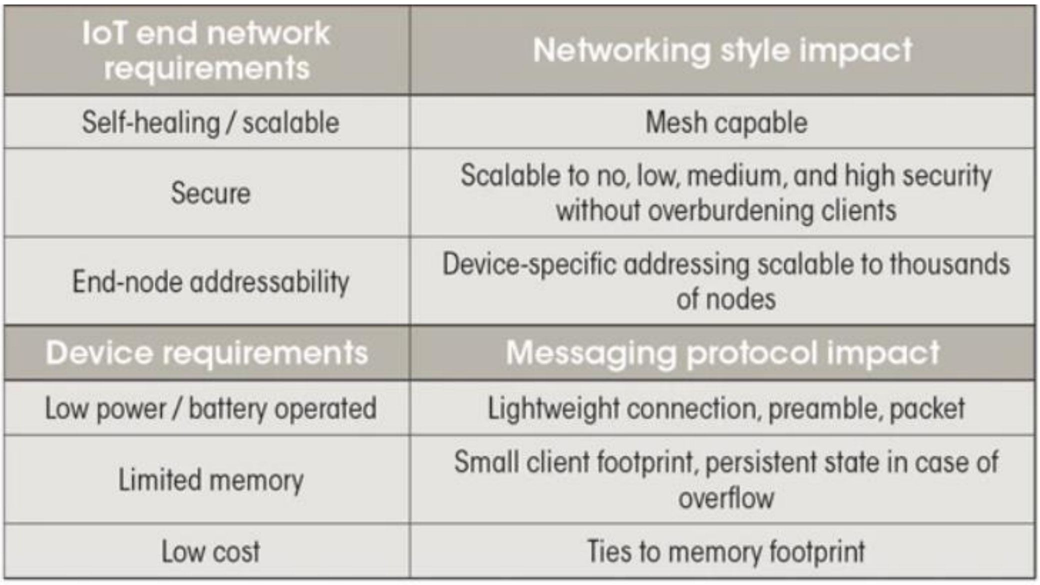
	Transport	Paradigm	Scope	Discovery	Content Awareness	Data Centricity	Security	Data Prioritisation	Fault Tolerance
AMQP	TCP/IP	Point-to-Point Message Exchange	D2D D2C C2C	No	None	Encoding	TLS	None	Impl. Specific
CoAP	UDP/IP	Request/ Reply (REST)	D2D	Yes	None	Encoding	DTLS	None	Decentralized
DDS	UDP/IP (unicast + mcast) TCP/IP	Publish/ Subscribe Request/ Reply	D2D D2C C2C	Yes	Content-Based Routing, Queries	Encoding Declaration	TLS, DTLS, DDS Security	Transport Priorities	Decentralized
MQTT	TCP/IP	Publish/ Subscribe	D2C	No	None	Undefined	TLS	None	Broker is the SPoF

TCP: Transmission Control Protocol **IP:** Internet Protocol **D2D:** Device-to-Device **D2C:** Device-to-Cloud **C2C:** Cloud-to-Cloud
TLS: Transport Layer Security **DTLS:** Datagram Transport Layer Security

Qualitative Comparison of IoT Standards

Table 3.1: More Protocol Comparisons

From table 2, we see some major differences between protocols. CoAP and DDS runs on the top of UDP (User Datagram Protocol) while MQTT and AMQP runs on TCP (Transfer Control Protocol). Although UDP is not reliable, protocols that use it provide their own mechanisms and functions to achieve the reliability mechanism. This is achieved using “Confirmable Messages” and “Non-Confirmable Messages”. In addition, we can see the scope of each protocol, data centricity and their security protocols.



IoT end network requirements	Networking style impact
Self-healing / scalable	Mesh capable
Secure	Scalable to no, low, medium, and high security without overburdening clients
End-node addressability	Device-specific addressing scalable to thousands of nodes
Device requirements	**Messaging protocol impact**
Low power / battery operated	Lightweight connection, preamble, packet
Limited memory	Small client footprint, persistent state in case of overflow
Low cost	Ties to memory footprint

Figure 3.2: IoT device requirements

3.1 Message Queuing Telemetry Transport (MQTT)

MQTT is a protocol designed to gather data from the devices and communicate it to the servers. It is a lightweight protocol using the publish/subscribe mechanism. The name suggests that this protocol is for remote monitoring. The MQTT protocol was initially created to link sensors on oil pipelines with communications satellites, with an emphasis on minimal battery loss and bandwidth consumption. MQTT works on Transmission Control Protocol (TCP) to ensure reliability and prevent data loss. It is a good choice for the networks experiencing various levels of latency due to poor bandwidth. When a client wants to send data to the broker, this is known as a "publish." When a client wants to receive data from the broker, it will "subscribe" to a topic or topics. When a client subscribes to a certain topic, it will receive all messages published on that topic going forward. Some benefits of MQTT are:

- Security

MQTT supports TLS/SSL for encrypting connections between devices and the broker. On the other hand, the broker can control the access of each device. In this model, each device can provide or consume data. In MQTT networks, "Topics" are essential to organize exchanging information. Topics organize messages in the same way directories organize files. The broker can block the access of unpermitted devices to restricted Topics. It means you can set permission for each topic to limit different devices' access. There is an extended version of MQTT known as SMQTT [12] where S stands for Secure. It uses encryption based lightweight protocol and it allows broadcast encryption, where one message is encrypted once, and multiple clients receive that message securely. This process consists of four phases namely setup, encryption, publish and decryption. In the first phase the subscribers and the publishers register themselves to the broker and get the master secret key.

- Ensure message delivery (QoS)

As MQTT origin is the Oil industry, it developed in a way that provides the highest reliability in worst network conditions. MQTT protocol provides more reliability by adding some flags. QoS (Quality of Service) will guaranty message delivery with 3 possible levels:

QoS 0: At most once delivery

QoS 1: At least once delivery

QoS 2: Exactly once delivery

The default QoS level is QoS 0. This level is suitable for Reliable network conditions if data loss is acceptable by the scenario. This would send the message and never acknowledge. It is just a one-time send without confirmation about the message reaching the destination. It is more suited to situations where the importance is low.

The other QoS level is QoS1. This would make sure the data reaches one-time minimum. It guarantees that the data reaches the destination at least once. It gives an acknowledgment about the message arrival at the intended destination. When the data being sent is received and confirmed by the other node, it will send a response/acknowledgment to the sending node. The sender waits for acknowledgment, and it saves the data to be sent and keeps resending it at regular intervals.

QoS2 delivers the highest messaging quality. This rule will make sure that the data is received and properly fetched by the intended node. When the sender has QoS level 2 messages it sends a message announcement. The proposed receiver gets prompt and then would decrypt it. It shows that it is ready to receive data. The publishing node sends the data, and when the receiver decrypts and gets the data, the whole process is done with an ack/talk back.

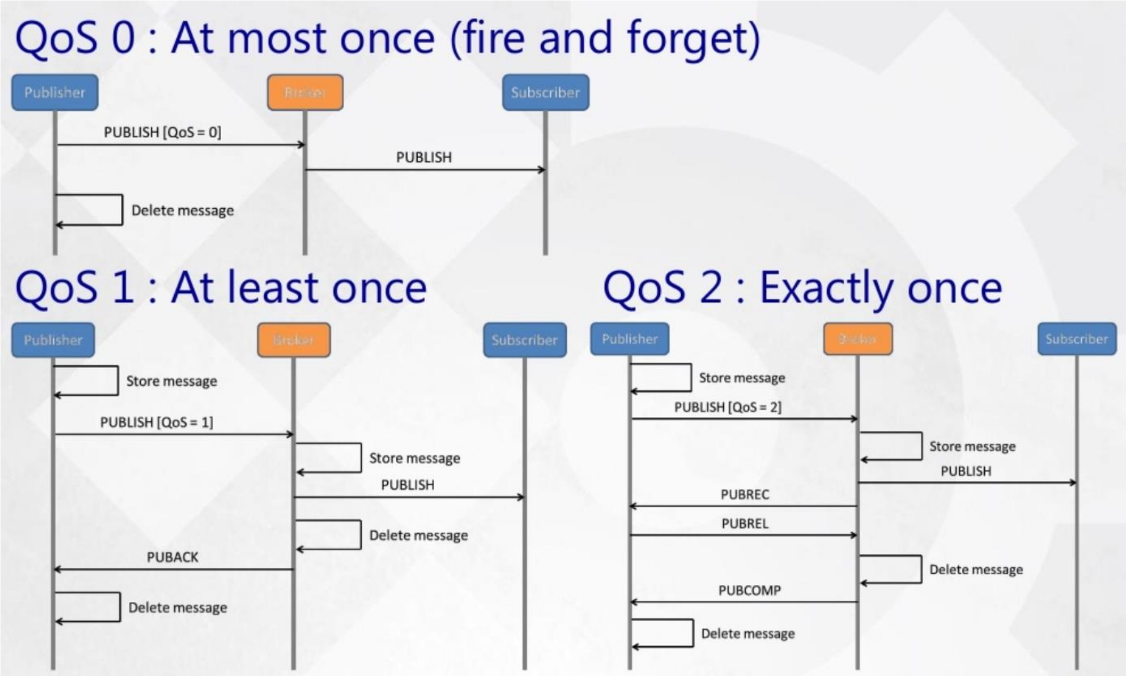


Figure 3.3: Levels of QoS

- Low battery Consumption

MQTT consumes 170 times less energy on 3G Networks and 47 times less energy on Wi-Fi networks compared to HTTP. MQTT empowers IoT developers to build devices that stay connected for +10 years using a battery.

- Lightweight protocol

IoT developers employ lightweight protocols for connecting things due to prevent overload on the network as each IoT device needs to send or receive data multiple times an hour on average. This made usability on small devices to have low memory and low processing power. As most IoT devices do not have powerful memory and processors, this protocol is well-suited for these devices.

- Time and Synchronization Decoupling

In the sensor network certain nodes may be active or in sleep mode at a given time. Sleep mode enables low power mode to be activated which reduces the power consumption during unwanted times. A node could now send information even if another node is sleeping.

The messages are always stored in a queue by the broker until they are consumed by a client or node. If a node is processing with some published information and another node publishes new information to which the current node has subscribed, then the message is queued until the current operation is completed. This will reduce repeated operations on the devices that were sleeping.

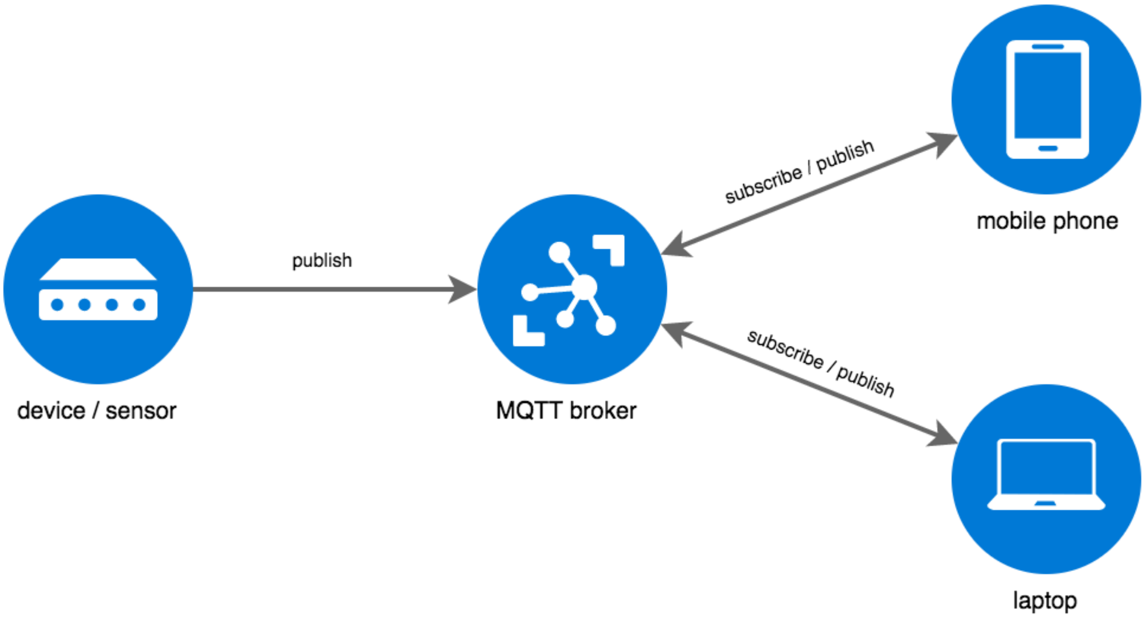


Figure 3.4: MQTT Architecture

Despite these architectural advantages, though, MQTT has three important drawbacks that raise questions about its suitability for many IoT systems and scenarios:

- Not a data protocol

Although it acts as a data transport layer it does not specify a particular format for the data payload. The data format is determined by each client that connects, which means there is no interoperability between applications. MQTT is explicitly not interoperable. It specifies that each client is free to use whatever data payload format it wants. To work on these environments, you must either translate data protocols for each new connected device and client, or you need to source all devices and programs.

- No intelligent routing

MQTT brokers are designed to be agnostic to message content. This design choice can cause problems for industrial applications communicating over the IoT. The broker cannot be intelligent about routing, based on message content. Clients cannot be told when data items become invalid and the broker is unaware of the data it is holding.

- Central Broker

For a distributed system, using central broker might be a bad idea because a single point of failure will affect the entire system.

- TCP

TCP was designed for devices that had more memory and processing power than many of the lightweight, power constrained IoT devices have available to them. TCP requires more handshaking to set up communication links before any messages can be exchanged. This increases wake-up and communication times, which affects the long-term battery consumption. TCP connected devices tend to keep sockets open for each other with a persistent session. This adds to power and memory requirements.

