Comparison of Internet of Things (IoT) Data Link Protocols

Azamuddin Bin Ab Rahman (A paper written under the guidance of Prof. Raj Jain)

Download

Abstract:

ZigBee, Bluetooth LE, Z Wave, NFC, HomePlug GP and Wi-Fi are six protocols standard for short range wireless communications with low power consumption. From an application point of view, ZigBee is designed for reliable wirelessly networked monitoring and control network, Bluetooth is intended for a cordless mouse, keyboard, and hands-free headset, Z-Wave is for home appliances to communicate with one another for the purposes of home automation, and NFC is to establish radio communication with each other by touching the devices together. Furthermore, HomePlug GP specifications target broadband applications such as in-home distribution of low data rate IPTV, gaming, and Internet content, while Wi-Fi is directed at computer-to-computer connections as an extension or substitution of cabled networks. In this paper, we provide a study of these six wireless communication standards, comparing their main features and behaviors in terms of various metrics, including the transmission time, modulation type, and power consumption. It is believed that the comparison presented in this paper would benefit researchers in selecting an appropriate protocol.

Keywords: IoT, Data Link Protocols, ZigBee, Bluetooth, Bluetooth Low Energy (LE), Z-Wave, Near Field Communication (NFC), HomePlug Green PHY (GP), Wi-Fi.

Table of Contents:

1.0 Introduction

The Internet-of-Things (IoTs) is a vision of connectivity for anything, at anytime and anywhere, which may impose an impact on our daily life dramatically as what internet has had in the past 20 years. It is regarded as an extension of today's Internet to the real world of physical objects, which is often associated with such terms as 'ambient intelligent', 'ubiquitous network', and 'cyber-physical system'. In recent years, with the development of computer science, communication technology and the network of things has made a great breakthrough. The IoT applications has been used in many fields, from the earliest wireless sensor networks such as the smart grid, smart healthcare, smart agriculture, military and so on. A combination of technologies, including low-cost sensors, low-power processors, scalable cloud computing, and ubiquitous wireless connectivity, has enabled this revolution. Many companies are using these technologies to embed intelligence and sensing capabilities in their products, thereby enable objects to sense, learn from, and interact with, their environment. Some of these devices engage in machine-to-machine communication. For example, sensors on the roadway electronically alert cars to potential hazards, and the smart grid sends dynamic electricity pricing data to home appliances in order to optimize power consumption. The wireless technology standards are everywhere.

Bluetooth, ZigBee, Wi-Fi, and cellular technologies are the most well known standards. A combination of these standards is envisaged to be used to construct the smart home. Effectively all wireless technologies that can support some form of remote data transfer, sensing and control are candidates for inclusion in the smart home portfolio. Interacting with individual devices and appliances can introduce a basic level of intelligence to the home environment. However, the level of intelligence can be greatly enhanced once devices, be it simple sensors or complex appliances, can exchange information and effectively share the decision making process to offer a certain type of service to the occupant of an intelligent environment.

Bluetooth, ZigBee, Wi-Fi, and cellular technologies are the most well known standards. A combination of these standards is envisaged to be used to construct the smart home. Effectively all wireless technologies that can support some form of remote data transfer, sensing and control are candidates for inclusion in the smart home portfolio. Interacting with individual devices and appliances can introduce a basic level of intelligence to the home environment. However, the level of intelligence can be greatly enhanced once devices, be it simple sensors or complex appliances, can exchange information and effectively share the decision making process to offer a certain type of service to the occupant of an intelligent environment.

The remainder of this paper is organized as follows. Section II, we describe some of IoT data link protocols (ZigBee, Bluetooth Low Energy (LE), Z-Wave, NFC, HomePlug GP, and Wi-Fi); in Section III, we compare these six protocols that have been chosen and finally, conclusion is presented in Section IV.

2.0 IoT Data Link Protocols

This section introduces the Bluetooth LE, Z-Wave, ZigBee, NFC, HomePlug GP and Wi-Fi protocols, which corresponds to the IoT data link Protocols. The IEEE defines only the PHY and MAC layers in its standards. For each protocol, separate alliances of companies worked to develop specifications covering the network, security and application profile layers so that the commercial potential of the standards could be realized. The major goal of this paper is not to contribute to research in the area of wireless standards, but to present a comparison study of the six main short-range wireless networks.

2.1 ZigBee

ZigBee is a new technology of a short-range, low complexity, low-power consumption, low-data-rate, low-cost and duplex wireless communication [li14]. It is applied on the low- data-rate wireless data communication between various electronic equipment within a short distance. The physical layer and link layer protocol of ZigBee technology applied mainly IEEE802.15.4 standard, and the ZigBee Alliance that was set up in August 2002 is responsible for the development of network layer and application layer and so on. IEEE 802.15.4 ZigBee standards were approved in the May 2003 [shyan13]. ZigBee is characterized by short distance wireless communication and low power consumption. ZigBee leverages the IEEE 802.15.4 physical layer. Though the maximum transmission speed is 250 kbps and lower than Bluetooth and Bluetooth LE, it is suitable for the application for which data traffic is a little and a lot of devices are necessary.

Radio modules corresponding to this specification are provided from many vendors. So it is convenient to construct sensor network, and try to apply to a variety of monitoring and control applications such as air-conditioning control, lighting control, physical distribution management, house control, the measurement instrument and so on. IEEE 802.15.4 has set up a working group to define a low complexity, low-cost and low- power consumption low-rate wireless connectivity that would be used in