3.2 Constrained Application Protocol (CoAP)

CoAP is a web transfer protocol used for constrained nodes and networks and is a very efficient RESTful protocol specialized for M2M applications. Also, it can be an enhancement of HTTP for low power devices. Some features of CoAP include User Datagram Protocol (UDP) binding with reliability and multicast support, GET, POST, PUT, DELETE methods. Additionally, CoAP also supports publish-subscribe thanks to the usage of an extended GET method. Some benefits of CoAP are:

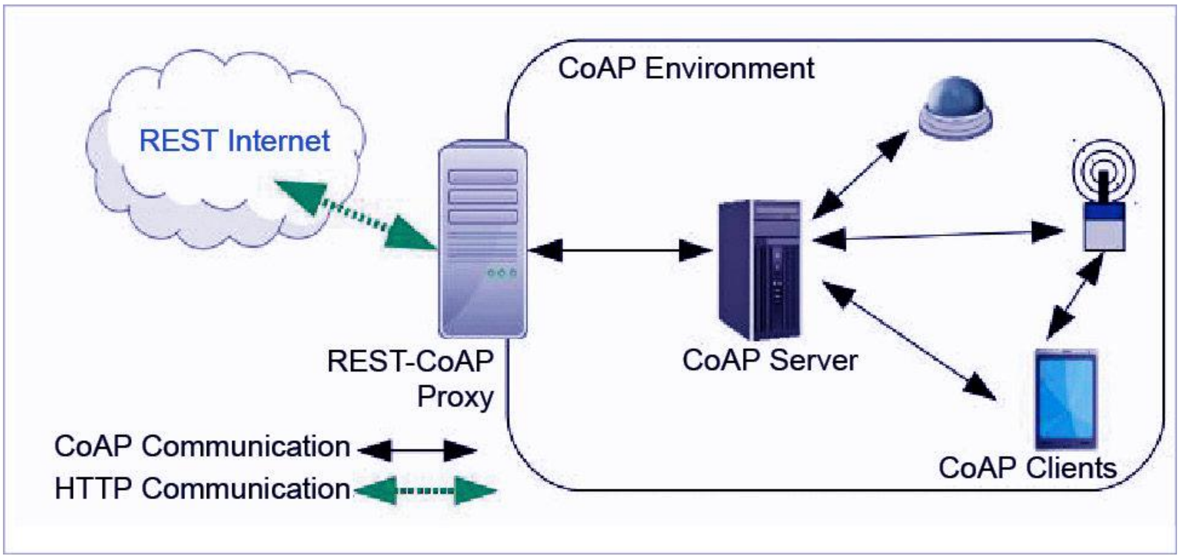


Figure 3.5: CoAP Environment

- User Datagram Protocol (UDP)

CoAP uses UDP as its background which is a bit less reliable. To compensate for the unreliability of UDP protocol, CoAP defines a retransmission mechanism and provides resource discovery mechanism with resource description. It also relies on redundant way of messaging rather than standard connections. On the other side, based on lightweight UDP protocol, CoAP allows IP multicast, which satisfies group communication for IoT. The packets here are connectionless which makes it unreliable, but they allow quicker wake from sleep and data send/ack cycles. They also use lesser payload for packets which reduces the overall payload as it helps nodes to save power and operate for a long time.

- Use of Multicast

CoAP can be used with multicast which would allow sensor nodes to send their updates to a multicast group as opposed to a single server. This can be used for a server to simply listen to a multicast group and auto-discover not require the clients to have prior knowledge of the server.

- Sends Multiple Nodes

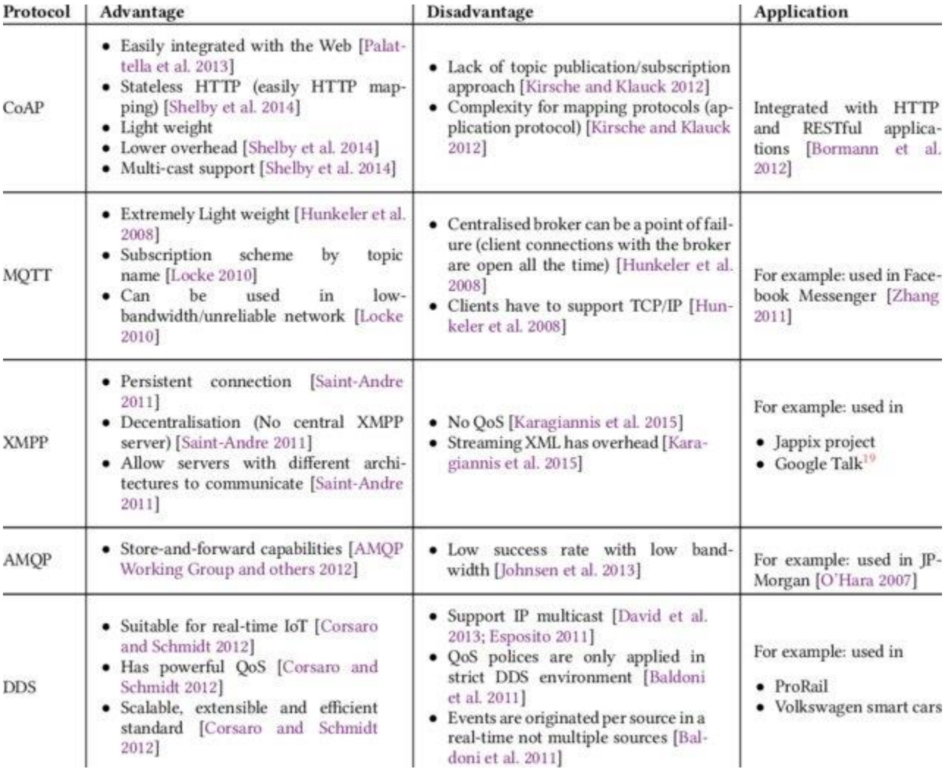
It also favors multi-node or single to multiple transfer requirements. This is possible because constrained application protocol is basically built with IPV6 support which by default allows multiple node transfers.

- Resource/Service Discovery

CoAP uses URI (Uniform Resource Identifier) to implement a standard communication interface to given nodes in any network and allow the packets to have additional flexibility.

- Async-Data Transfer

Many messages in the CoAP are transmitted using request and report standard model and CoAP also has a simplified “observe” mechanism. For example, the observing mode for node-1 can manage node-2 for a given data transfer cycle. Whenever a second node sends any relevant data, primary node will receive it after its sleep cycle.



Protocol	Advantage	Disadvantage	Application
CoAP	• Easily integrated with the Web [Palattella et al. 2013] • Stateless HTTP (easily HTTP mapping) [Shelby et al. 2014] • Light weight • Lower overhead [Shelby et al. 2014] • Multi-cast support [Shelby et al. 2014]	• Lack of topic publication/subscription approach [Kirsche and Klauck 2012] • Complexity for mapping protocols (application protocol) [Kirsche and Klauck 2012]	Integrated with HTTP and RESTful applications [Bormann et al. 2012]
MQTT	• Extremely Light weight [Hunkeler et al. 2008] • Subscription scheme by topic name [Locke 2010] • Can be used in low-bandwidth/unreliable network [Locke 2010]	• Centralised broker can be a point of failure (client connections with the broker are open all the time) [Hunkeler et al. 2008] • Clients have to support TCP/IP [Hunkeler et al. 2008]	For example: used in Facebook Messenger [Zhang 2011]
XMPP	• Persistent connection [Saint-Andre 2011] • Decentralisation (No central XMPP server) [Saint-Andre 2011] • Allow servers with different architectures to communicate [Saint-Andre 2011]	• No QoS [Karagiannis et al. 2015] • Streaming XML has overhead [Karagiannis et al. 2015]	For example: used in • Jappix project • Google Talk[19]
AMQP	• Store-and-forward capabilities [AMQP Working Group and others 2012]	• Low success rate with low bandwidth [Johnsen et al. 2013]	For example: used in JP-Morgan [O'Hara 2007]
DDS	• Suitable for real-time IoT [Corsaro and Schmidt 2012] • Has powerful QoS [Corsaro and Schmidt 2012] • Scalable, extensible and efficient standard [Corsaro and Schmidt 2012]	• Support IP multicast [David et al. 2013; Esposito 2011] • QoS polices are only applied in strict DDS environment [Baldoni et al. 2011] • Events are originated per source in a real-time not multiple sources [Baldoni et al. 2011]	For example: used in • ProRail • Volkswagen smart cars

Table 3.2:Advantages and Disadvantages of Different Protocols

There are certain disadvantages with CoAP which are as following:

- Message unreliability

UDP does not guarantee the delivery of datagrams. CoAP adds a method to request a confirmation acknowledgement to confirm the message was received. This does not verify that it was received in its entirety and decoded properly.

- Network Address Translation (NAT) issues

Devices behind Network Address Translation can have their IP change dynamically over time and CoAP can have problems communicating with that devices.

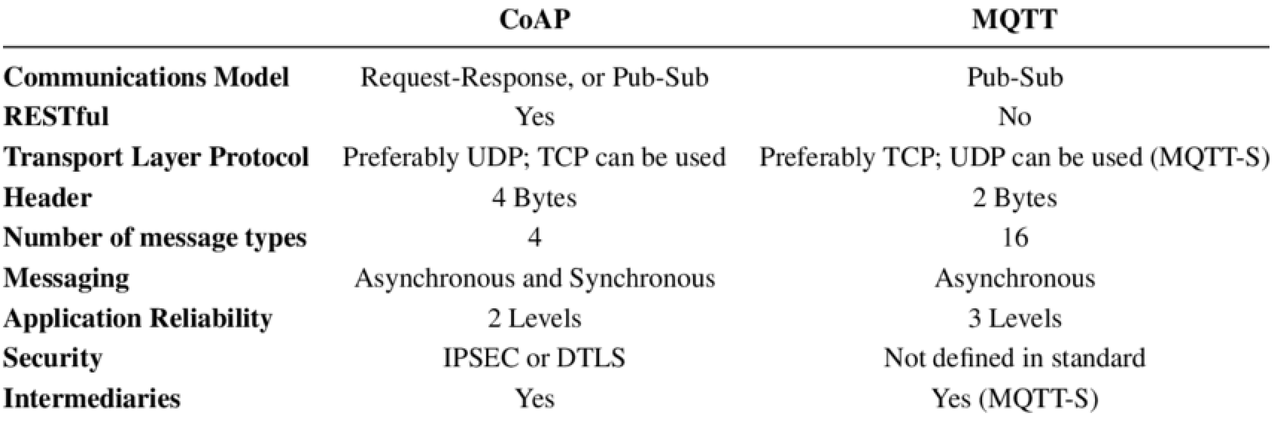
- Complexity

Mapping protocols is very complex.

3.2.1 MQTT vs CoAP

MQTT and CoAP are rapidly emerging as leading lightweight messaging protocols for the booming IoT market. Each protocol offers unique benefits, and each poses challenges and tradeoffs. Both protocols are being implemented for mesh-networking applications, in which lightweight end nodes are a necessary aspect of almost every network, and for gateway bridging logic to allow inter-standard communication.

MQTT is currently a more mature and stable standard than CoAP. For many IoT developers, it is easier to get an MQTT network up and running very quickly than a similar network using CoAP. That said, CoAP has tremendous market momentum and is rapidly evolving to provide a standardized foundation, with important add-ons now in the ratification pipeline.



	CoAP	MQTT
Communications Model	Request-Response, or Pub-Sub	Pub-Sub
RESTful	Yes	No
Transport Layer Protocol	Preferably UDP; TCP can be used	Preferably TCP; UDP can be used (MQTT-S)
Header	4 Bytes	2 Bytes
Number of message types	4	16
Messaging	Asynchronous and Synchronous	Asynchronous
Application Reliability	2 Levels	3 Levels
Security	IPSEC or DTLS	Not defined in standard
Intermediaries	Yes	Yes (MQTT-S)

Table 3.3:CoAP vs MQTT

3.3 Extensible Messaging and Presence Protocol (XMPP)

XMPP is an open set of rules for streaming XML elements to swap messages and presence information in close to real-time. The primary method of communication using XMPP is short messages. The XMPP protocol is based on the typical client server architecture, in which the XMPP client uses the XMPP server with the TCP socket. XMPP provides a general framework for messaging across a network, offering a multitude of applications beyond traditional instant messaging (IM) and the distribution of presence data. It enables the discovery of services residing locally or across a network, as well as finding out about the availability of these services. It enables the near-real-time exchange of structured yet extensible data between any two or more network entities. Any person over the network can create his/her own XMPP server also creating their own communication experience.

XMPP is well-matched for cloud computing where virtual machines, networks and firewalls would otherwise present obstacles to alternative service discovery and presence-based solutions. XMPP can be useful at many levels and may prove ideal as an extensible middleware or a message-oriented middleware (MOM) protocol. Some benefits of XMPP are:

- Very robust and powerful

With its open nature, anyone may run an XMPP server, given that they possess the hardware and knowledge to do so. If a single XMPP server is taken offline, only users of that specific server are affected, while those of other servers are unaffected.

- Extendable and adaptable

Creation of bots can enable a user to accomplish tasks such as posting to a blog, adding and removing reminders and calendar information, and even controlling media devices within their own house.

- Plethora of clients

There are XMPP clients for nearly every device, including at the command line level for both Windows and UNIX-based systems.

Some drawbacks of XMPP are:

- No official client or server

It is a decentralized system, and even when someone is using an XMPP service they often do not know it is XMPP due to the lack of branding or openness from the service provider.

- Overhead

Streaming XML has overhead due to text-based communication compare to binary based communication.

- QoS

It does not have QoS mechanism that gets used as MQTT protocol.

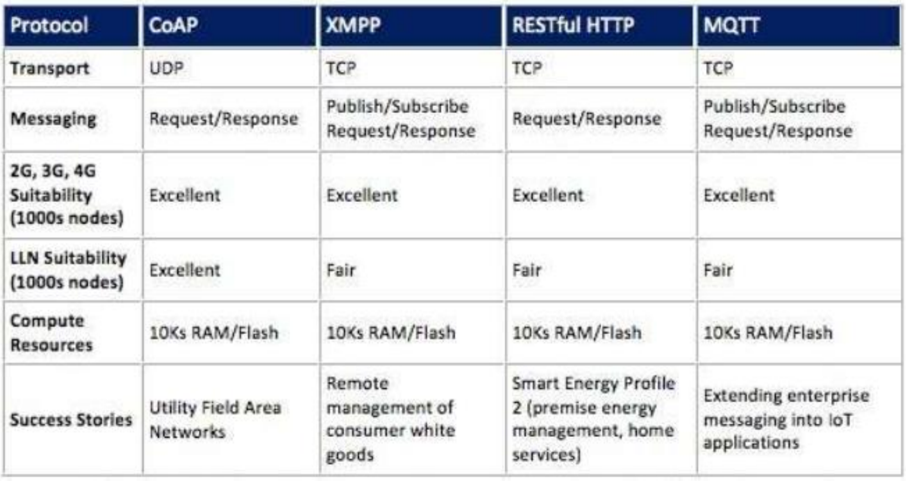
3.3.1 XMPP vs MQTT

- When implementing Machine to Machine on memory-constrained devices you choose MQTT as is a lightweight publisher/subscriber protocol.

- XMPP defines the message format and get structured data from devices unlike MQTT. This helps validate messages, making it easier to handle and understand data coming from these connected devices.
- With XMPP's federation function different manufacturers connected to different platforms can talk to each other with a standard communication protocol.
- MQTT has different levels of quality of service.
- MQTT has a scalability problem when the number of devices increases, while XMPP scales very easily.

3.4 RESTful Hypertext Transfer Protocol (HTTP)

The Representational State Transfer (REST) architectural style [REST] is a set of guidelines and best practices for building distributed hypermedia systems. At its core is a set of constraints, which when fulfilled enable desirable properties for distributed software systems such as scalability and modifiability. Since RESTful APIs are often simple and lightweight, they are a good fit for various IoT applications.



Protocol	CoAP	XMPP	RESTful HTTP	MQTT
Transport	UDP	TCP	TCP	TCP
Messaging	Request/Response	Publish/Subscribe Request/Response	Request/Response	Publish/Subscribe Request/Response
2G, 3G, 4G Suitability (1000s nodes)	Excellent	Excellent	Excellent	Excellent
LLN Suitability (1000s nodes)	Excellent	Fair	Fair	Fair
Compute Resources	10Ks RAM/Flash	10Ks RAM/Flash	10Ks RAM/Flash	10Ks RAM/Flash
Success Stories	Utility Field Area Networks	Remote management of consumer white goods	Smart Energy Profile 2 (premise energy management, home services)	Extending enterprise messaging into IoT applications

Table 3.4: Comparison of communication protocols for IoT devices

3.5 ZigBee

Zigbee is based on the IEEE's 802.15.4 personal-area network standard. Zigbee is a specification that has been around for more than a decade, and it is widely considered an alternative to Wi-Fi and Bluetooth for some applications including low-powered devices that do not require a lot of bandwidth - like your smart home sensors. It is designed for home automation, medical device data collection and small-scale projects which need wireless connection. Its low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics. ZigBee devices can have defined rate of 250 Kbit/s and can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. It was standardized in 2003 and was developed by ZigBee Alliance.

ZigBee is one of the most popular industry wireless mesh networking standard for connecting sensors, instrumentation, and control systems. ZigBee, a specification for communication in a wireless personal area network (WPAN), has been called the "Internet of things.“ ZigBee is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks. Low data rate wireless networking standards that can eliminate the costly and damage prone wiring in industrial control applications. The IEEE 802.15.4 standard provides a simple networking layer and standard application profiles that can be used to create interoperable multi-vendor consumer electronic solutions.

IEEE 802.15.4 contains Wireless MAC and PHY specifications for low-rate wireless personal area networks (LR-WPANs) such as ZigBee. Its main purpose is the communication between 2 devices.

The ZigBee Alliance company consists of 50+ companies like IP providers and Original equipment manufacturers and it defines upper layer of protocol stack: from network to application including application profiles. Its main purpose is to create a network topology and add features such as security, encryption, association and in the upper layer application services.

3.5.1 Architecture design of ZigBee

ZigBee specifies three different device types: the ZigBee Coordinator (ZC), the ZigBee Router (ZR), and the ZigBee End Device(ZED) . The coordinator represents a unique device that coordinates all information from the end-devices of the network. It is responsible of the communication with other devices. The router can manage information of the network, handling the routing of the packets. Typically, it is used when within a network there are some physical obstacles that do not allow the transmission of packets. And last ,the end-device is a terminal node responsible of gathering information directly from the sensors. Also, it is the less expensive hardware due to its role of collecting data periodically while saving battery energy as much as possible.

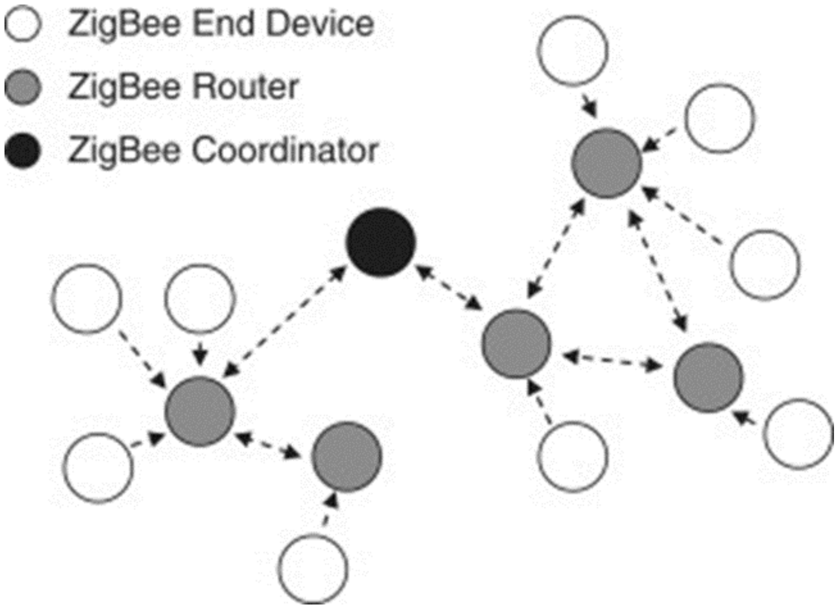


Figure 3.6: ZigBee device types

The network of ZigBee can be composed by multiple unities, with most of them being end-devices. If necessary, a router can be added to the network, but for every network the coordinator is just one. There are 4 topologies as you can see in the figure 9 below:

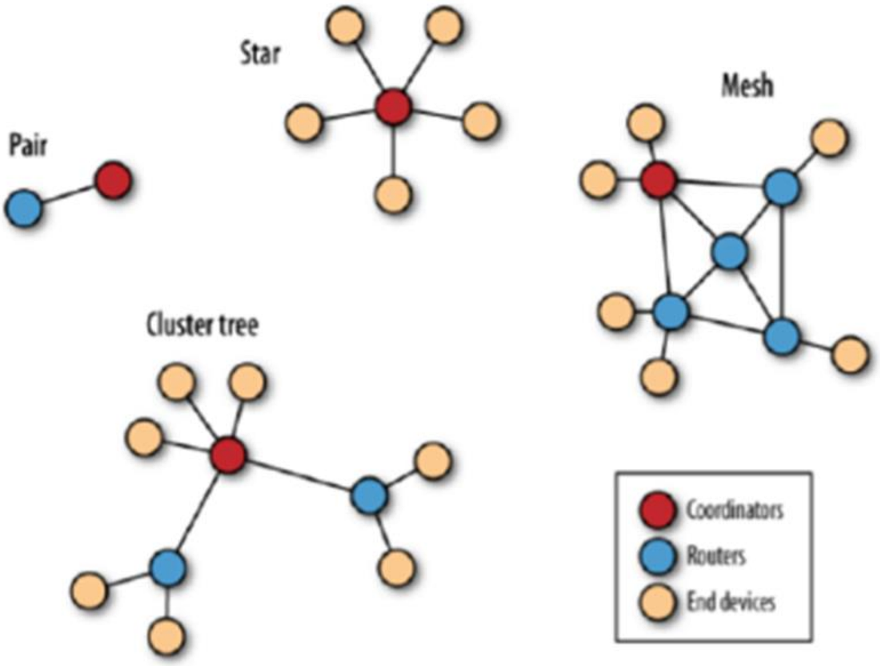


Figure 3.7: ZigBee topologies

1. Pair is the simplest topology. It is defined by two nodes: a coordinator and an end-device. The end-device sends the information acquired by the sensor directly to the coordinator.

2. Star is like the previous one, but includes multiple end-devices, with each one being linked with the coordinator.

3. Mesh is a more complex network. The nodes can pass messages along to other routers and end-devices as needed. The coordinator manages the network. Various end-devices may be

attached to any router or directly to the coordinator and each router can communicate with the coordinator or with other routers.

4. Cluster tree is a topology defined similarly to a mesh, but with the routers not being allowed to communicate with other routers.

Most used topology is the mesh topology because it creates a more reliable monitoring and communication network, especially in underground spaces and tunnels.

3.5.2 ZigBee in IoT

ZigBee is a mesh network protocol designed to carry small amounts of data across medium distances. It runs on a mesh topology network, meaning information from a single sensor node travels across a group (or "mesh") of modes until the transmission reaches the gateway. ZigBee is a local area network (LAN) that it is not intended to connect to devices directly around a user. Instead, it connects to devices that need a wider range. Because of this, it is an ideal protocol for home automation and smart lighting. Some examples are:

- Zigbee Home Automation is a global standard, which helps to create smart homes that can control appliances, security and energy management increasing customers' comfort and convenience. Also, it enables consumers to manage energy consumption, home security and to save money.

- ZigBee Health Care Automation offers a global standard for interoperable products enabling secure and reliable monitoring and management of non-critical, low-acuity healthcare services targeted at chronic disease, ageing independence and general health, wellness, and fitness.

- ZigBee Consumer Automation is designed for a broad range of consumer electronics products, such as TVs and set-top boxes. It promised many advantages over existing remote-control solutions, including richer communication and increased reliability, enhanced features, and flexibility.

- ZigBee Industrial Automation offers faster installation and maintenance, cost savings, and easier plant reconfiguration for different industrial appliances like environmental surveillance or military operations.

3.5.3 Pros and Cons of ZigBee

Some overall advantages are:

- flexible network structure
- very long battery life
- mesh network topology with low cost, multi hope data transmission and is power effective

- easy to install and reliable
- power saving and power consumption of communication

Some overall disadvantages are:

- short range
- Low complexity, and low data speed
- high maintenance cost
- Low transmission, as well as low network stability
- is not secure like Wi-Fi based secured system

3.5.4 ZigBee Security Services

ZigBee security deploys the AES(Advanced Encryption Standard) 128-bit encryption algorithm, where it includes security services as in key establishment, key transport, frame protection, and device management as well. Security in ZigBee is characterized in simplicity, directness, and end-to-end security. Each source and destination nodes are responsible for exchanging the key directly, each layer is responsible for securing a frame and data is transmitted without the need to decrypt and encrypt at each hop.

ZigBee is characterized in a few built-in security services and features; however, its applications are still vulnerable to network attacks as in sniffing the network key which is sent in plaintext for instance. In the figure we can see some of the ZigBee attacks categorized.

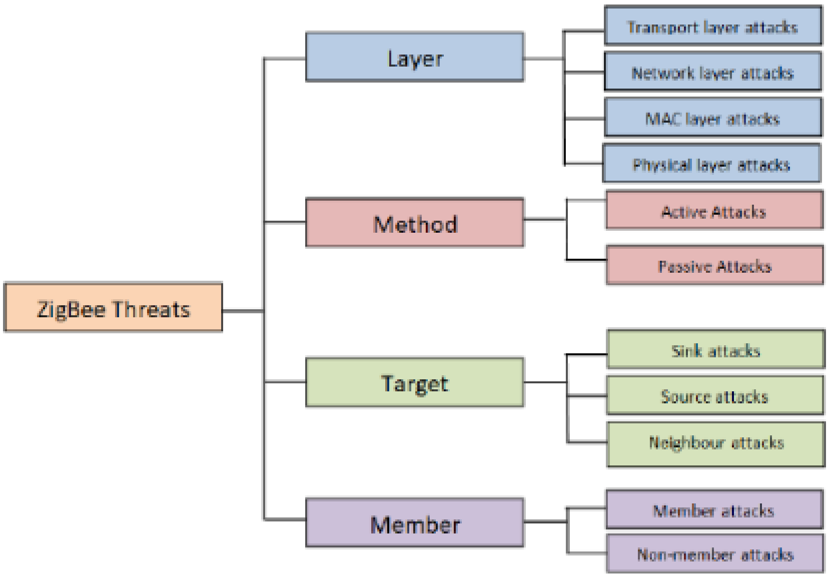


Figure 3.8: ZigBee Threats

<u>One Layer Attack</u> is the Transport layer attacks where attacks might include flooding and de-synchronization, where the targeted node is flooded by a numerous number of invalid connection establishment requests and forging packets to one or both ends of connection so that host requests to retransmit the missed packet frames.

One method attack is the Passive one where the attacker monitors the data traffic without affecting its integrity and sensitive information can be collected for some other malicious intent.

One target attack is the Sink attacks where the sink attack can take place when a malicious node announces a route to be the shortest path. Usually, this attack is combined with wormhole attack.

Also, there is the Ghost Attack where the attacker sends faked messages to lure node to intentionally to deplete that node's energy by redundant security-related computations.

3.5.5 Countermeasures for the attacks

1.Enhancement of the encryption algorithm by applying the XOR twice as well as updating the encryption key based on time synchronization. (this prevents penetration attacks)

2.Using new key distribution scheme to the algorithm and combining it with the hand-shake protocol used for new nodes while joining the network (this prevent Man-in-the-Middle attacks)

3.Deploying the Received Signal Strength (RSS) to prevent identity theft or data spoofing. (this prevents DoS attacks)

4.Using a new key management scheme based on the link, network, and cluster keys. The link key would be unique between any two ZigBee participant nodes. (this prevents attacks that target the ZigBee public application profiles)

3.5.6 Interference Problems

ZigBee devices support low power and low data rate transmissions and they designed to be cost effective to guarantee a successful commercial spread. To reduce the cost , they were designed to work in the crowded and overloaded 2.4 GHz ISM commercial band. The coexistence of different wireless technologies causes interference and packets collision, then packet retransmission. Which in turn, cause delay and reduce the delivery ratio. Moreover, ZigBee packet loss and retransmission leads to faster draining of the sensor battery.

- Interference Problem between ZigBee and Wi-Fi

Wi-Fi's three non-overlapping channels (1, 6, and 11) use the exact same frequencies as ZigBee channels 11-22. So, when deploying ZigBee and Wi-Fi networks in the same environment, channel planning for peaceful coexistence is key. Normally, we get three Wi-Fi channels to work with (utilizing 1, 6, and 11), but to make room for ZigBee, we may have given up channel 11.

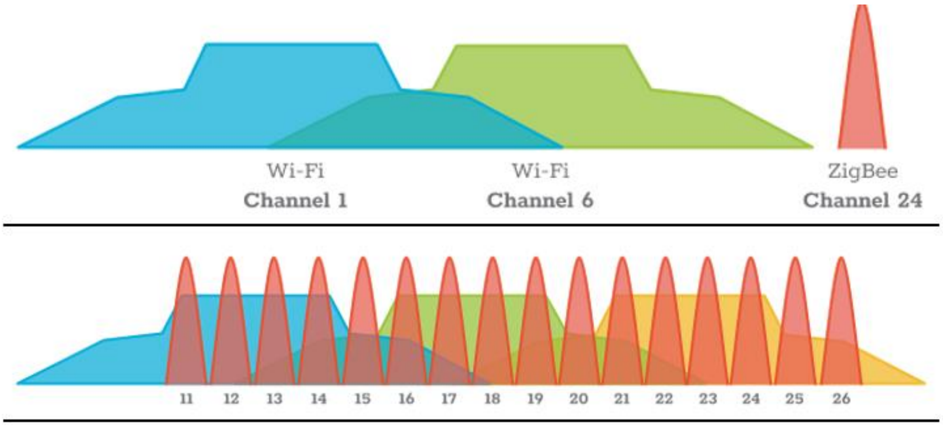


Figure 3.9: ZigBee and Wi-Fi channels

- Interference Problem between ZigBee and Bluetooth

For Bluetooth to cause any interference with a ZigBee signal, it must meet two criteria. Firstly, the Bluetooth signal must be sufficiently strong to completely swamp the ZigBee signal, because ZigBee can still function correctly in the presence of radio noise. Secondly, the Bluetooth signal must be transmitting on the same radio frequency and at the same time as the ZigBee signal. As the ZigBee radio frequency is fixed, and the Bluetooth hops from one channel to another in a pseudo-random sequence, a Bluetooth signal will be transmitted on the same frequency as a ZigBee signal. Bluetooth transmits 1600 times per second, and hops across 79 channels. On average, it will transmit on the same frequency as a ZigBee signal 20 times per second. As Bluetooth hops from one channel to another in a pseudo-random manner, it could transmit on the same frequency as a ZigBee signal more often or less often than this during one second. If interference does occur, the ZigBee standard includes an automatic retry facility.

3.5.7 Thoughts on ZigBee

Zigbee is a powerful, energy-efficient, and affordable smart home technology. It is widely used for lighting by big brands. Next to lighting, it is found in sensors, plugs, roller blinds and many more attractive products from a variety of brands. Also, with ZigBee you can build a good mesh network in your home which will relay signals and because the devices are cheaper, you can automate your home for less. But ZigBee is the not only solution to build a strong automated home or a good IoT application. There are more wireless smart home technologies out there. Whether you should go with Z-wave and ZigBee or Wi-Fi depends on what is more important to you when it comes to your smart home experience. If you want everything to work with Google or Alexa and do not want to add smart hub complications, then Wi-Fi devices are the best option. But if you want local, cloudless control—and a smart home you can fine-tune to the most advanced specifications—ZigBee and Z-Wave win. Zigbee and Z-Wave have been lumped together, but they are not the same thing. While they are generally similar in power, range, and low price, they are incompatible with each other, and there are some technical differences that attract product developers to one over the other. So, to choose which one you will use you will have to think which one is suited more.

3.6 Z-Wave

Z-Wave is a proprietary wireless communications protocol designed for home automation, specifically, to remote control applications in residential and light commercial environments. The technology uses a low-power RF radio embedded into home electronics devices and systems, such as lighting, home access control, entertainment systems and household appliances.

Z-Wave is a next-generation wireless ecosystem that lets all your home electronics talk to each other, and to you, via remote control. It uses simple, reliable, low-power radio waves that easily travel through walls, floors, and cabinets. Z-Wave control can be added to almost any electronic device in your house, offices, and hospitals even devices that you would not ordinarily think of as "intelligent," such as appliances, window shades, thermostats, and home lighting.

Figure 3.10: Z-Wave Plug-On module for Raspberry PI

3.6.1 Spectrum

Z-Wave is a low-power wireless technology designed specifically for remote control applications. The Z-Wave RF system operates in the sub–Giga hertz frequency range and is optimized for low-overhead commands such as on-off and raise-lower, with the ability to include device metadata in the communications.

It is largely unaffected by interference from common household wireless electronics that operate in this range because Z-Wave operates apart from the crowded 2.4 GHz frequency. Although, Z-Wave does share a range used by some cellphones and would be susceptible to interference from such devices. However, this freedom from normal household interference allows for a standardized low-bandwidth control medium that can be reliable alongside common wireless devices.

Z-Wave is easily embedded in consumer electronics products, including battery operated devices such as remote controls, smoke alarms and security sensors because of its low power consumption and low cost of manufacture.

3.6.2 Benefits of Z-Wave

Z-Wave delivers on all the promises of the wired home and welcomes exciting new possibilities as hundreds of Z Wave enabled products are already widely available. Some benefits of Z-Wave are:

- Simple

It is very easy to set up the wireless network by adding or removing devices without interfering with the router. Being able to easily add other devices into the Z-wave network helps build a home automation system. You do not need technical know-how to set up the device.

- Affordable

Z-Wave is accessible and easy for the do-it-yourselfer.

- Powerful

Z-Wave's intelligent mesh networking understands the present status of any enabled device and gives you confirmation that your devices have received the automatic or manual control commands you want.

- Versatile

Can monitor and control almost everything in your house.

- Interoperable

Z-wave allows users to mix and match devices together. This gives them total freedom to decide which devices to connect.

3.6.3 Drawbacks of Z-Wave

Some drawbacks of Z-Wave are:

- Resource requirements

Z-wave is battery intensive and consumes more power compared to other wireless technologies. This makes you replace the battery more often.

- Signal transmission

If the size of your home is bigger than 28 sq. meters, some devices will lose signal transmission information. Some of these devices will not be able to send or receive commands from the central controller, hub.

- Network security

Z-wave uses radio frequency transmission and hackers can tap into your network.

3.6.4 Z-Wave in IoT

- Convenience

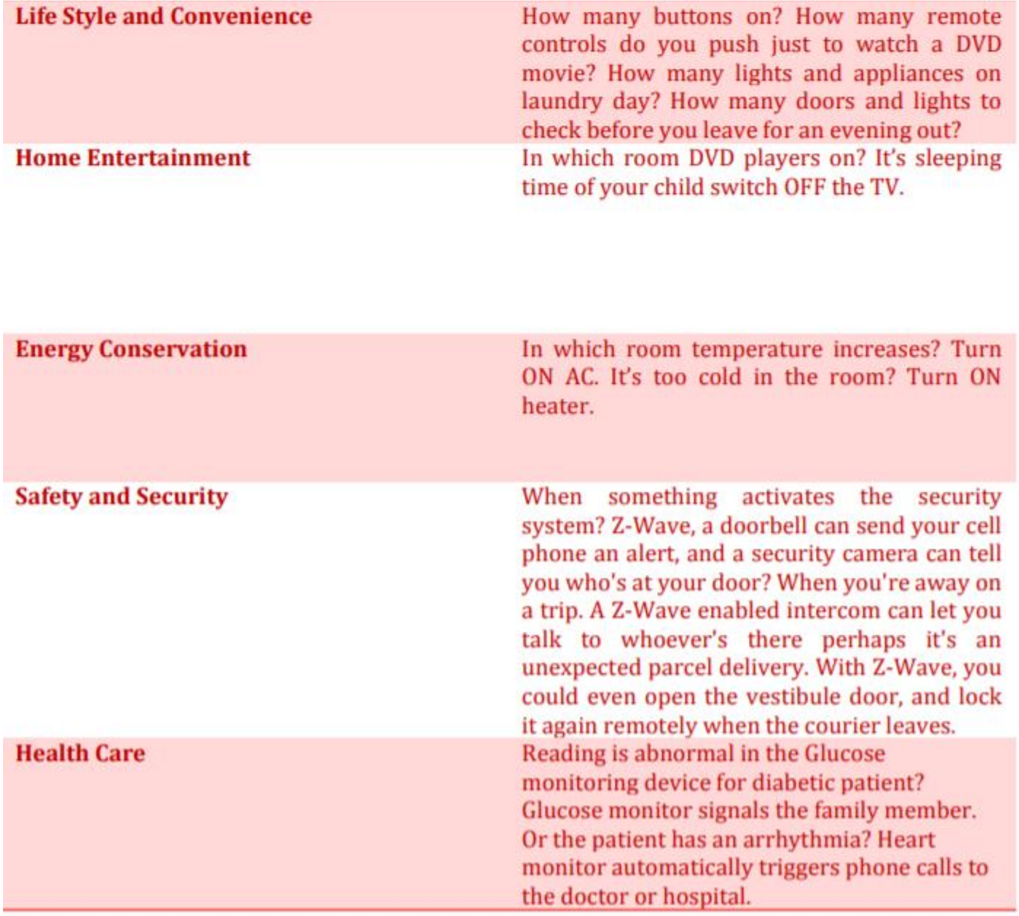
The ability to have your electronics work together as a team. With Z-Wave,
you can finally have the convenience of unified control over all your home electronics, and customize their operation to your preferences and your lifestyle. Z-Wave wireless control system gives you the power wirelessly to control all your devices with only one wireless device and with a single unified action.

- Automation

Z-Wave wireless control allows you to automate home's, office's, or facility's illumination so that you get the lighting you want when you are at home. For example, Z-Wave further economizes your energy usage by regulating your HVAC (heating, ventilation, and air conditioning) and Thermostat.

- Health Care

It is inexpensive and light enough to be built into virtually personal technology, such as blood pressure monitors and weight scales. At the same time, it is powerful and reliable enough for critical healthcare applications.



Life Style and Convenience	How many buttons on? How many remote controls do you push just to watch a DVD movie? How many lights and appliances on laundry day? How many doors and lights to check before you leave for an evening out?
Home Entertainment	In which room DVD players on? It's sleeping time of your child switch OFF the TV.
Energy Conservation	In which room temperature increases? Turn ON AC. It's too cold in the room? Turn ON heater.
Safety and Security	When something activates the security system? Z-Wave, a doorbell can send your cell phone an alert, and a security camera can tell you who's at your door? When you're away on a trip. A Z-Wave enabled intercom can let you talk to whoever's there perhaps it's an unexpected parcel delivery. With Z-Wave, you could even open the vestibule door, and lock it again remotely when the courier leaves.
Health Care	Reading is abnormal in the Glucose monitoring device for diabetic patient? Glucose monitor signals the family member. Or the patient has an arrhythmia? Heart monitor automatically triggers phone calls to the doctor or hospital.

Figure 3.11: Z-Wave Application Areas

3.6.5 Z-Wave vs ZigBee

ZigBee and Z-Wave target the same general applications. Of the two, ZigBee is by far the more versatile since it can be configured for virtually any short-range wireless task. Profiles are readily available to minimize development time for common applications. On the other hand, the protocol is far more complex, resulting in longer development times. Z-Wave uses a far simpler protocol, so development can be faster and simpler.

For a given power level of 0 dBm, Z-Wave's range is greater than ZigBee simply because the lower operating frequency supports it with pure physics. That also translates into a more reliable connection in some applications.

ZigBee uses the widely populated 2.4-GHz ISM band, which it must share with Wi-Fi, Bluetooth, and other radios that can produce interference. Most ZigBee devices have co-existence features that help mitigate interference, yet the potential is greater in the 2.4-GHz band than the 908.42-MHz channel of Z-Wave.

3.7 Bluetooth Low Energy

Bluetooth Low Energy was not an upgrade to the original Bluetooth, but rather it is a new technology that utilizes the Bluetooth brand but focuses on the Internet of Things (IoT) applications where small amounts of data are transferred at lower speeds. IoT applications rely on BLE for local, energy-efficient data exchange between smartphones and resource constrained peripherals. Common uses of BLE are iBeacon-based localization [13], smart wristbands/watches and environmental sensors and actuators [14].Most smartphones are readily equipped with BLE and this sets BLE apart from other low power wireless technologies such as ZigBee or Thread.

3.7.1 Architectural Design of BLE

Bluetooth Low energy as we see in the figure 14 below is categorized in different layers with each layer having their own function:

- Physical Layer

Transmitter uses GFSK modulation and operates at unlicensed 2.4 GHz frequency band. BLE offers data rates of 1-2 Mbps and it uses frequency hopping transceiver.

- Link Layer

Link layer is responsible for advertising, scanning, and creating/maintaining connections. The role of BLE devices changes in peer to peer (i.e., Unicast) or broadcast modes. The common roles are Advertiser/Scanner (Initiator), Slave/Master or Broadcaster/Observer.

- Host Controller Interface (HCI)

Communication between controller and host through standard interface types.

- Logical Link Control and Adaptation Protocol (L2CAP)

Offers data encapsulation services to upper layers.

- Security Manager Protocol (SMP)

Device pairing and key distributions to securely connect and exchange data between BLE devices.

- Generic Access Profile (GAP)

This layer directly interfaces with application layer and/or profiles on it to handle device discovery and connection related services as well as taking care of initiation of security features.

- Generic Attribute Profile (GATT)

Sub-procedure to handle data communications between two BLE devices

- Attribute Protocol (ATT)

Exposes certain pieces of data or attributes.

- Application Layer

The BLE protocol stack uses profiles that define the vertical interactions between the layers as well as the peer-to-peer interactions of specific layers between devices as well as handling device discovery and connection related services for the BLE device.

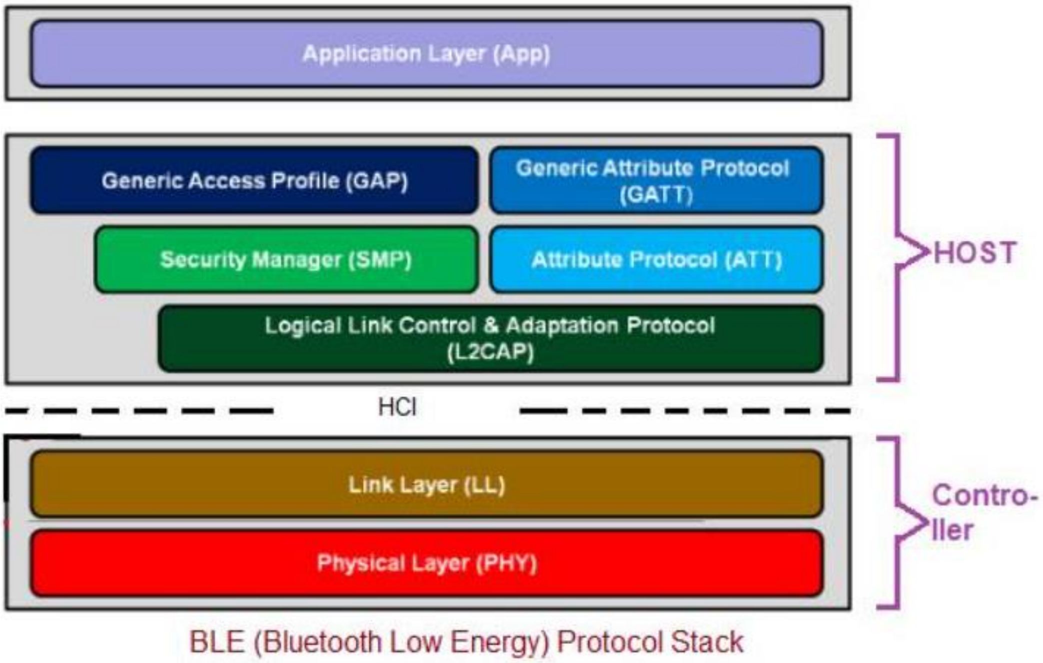

Application Layer (App)
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Security Manager (SMP)
Attribute Protocol (ATT)
Logical Link Control & Adaptation Protocol (L2CAP)
HOST
HCI
Link Layer (LL)
Physical Layer (PHY)
Contro-ller
BLE (Bluetooth Low Energy) Protocol Stack

Figure 3.12: Protocol Stack of BLE

3.7.2 BLE in IoT

- Healthcare

Due to its capabilities, low power, and cost, BLE is ideal for medical applications. Cellphones supporting this technology is making it possible for hospitals to better engage with their patients before, during and after each visit.

- Sports and Fitness

Implementation of Bluetooth Smart sensors in sports devices to instantaneously transmit data such as running cadence, stride length, total distance, or cycling speed, distance, and pedal cadence to Bluetooth Smart Ready devices like smart phones. Some examples are runners with polar heart-rate sensors that keep track of a target heart rate. Another example is cyclists with sensors on their bike wheels that measure speed and cadence.

- Peripherals

Wires are no longer needed to be connected. Everything can be united under a single wireless protocol.

- Automation

BLE solutions are most appropriate for home lighting, heating, and ventilation systems.

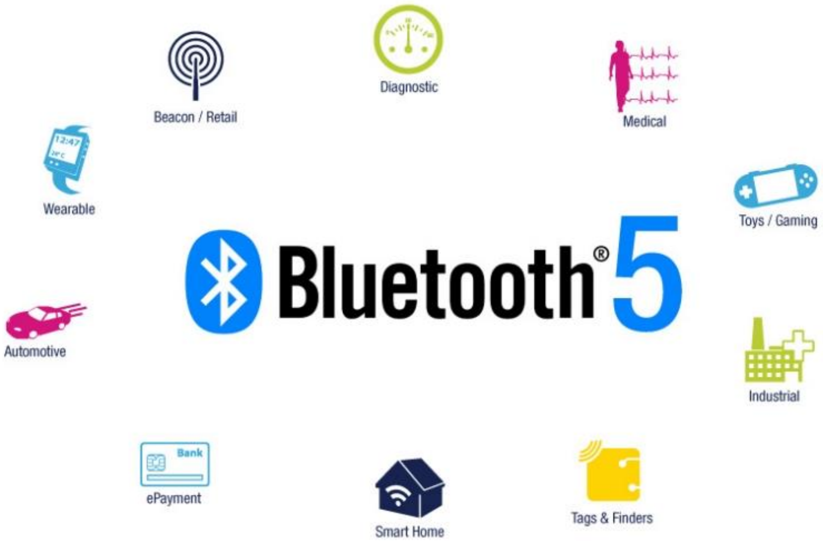


Figure 3.13: Bluetooth Low Energy in IoT

3.7.3 Benefits/Drawbacks of BLE

-Some benefits of BLE are:

- Lower power consumption

BLE achieves the optimized and low power consumption by keeping the radio off as much as possible and sending small amounts of data at low transfer speeds.

- Easy access to the specification documents.

You do not have to be a member of the official group or consortium for that technology to access the specification.

- Low cost of modules and chips

Cheapest in the market

- Worldwide existence

Almost all smartphones in the market have BLE.

-Some drawbacks of BLE are:

- Low data rates

Only supports 1 Mbps and 2 Mbps data rates unlike Wi-Fi and cellular technologies that offer higher data rates.

- Small distance wireless communication

It supports up to 200 meters in Line of Sight unlike cellular and Wi-Fi devices that support long distance wireless communications.

- Open to attacks

Due to wireless transmission/reception it is open to interception and attack.

3.8 Narrowband-IoT

Narrowband-Internet of Things (NB-IoT) is a standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services. NB-IoT significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage. The biggest feature of this network is the use of the existing LTE network (the GSM network). So, it does not need new special devices. Examples of NB-IoT can be several smart city applications, some smart home applications, smart meters, smart grid applications, smoke detectors, and industrial IoT applications with many low-power devices. Some advantages of NB-IoT are:

- Very low power consumption
- Excellent extended range under the floor and under the ground
- Easy installation of existing cellular network architecture
- Network security and reliability
- Low component cost

Some disadvantages of NB-IoT are:

- High Cost

Each device on the network must be paid. The addition of telecommunication taxes makes costs higher.

- Reliability

Modules do not have reliable maturity yet.

- Deployment

Deployment in deprecated GSM spectrum could be problematic.

3.9 LoRaWAN

LoRaWAN is the network communication protocol, based on LoRa technology layer, which allows to network with a set of Base Stations. LoRaWAN is a WAN communication technology with low power and it has been widely used within the Internet of Things in various fields.

A typical LoRaWAN network consists of end-devices (motes), gateways and a server which collects and analyzes information mined by the motes. LoRaWAN network topology is deployed in a star-of-stars topology in which gateways relay messages between end-devices and a central network server. The gateways are connected to the network server via standard IP connections and act as a transparent bridge, simply converting RF packets to IP packets and vice versa.

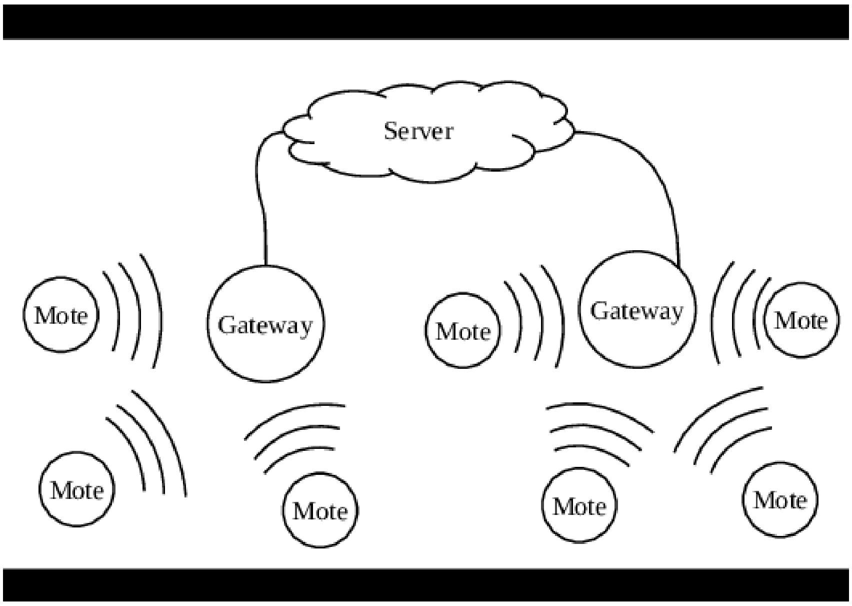


Figure 3.14: Topology of a LoRaWAN network

LoRaWAN motes are divided into three classes:

- Class A

Provides the lowest energy-consumption for the motes although it has long delays in downlink.

- Class B

Implements bidirectional communication with scheduled downlink receive slots.

- Class C

Devices listen to the channel continuously providing the lowest downlink latency, but in exchange requiring extremely high-power consumption.

LoRaWAN utilizes two layers of security: one for the network and one for the application. The network security ensures authenticity of the node in the network while the application layer of security ensures the network operator does not have access to the end user’s application data. A unique 128-bit Network Session Key shared between the end-device and network server and a unique 128-bit Application Session Key (AppSKey) shared end-to-end at the application level.

The LoRa communication module is commonly used for reading smart wireless meters. The distribution box's data collection system transmits each household's power consumption information to the LoRa module, and the LoRa module transmits the data over the gateway. Offer center remote control. The benefits of the LoRa module's low power consumption and low cost are more conducive to large-scale promotion and help grow smart cities. Some benefits of LoRaWAN are:

- Open frequency

Operates on unlicensed frequencies.

- Battery Life

Sensor batteries can last for 2–5 years (Class A and Class B).

- IoT deployments

Low bandwidth makes it ideal for practical IoT deployments with less data.

- Security

Two Layers of Security. A layer of security for the network and one for the application with AES encryption.

Some disadvantages of LoRaWAN are:

- Limited Payload

Payload is limited to 100 bytes

- Not for real time applications

Real time applications require lower latency and bounded jitter requirements.

- Open frequency

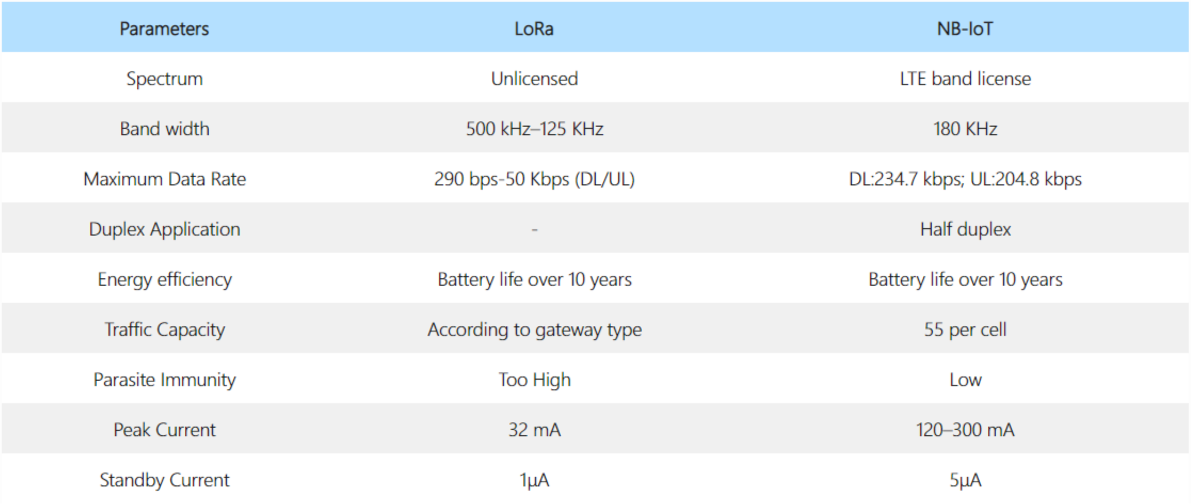
You may get interference on that frequency and the data rate may be low.

3.9.1 LoRaWAN vs NB-IoT

NB-IoT works on a cellular, licensed spectrum, the devices must be synced with the network at regular intervals. NB-IoT services are synchronized and they are provided over licensed frequency bands, the costs for frequency band licensing are significant. NB-IoT works best in sophisticated urban locations. In addition, NB-IoT is a cellular-grade wireless technology and it makes chips to be more complex.

On the other hand, no network synchronization is required in the ALOHA-based LoRa architecture. The LoRa IoT technology works on license free radio frequency spectrum and its applications have minimal costs while battery performance receives a boost. Since

LoRaWAN does not rely on cellular data or Wi-Fi for functioning, its coverage remains relatively steady across all types of locations.



Parameters	LoRa	NB-IoT
Spectrum	Unlicensed	LTE band license
Band width	500 kHz–125 KHz	180 KHz
Maximum Data Rate	290 bps-50 Kbps (DL/UL)	DL:234.7 kbps; UL:204.8 kbps
Duplex Application	-	Half duplex
Energy efficiency	Battery life over 10 years	Battery life over 10 years
Traffic Capacity	According to gateway type	55 per cell
Parasite Immunity	Too High	Low
Peak Current	32 mA	120–300 mA
Standby Current	1µA	5µA

Table 3.5: Comparison of LoRa and NB-IoT

3.10 Major Classification of Protocols

This unit is about a general classification of protocols to which the above protocols mentioned are a subset.

3.10.1 Ethernet

A system for connecting several computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems. It uses certain methods namely carrier sense multiple access and collision detection in which they are the core principles on how Ethernet works. Every system connected on Ethernet would check for traffic on the wire and if some other system is transmitting then this system would wait until its done and then put its data on the wire. Every Ethernet network interface card (NIC) is given a unique identifier called a MAC address. The MAC address comprises of a 48-bit number and within the number the first 24 bits identify the manufacturer, and it is known as the manufacturer ID or Organizational Unique Identifier (OUI) and this is assigned by the registration authority. It is considered as a network wired protocol [15].

Some advantages of Ethernet are:

- It does not require any switches or hubs
- Maintenance and administration are simple.
- The cable used to connect systems in ethernet is robust to noise.
- As it is robust to the noise, the quality of the data transfer does not degrade. The data transfer quality is good.
- With a Gigabit network, users can transfer data with the speed of 1-100Gbps.

- To form an Ethernet, we do not need much cost. It is relatively inexpensive. It is costless as compare to other systems of connecting computers.
- In Ethernet, all the nodes have the same privileges. It does not follow client-server architecture.

Some disadvantages of Ethernet are:

- As the network cannot set priority for the packets, it is not suitable for a client-server architecture.
- Not suitable for traffic-intensive applications. If the traffic on the Ethernet increases, the efficiency of the Ethernet goes down.
- It provides connectionless communication over the network.
- It offers a nondeterministic service.
- It does not hold good for real-time applications as it requires deterministic service.
- As the network cannot set priority for the packets, it is not suitable for a client-server architecture.
- Cannot be used for long distance network. Only with the use of Copper or Fiber.

3.10.2 Local Talk

Local Talk is a network protocol developed by Apple Computer, Inc. for Macintosh computer machines and it is quite similar in operation to Ethernet. LocalTalk adapters and special twisted pair cable can be used to connect multiple computers through the serial port. The difference it has from Ethernet is that any system before transmitting data over the wire would transmit a signal for intent to allow less collision of data between systems.

3.10.3 Token Ring

Token Ring protocol was developed by IBM and is a communication protocol used in Local Area Network (LAN). In a token ring protocol, the topology of the network is used to define the order in which stations send. In this protocol, all systems are connected in a logical ring, such that token moves from one system to other. If a system is idle and does not transmit any information, then the token moves around the ring. In another case the information/data to be transmitted will be attached to the token and will rotate around until reaches the required system [16].

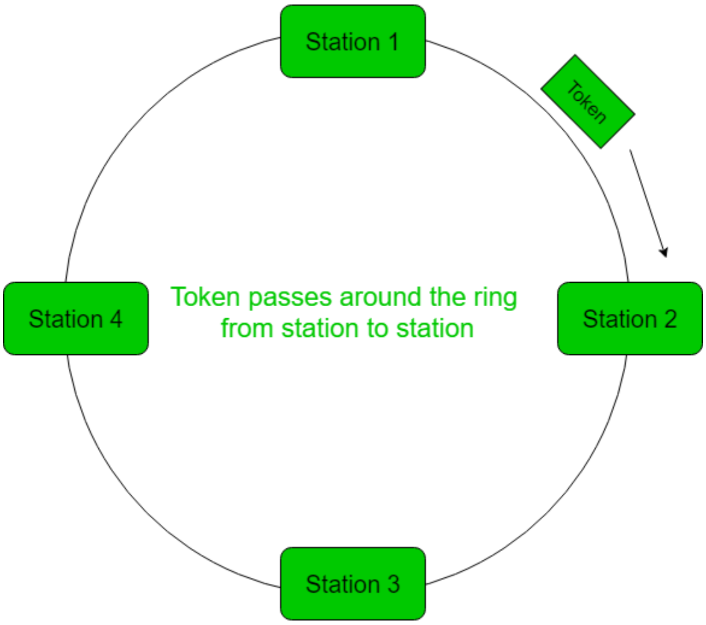


Figure 3.15: Token Ring

3.10.4 TCP/UDP

Transmission Control Protocol and User Datagram protocol are two types of Internet protocols. TCP is a connection-oriented protocol and UDP is a connectionless protocol where data is sent in small packets in chunks. TCP is significantly slower than UDP because of its weight. In TCP there is always absolute guarantee that data is transferred if not attempts are made to re-transfer or recover a lost data packet. It is not so in UDP, faulty or lost packets are dropped, and no attempts are made to re-transmit them. UDP is more used where fast and efficient transmission is required.

Some key differences between them are:

- Speed

UDP is faster than TCP because it has less to do. UDP does not guarantee delivery of transferred packets and just sends data without establishing a connection. On the other hand, TCP must establish a connection and handle error control.

- Reliability

TCP is known for being reliable. When you send data via TCP, it is guaranteed to arrive at your intended destination without errors. On the contrary, UDP is an unreliable protocol and does not guarantee data delivery because it does not track packets between the sender and receiver.

- Connection/Connection-less

TCP is a connection-oriented protocol whereas UDP is a connection-less protocol. When it comes to UDP it does not require an explicit connection to send data but in TCP, a connection is established between a sender and receiver before sending data.

- Flow and Congestion Control

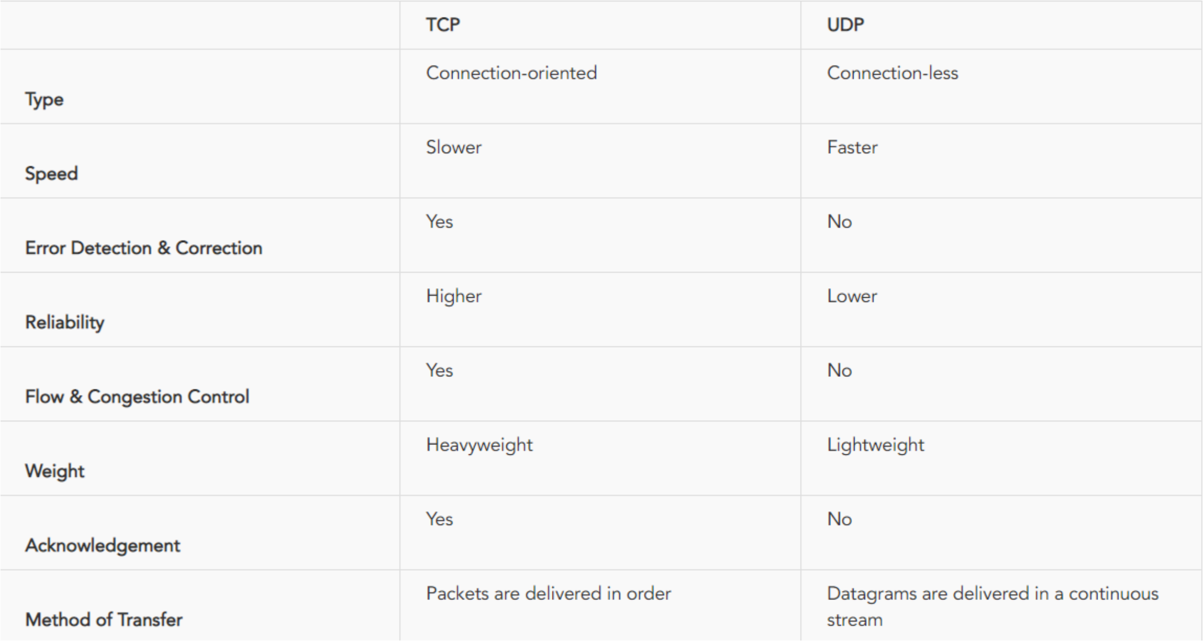
UDP does not offer flow and congestion control as packets are received in a continuous sequence or they are dropped. Although, TCP uses flow and congestion control ensures that a sender does not overwhelm a receiver by transmitting too much data too quickly.

UDP is well suited for applications where efficiency and speed are more critical than reliability like:

- VPN tunneling
- Voice over Internet Protocol (VoIP)
- Online games
- Media streaming

TCP is well suited for applications where reliability is a bigger concern than timing like:

- Email
- Secure Shell (SSH)
- Web browsing (HTTP and HTTPS)
- File Transfer Protocol (FTP)



	TCP	UDP
Type	Connection-oriented	Connection-less
Speed	Slower	Faster
Error Detection & Correction	Yes	No
Reliability	Higher	Lower
Flow & Congestion Control	Yes	No
Weight	Heavyweight	Lightweight
Acknowledgement	Yes	No
Method of Transfer	Packets are delivered in order	Datagrams are delivered in a continuous stream

Figure 3.16: TCP vs UDP Comparison Table

Chapter 4

4. Communication Models, Parameters, and their Limitations

How will the devices be connected and what would communication be like? How will wireless communication protocols evolve? Brief overview and illustration of each of the Internet of Things communication techniques, their pros and cons, and their smartphone compatibilities will be provided.

4.1 Communication Models

Major modes of communication for IoT or any internet connected system with multiple nodes allow manufacturers to select the mode of communication in a wide aspect considering the requirements and cost factors. Cost effective data nodes will help deploy the IoT network faster and keep the maintenance costs limited. An IoT system may consist of combinations where multiple technologies and protocols can synchronize. The wireless communication protocols are boiled down into the following 6 standards:

4.1.1 Satellite

Satellite communications enable cell phone communication from a phone to the next antenna of about 10 to 15 miles. They are called GSM, GPRS, CDMA, GPRS, 2G / GSM, 3G, 4G / LTE, EDGE based on connectivity speed. They play a very major role in the growth of IoT. Satellites are the only way to establish a connection between devices if the devices are geographically separated by a long distance. Satellite is useful for communication that utilize low data volumes, mainly industrial purposes.

Some pros of Satellite Communication are:

- Stable connection
- Universal compatibility

Some cons of Satellite Communication are:

- No direct communication from smartphone to device as it has to go through satellite.
- High monthly cost
- High power consumption

4.1.2 Wi-Fi

Wi-Fi is a wireless local area network (WLAN) that utilizes the IEEE 802.11 standard through 2.4GhZ UHF and 5GhZ ISM frequencies. Wi-Fi is one way of connecting the nodes in IoT. Wi-Fi provides Internet access to devices that are within the range. The purpose served by satellites cannot be served by Wi-Fi, but satellites are not always the solution as they are of high cost. Wi-Fi is useful for many Internet of Things connections, but such connections typically connect to an external cloud-server and are not directly connected to the smartphone.

Some pros of Wi-Fi are:

- Universal smartphone compatibility
- Affordable
- Well protected and controlled
- Rapid Connection setup times
- Wi-Fi access points can be directly connected to the internet without any change in the module.
- Security and Integrity
- Flexibility

Some cons of Wi-Fi are:

- Relatively High power usage
- Instability and inconsistency of Wi-Fi

4.1.3 Radio Frequency (RF)

Radio frequency communications are probably the easiest form of communications between devices. In some applications, Wi-Fi is too complicated to be used in the sensor technology. In such cases, Radio Frequency is used as an option to connect the nodes in the IoT Protocols like ZigBee or Z-Wave use a low-power RF radio embedded or retrofitted into electronic devices and systems. Radio frequency communication protocol is useful for large deployments.

Some benefits of RF are:

- Low energy and simplicity for its technology is not dependent on the new functionality of phones.
- Low cost and Low power consumption
- High transmission range

A drawback of RF is:

- RF Devices cannot be connected to the Internet without a central hub connect them.

4.1.4 Radio Frequency Identification [RFID]

Radio frequency identification (RFID) is the wireless use of electromagnetic fields to identify objects. An Active Reader Active Tag (ARAT) system uses active tags awoken with an interrogator signal from the active reader. This ID makes sure that the object is uniquely identified. With this technology the data can be monitored. The devices connected through RFID in IoT send data to a central server which stores the data in human-readable format. Examples include animal identification, factory data collection, road tolls, and building access.

Some benefits of RFID are:

- Established and widely used technology.
- No power required.

Some drawbacks of RFID are:

- Smartphones incompatibility
- Tags need to be present as identifier and be handed over before
- Highly insecure

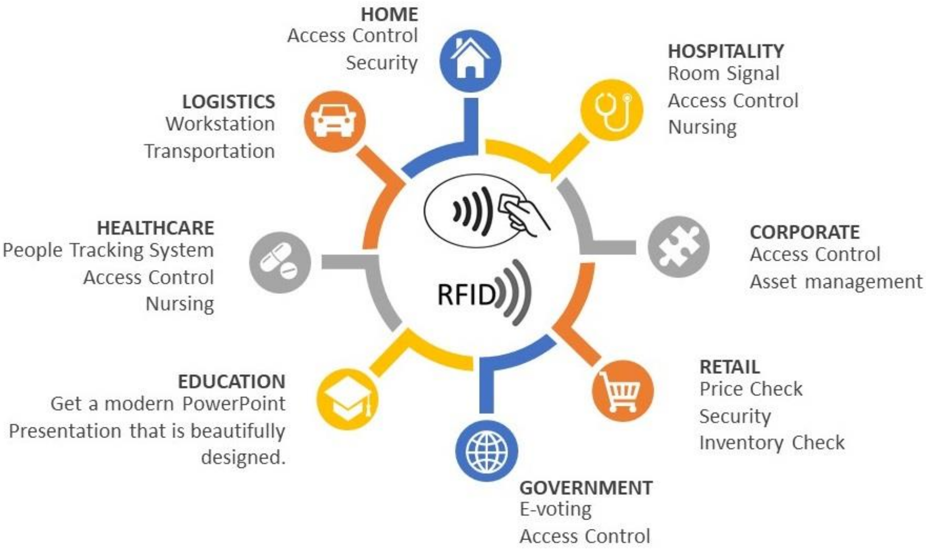


Figure 4.1: RFID in IoT

4.1.5 Near-Field Communication NFC [17]

NFC uses electromagnetic induction between two loop antennas located within each other’s near field, effectively forming an air-core transformer. NFC involves an initiator and a target; the initiator actively generates an RF field that can power a passive target that enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or battery-less cards. NFC provides high levels of convenience and interaction among all the devices in the home. All the devices can be added to a home network and can be controlled with our mobile phones and tablets. NFC gives a tap-and-go experience and its devices can register themselves on their own. For example, they can remember their warranty dates and they can remind people of when a service is required. NFC devices can be used in contactless payment systems, like those currently used in credit cards and electronic ticket smartcards, and it allow mobile payment to replace or supplement these systems.

Some benefits of NFC are:

- Short range and supports encryption.
- Low-speed connection with extremely simple setup
- Efficient data tracking
- One-step payments
- Personalized settings

A drawback of NFC is:

- His short range might not be feasible in many situations for it as it has limited availability in the market of smartphones.

4.1.6 Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances. Bluetooth exists in many products, such as telephones, tablets, media players, robotics systems. The technology is extremely useful when transferring information between two or more devices that are near each other in low-bandwidth situations. The presence of Bluetooth in our smartphones makes it easy for the developers to design a service based on it. It is so energy and power efficient that make devices run with less battery for long periods of time.

Some advantages of Bluetooth are:

- Most widely used technology.
- Every device has Bluetooth.

Some disadvantages of Bluetooth are:

- Issues in usage of Bluetooth are turned off.
- Might need to be replaced as hardware changes rapidly.

4.1.7 Summary of Communication Models

Among all the above-mentioned modes of communication, satellites are used for large networks and remaining is used for modular communication. There is no personal favorite of which mode is the best because every time there is a different use-case. For example, you use Wi-Fi if you would like to transfer large amounts of files and NFC if you want quick, short-range interaction. Henceforth, the best suited communication protocol really depends on your goals and your clearly defined use-case. In terms of security the weakest mode of communication which can be hacked or attacked by intruders is Wi-Fi and weakest mode to jam is RF.

4.2 Communication Parameters

4.2.1 Required Power

Power supply must be efficient as hundreds of nodes are spread across vast area and connectivity for communication is done via a feasible wireless technology. Hence if a node can work well with low power consumption it would be convenient to power each node from where it is located. On the other hand, if a node uses a lot of power then it increases overall system cost in terms of power consumption as well as cabling and maintaining power cables.

4.2.2 Equipment Limitation

Intruders can bypass the inbuilt layers of security and directly corrupt the data over the wire if the sensor or the node itself must be rigid and expose any of its electrical contacts to the outside world.

4.2.3 Cost of Hardware

When thousands of nodes are being used for data collection to design a system, the cost per node for implementation is very critical since it is common for some of the nodes to be down or get damaged. In conclusion, if the cost per node is very high then any replacement of nodes will be very difficult, and the maintenance of the entire system will become unfeasible.

4.2.4 Speed of Data

Data speed is crucial if the number of tuples of data sent by the sensor or a node is high enough. For example, if a temperature value is the only thing to be sent, it can be done with extremely low bandwidth network. If some data must be sent like 200 times a second to maintain precision, then in such cases higher bandwidth is required.

4.2.5 Range of Communication

Range is the first thing you consider before setting up an IoT system. Depending on the environment a suitable communication mode must be chosen to ensure a long-range communication or a small-range communication .

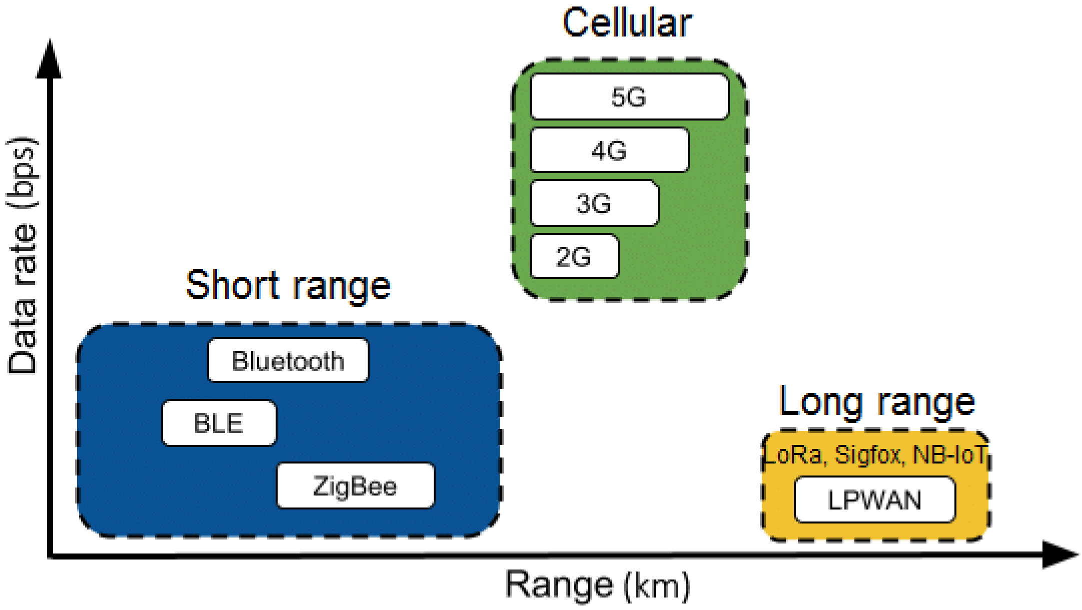


Figure 4.2: Range of Communication between different Protocols

4.3 Use Cases and Limitations

Every technology mentioned has its own limitations and use cases. For example, wireless tech is limited by its range and strength where wired tech is limited by its power, installation costs and wear. When you must choose a protocol for a given IoT system there are different parameters which have to be considered. Cases like this will need a broader understanding of using an efficient protocol and using an effective mode of communication. Large IoT systems may use multiple protocols and modes to achieve the overall optimal throughput. New modes of communication between modules have been evolving and hardware which is compatible with these is also being researched.

4.3.1 Bluetooth Limitations

- Distance

Class-2 Bluetooth devices like smartphones and laptop have a range of 10 meters. Class-1 Bluetooth devices that need more power can communicate up to 100 feet, but they are unable to be used in small portable devices.

- Slow Data Transfer Rate

Data transfer rate is around only 3 Mbps. There are different versions of Bluetooth and each of them has different speeds. Latest versions use Bluetooth in a combination with Wi-Fi to stream music or files across two devices.

- Interference

There is a frequency at which these radios work and Bluetooth devices operate at 2.4GHz which also is used by many other wireless devices. Bluetooth is designed to hop frequencies for data transfer multiple times a second to avoid interference, but if multiple devices are trying to use the same bandwidth with similar principles, it becomes difficult to avoid interference.

4.3.2 Wi-Fi Limitations

- Obstacles

Signal strength is determined from the obstacles and physical objects in the environment. Depending on the density of materials used, it becomes difficult for Wi-Fi to pass through certain materials.

- Interference

Interference is a factor for Wi-Fi as well since it operates on 2.4GHz and 5 GHz. Devices like Microwave Ovens emit high power signals at 2.4GHz and most of it is random noise which affects the whole area enough to bring down the efficiency. Also, when people get connected from distinct networks will lead to slow speeds for all.

4.3.3 Near-Field Communication (NFC) Limitations

- Expensive

  NFC technology may be too expensive for some companies, as it usually involves a suite of related devices, equipment, and upgrade-dependent standards.

- Security

Nowadays, it is easy to clone NFC or chip ID using an NFC reader. Mobile hackers have developed ingenious ways of gaining unauthorized access to personal financial data stored on phones, and the fight to secure that data is always ongoing . This can lead to steal of data while making payments, since the NFC reader may be duplicated.

Figure 4.3: NFC payment

4.3.4 Satellite, Radio Frequency (RF) and Radio Frequency Identification (RFID) Limitations

Common limitations between Satellite, RFID and Radio Frequency are interference, power, and ranges. Extremely large range for Satellite communication compared to all other modes of communication and the bandwidth at which one can communicate would be less depending on the distance.

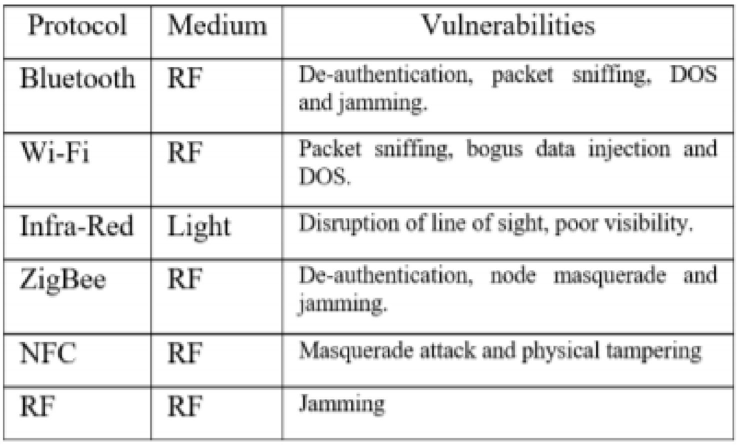
Chapter 5

5. Security Issues

Largely connected networks are prone to multiple attacks and drawbacks. Attackers aim for user’s information theft, and to damage the reputation of organization targeting the IoT devices or the weakness of Web of Things communication protocols. Some attacks are structured Query Language (SQL) injection, Cross-site Scripting attacks, session hijacking, integrity issues of information, click hijacking, link redirections, and usage of third-party Application Program Interface (APIs) with well-known vulnerabilities, etc.

5.1 Vulnerabilities

These attacks happen in the existing internet every day and have their own defense mechanism too. Antivirus programs prevent any malware from affecting the systems. In most of these attacks on the internet either the user’s private data is collected, or the required service is blocked. This is not the case in IoT, here we have data nodes which are either sensors or things equipped with a communication module. There are multiple ways for a system to be affected and it can pertain to single node or whole system. For example, the MQTT has too many security issues such as authentication, authorization, confidentiality, and integrity. Low power processing devices decrease the overhead of processing messages while exchange happen between devices. Some critical security issues can occur like fake devices insertion, DoS attack, or remote code execution attack as the MQTT protocol process messages incorrectly. Also, CoAP that uses Datagram Transport Layer Security (DTLS) protocol can be breached as its communication finishes with proxies [18]. As the proxies have the functionality of packet holding, Man-in-the-Middle (MITM) attack or DDoS attack can be performed by compromising the security of proxy.



Protocol	Medium	Vulnerabilities
Bluetooth	RF	De-authentication, packet sniffing, DOS and jamming.
Wi-Fi	RF	Packet sniffing, bogus data injection and DOS.
Infra-Red	Light	Disruption of line of sight, poor visibility.
ZigBee	RF	De-authentication, node masquerade and jamming.
NFC	RF	Masquerade attack and physical tampering
RF	RF	Jamming

Table 5.1: Protocol’s vulnerabilities

5.2 Defense

Any IoT system which has secure data transactions and deals with crucial data needs each of following components to make sure the whole system stays reliable and efficient as a single security flaw can bring down an entire system:

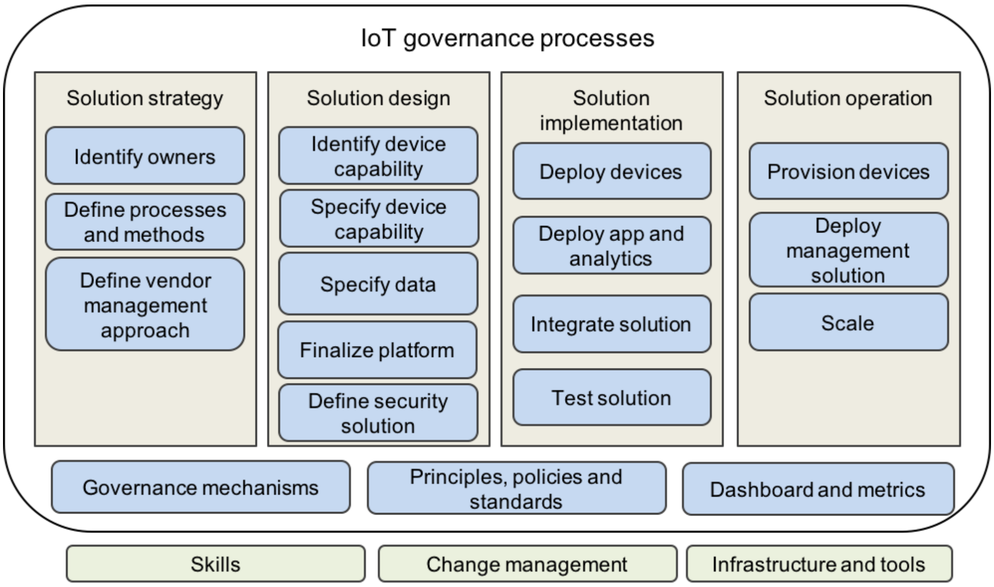


Figure 5.1: IoT governance

- Device authentication

A device should authenticate itself before transmitting or receiving data when it is plugged into a network. Machine authentication will allow a device to access the network according to the credentials that are stored in a secure area, just the way a user authentication allows the user to access a corporate network based on username and password.

- Access control

Access control is used to ensure that even if any component in the system is compromised, there would be minimal access for the intruder to other parts of the system. To gain access to a network, even if corporate credentials are managed to be stolen, the compromised information would be limited to only the areas in the network that are authorized by credentials. Minimum access needed to perform a task is authorized to minimize the effectiveness of any security breach according to the least privilege principle.

- Firewalling and Intrusion Prevention Systems

An Intrusion Prevention System monitors network traffic for signs of a possible attack. When it detects potentially dangerous activity, it takes action to stop the attack. Often this takes the form of dropping malicious packets, blocking network traffic, or resetting connections. The IDPS also usually sends an alert to security administrators about the potential malicious activity.

Firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely.

- Updates and Patches

Thousands of devices perform critical services and are dependent on the security patches to protect themselves against the inevitable vulnerability. Security patches and software updates must be delivered in a way that requires the intermittent connectivity and limited bandwidth of an embedded device and eliminates the possibility of compromising functional safety. As soon as bugs are detected in a system patches must be released.

5.3 Authentication, Encryption, and Integrity

5.3.1 Authentication

Authentication can be as simple as a username and password or could have a randomly generated hash key which could be verified on the other end. Authentication can be considered as a basic token of verification if a given element is the intended one or authorized one. This process will make sure that data does not go into wrong hands. In case of IoT authentication [19] does not only happen between a user and a system but also happens between two different hardware IoT nodes. This is because any node despite its security and safety could get corrupted or affected by a malware that can creep into network. If authentication between nodes is not implemented, in such case there is every chance for that corrupt node to transmit the malware and affect all remaining nodes.

5.3.2 Encryption

Encryption can keep the data safe even if the authentication fails at any point while data transferring between two nodes. Encryption happens differently on different modes of communication. Encryption must be implemented at every port of exit. It could be a small node or a large node. Every point which sends out data needs encryption since a single unprotected point can be dangerous for a system.

5.3.3 Integrity

When the use of encryption and authentication is implemented well, it ensures the integrity of data being are transferred safely. The integrity of data is not lost when the data being sent is untouched and unmodified during transfer [20].

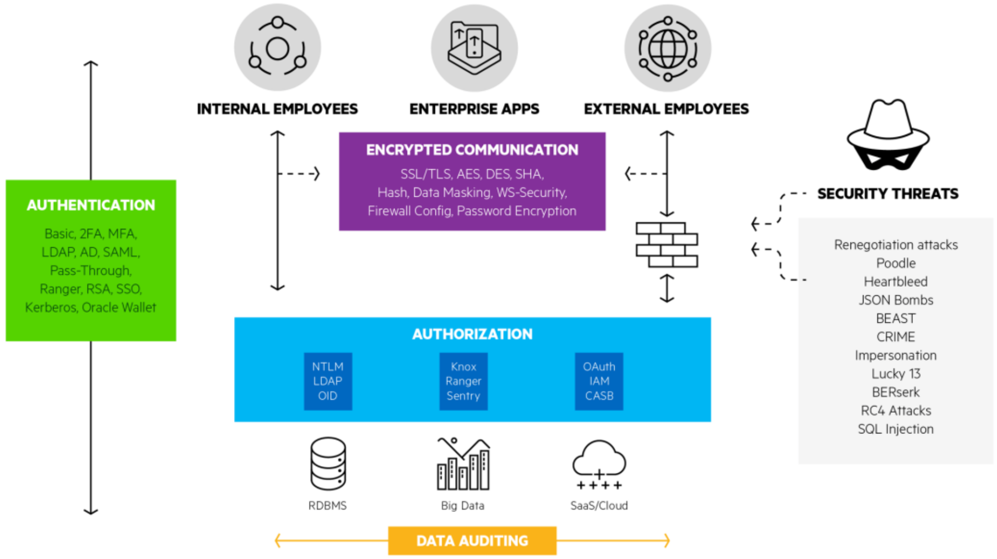


Figure 5.2: Data Security

Chapter 6

6. Implementing IoT

With IoT the number of inputs and outputs is unlimited making IoT much more flexible and scalable. To adapt to this new situation, or even become an implementor yourself, one of the most critical concepts to understand and to implement is the Internet of Things (IoT). There are two types of IoT: CIoT and IIoT. The difference is that CIoT focuses on the "Customer", whereas IIoT is focused on the "Industry" department. Deeper meaning of IoT can be categorized to:

- Connectivity

Any physical object that can be uniquely identified (URI) and a send/receive data by connecting to a network can connect to the internet. Cameras, video games, smartphones, vehicles, buildings can be connected among themselves with a central server or with the cloud.

- Information and Communication

Every information is shared to their designated endpoints either other things or servers by constantly sending information about status, actions, sensor data, and more with their unique ID attached.

- Action and Interaction

IoT is connection and information sharing. Most important part of that is the use of automation: computers using the data to automatically make decisions and monitor situations, letting people know the state of something or some process.

6.1 Challenges

There is always fear with new technologies emerging every day while considering implementing IoT as there are always potential issues related to lack of maturity and adoption that must be kept in mind. You must invest in new hardware, modify existing ones, and hire specialized personnel. You must think about privacy and security as all your data will be sent to the cloud and with everything connected to the internet that means you have yet another security concern aside from hacking and attacks. You must create a powerful infrastructure such as databases, network coverage, fast internet and systems designed for handling IoT. In addition, to meet the needs of the present and future, the systems you create must be flexible enough to evolve and adapt to the changing requirements over time.

6.2 Implementation Steps

It is important to ensure that IoT will improve your business in a way that will not only repay the investment but open the possibility for higher cost-efficiency of your existing service, product, or production line. Some steps you must follow to implement IoT are:

1. Business Objectives: What problem are you looking to solve, what do you want to achieve by solving it and what is the best and efficient way to solve it? IoT can more easily be implemented gradually, restricting it to the amount of capital you are able to expend every month or year on process optimization.

2. IoT Use Cases: IoT is relatively new but exists for long enough to have gotten well developed and established in some areas. After identifying your problem and goals, you should check if you have similar use case to other IoT implementations. The number and variety of enterprise IoT initiatives are growing, which means there is already several compelling use cases.

3. Hardware: Not all devices run on these different protocols we mentioned in this thesis so be aware about connectivity and interoperability before you commit to a purchase of a hardware like sensors, connection devices, gateways, and communication protocols.

4. IoT platform: The IoT platform defines how everything communicates and how data is handled. An IoT platform is the software used to control and centralize every aspect of the IoT network and its connected devices, including sending commands and gathering data, commonly by means of cloud integration. It can either be custom made in-house or obtained from a specialized supplier.

5. Create prototypes: Prototyping consists of using already available, less robust systems that can be easily attached and removed as needed, to figure out what works and what does not. Before starting implementation, gather a team from various departments like Computer, Software, Electronic, Mechatronic Engineer and IT Expert to think it through. You will need people with different expertise throughout the project's inception, design, prototyping, implementation, and incrementation as IoT involves many different systems interacting with each other.

6. Implement Machine Learning: Machine learning consists of an AI that is programmed to review data in real-time, identify patterns in them, and, depending on implementation, act on it.

7. Security: To protect your business, many measures have already been developed. You can find common solutions from the company Cloud Security Alliance (CSA) as it has a complete set of guidelines on how to properly secure IoT networks.

6.3 Risks

As with any investment, there are always risks associated. IoT is a rather new technology with very few standards, and few legacy equipment as of today, which means that investing in it is always riskier than investing in already established and well-tested technologies. Some risks are:

1. Implementation failure: Maybe your objective requires many things to be done in small time frames or your production facility is situated in an area that does not have fast enough internet or there is insufficient budget available. You may not be able to implement IoT into your business.

2. Security: As simple as a DDoS attack can shut down productions, or a well-planned attack can give unauthorized third parties access to all the data gathered by the sensors throughout the years or even your customer's information. If you are especially a small company this could be catastrophic for your business. Think about security measures like Endpoint security, Access Control, Encryption, and Fraud Management.

3. Internet coverage: If your production lines depend on IoT technology to function, whenever the internet goes down, production will stop.

6.4 Thoughts on Implementing IoT

The Internet of Things is a rather complicated world full of intricacies and risks, but also able to give you profit and reward. When you are implementing IoT every step of the project features new challenges and every challenge must be identified, acknowledged, and solved. Try to form a team of experts and work together every step of the way. If you do it slowly and safely, there is no need to fear to invest in IoT. Do not be afraid to ask, and do not be afraid to research. Even if it does not work, be patience. New technologies and solutions will come out, and maybe one of it can be your solution. More importantly implement security measures and maintain up-to-date documentation, as well as keeping it updated.

IoT is a great revolution in the way we do things as it can give you a competitive edge like never seen before. Try to read more in-depth information and knowledge regarding IoT in the Web of Things to create your own opinion and speculations.

Chapter 7

7. Conclusions

This thesis introduced a range of communication protocols used to implement IoT devices currently available on the market. Most used communication protocols were chosen and theoretically analyzed in depth. Also, the analysis described how to the protocols worked, what are their role and what benefits/drawbacks they have. Issue of the security of these protocols was also discussed and some solutions were provided. In addition, different measures were taken to help people choose which protocol is used best for each IoT device in each use-case and environment. From the analysis the following conclusions were noticed:

- Security

In terms of security, some of the communication protocols have the encryption and authentication mechanisms. LoRaWAN, ZigBee, BLE, NFC, Z-Wave use the Advanced Encryption Standard (AES) block cipher with counter mode, while Cellular and RFID use RC4. However, several serious weaknesses were identified. AES is extremely secure and slow while RC4 is extremely weak and very fast.

- Power Consumption

ZigBee, BLE, NFC, Z-Wave offer low power consumption as they are designed for portable devices and limited battery power. Cellular uses high power consumption.

- Data rate

LoRaWAN, ZigBee, BLE, NFC, Z-Wave have data rate lower than 2 Mbps while RFID has the highest data rate of 4 Mbps.

- Range

ZigBee, BLE, NFC, Z-Wave, RFID have shorter range and cover less than one km. LoRaWAN in an urban environment with an outdoor gateway, you can expect up to 2-3 km wide coverage, while in the rural areas it can reach beyond 5 to 7 km. Cellular can reach up to 8 km and in clear areas up to 40km.

Internet of Things is being implemented to almost any device you think of. Most of the necessary technological advances needed for it have already been made, and some manufacturers and agencies have already been using it in large-scale.

As there are many wireless technologies in the IoT network, each one has certain specifications and benefits. However, it is quite hard to conclude which one is perfect. Therefore, the question that someone needs to answer is which technology is the best one for my application. New technologies are coming up which would help IoT grow and allow more robust communications to happen. IoT will unveil a whole new era of data exchange, interaction and wireless devices embedded in every corner of the world.

Chapter 8

8. Future work

There is every scope of improvising the work done in this thesis. This chapter will discuss the further improvements and work that can be done to make this research more useful. We can create a hub of multiple IoT nodes and develop a prediction algorithm for the behavior of the nodes. This can be achieved by applying artificial intelligence along with machine learning algorithms.

Another extension would be to build a web interface to monitor all the nodes/sensors live with a given refresh frequency. A web service would pull data from all nodes at regular intervals and then would update the visualizations for the user in real time. This will help analyze the real-time problems that can occur during the data collection process, maintaining the data on a database and giving the application a seamless flow between data collection and representation to the user.

We can create a communication technology in smart grids and use a communication protocol like ZigBee. In the application part, we can build a single phased energy monitoring system and monitor the consumption values provided by the Internet. Application will have two separated units, the web server unit and sensor unit. These two units can be managed by an Arduino microcontroller card and the communication between these units by 2 ZigBee devices. The energy monitoring application can send energy consumption values received from the sensors to the web server using ZigBee implementation.

Another example could be to have 2 android devices connected to a test app and the test app will connect the 2 devices together through Bluetooth Low Energy. We could implement BLE in sequential-send mode, which means messages will not be sent out at the same time. Instead, each message will wait for a signal from the remote device before writing a new data to BLE characteristic. In this way, the connection between the devices will become more stable. Since the design of BLE aims to support lightweight data transfer, it is important to get its performance with the minimum payload. With this experiment we can try different patterns like sending multiple BLE packets of data by controlling the payload of a CoAP message or even having the packets doing a round trip where the header request always sends a response to the sender.

Bibliography

[1] Keertikumar M, Shubham M, R. M. Banakar, "Evolution of IoT in smart vehicles: An overview", 2015 International Conference on Green Computing and Internet of Things.

[2] Abdessamad Mektoubi, Hicham Lalaoui Hassani, Hicham Belhadaoui, Mounir Rifi, Abdelouahed Zakari, "New approach for securing communication over MQTT protocol A comparaison between RSA and Elliptic Curve" 2016 Third International Conference on Systems of Collaboration (SysCo).

[3] Pavel Smutný, "Different perspectives on classification of the Internet of Things", 2016 17th International Carpathian Control Conference (ICCC).

[4] Sanaah Al Salami, Joonsang Baek, Khaled Salah, Ernesto Damiani, "Lightweight Encryption for Smart Home" 2016 11th International Conference on Availability, Reliability and Security (ARES).

[5] Diana Cecilia Yacchirema Vargas, Carlos Enrique Palau Salvador, "Smart IoT Gateway for Heterogeneous Devices Interoperability", IEEE Latin America Transactions-2016.

[6] Zhaozong Meng, Zhipeng Wu, Cahyo Muvianto, John Gray, "A Data-Oriented M2M Messaging Mechanism for Industrial IoT Applications", IEEE Internet of Things Journal-2017.

[7] Xinlei Wang, Jianqing Zhang, Eve M. Schooler, Mihaela Ion, "Performance evaluation of AttributeBased Encryption: Toward data privacy in the IoT", 2014 IEEE International Conference on Communications (ICC).

[8] Jia Guo, Ing-Ray Chen, Jeffrey J. P. Tsai, Hamid Al-Hamadi, "A hierarchical cloud architecture for integrated mobility, service, and trust management of service-oriented IoT systems", 2016 Sixth International Conference on Innovative Computing Technology.

[9] Jarkko Kuusijärvi, Reijo Savola, Pekka Savolainen, Antti Evesti, “Mitigating IoT security threats with a trusted Network element”, 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST).

[10] H. Rashidzadeh, P. S. Kasargod, T. M. Supon, R. Rashidzadeh, M. Ahmadi, “Energy harvesting for IoT
sensors utilizing MEMS technology”, 2016 IEEE Canadian Conference on Electrical and Computer Engineering.

[11] G. V. Vivek, M. P. Sunil, “Enabling IOT services using WIFI - ZigBee gateway for a home automation system”, 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN).

[12] Meena Singh, M. A. Rajan, V. L. Shivraj, P. Balamuralidhar, “Secure MQTT for Internet of Things (IoT)”, 2015 Fifth International Conference on Communication Systems and Network Technologies.

[13] P. Martin, B.-J. Ho, N. Grupen, S. Munoz, and M. Srivastava, “Anibeacon primer for indoor localization,” inBuildSys’14. ACM, 2014.

[14] Eqiva, “Bluetooth smart radiator thermostat,” http://www.eq-3.com/products/eqiva/bluetooth-smart-radiator-thermostat.html, 2017.

[15] Virendra Gupta, Jayaraghavendran, “Invited Talk: IoT Protocols War and the Way Forward”, 2015 28th International Conference on VLSI Design.

[16] Shikhar Bahl, Peeyush Chandra, Vandana Rathore, Alka Shukla, Akash Garg, “Wireless ethernet for IoT: A case study”, 2016 10th International Conference on Intelligent Systems and Control (ISCO).

[17] Kishore Kumar Reddy N. G., Rajeshwari K., “Interactive clothes based on IOT using NFC and Mobile Application”, 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)

[18] G. Selander, J. Mattsson, F. Palombini, and L. Seitz, “Object Security of Coap (Oscoap)”, Internet Engineering Task Force (IETF) Internet-Draft work in progress, 2017

[19] Zhonglei Gu and Yang Liu, “Scalable Group Audio-Based Authentication Scheme for IoT Devices”, 2016 12th International Conference on Computational Intelligence and Security.

[20] Azhar Syed, R. Mary Lourde, ” Hardware Security Threats to DSP Applications in an IoT Network”, 2016 IEEE International Symposium on Nanoelectronic and Information Systems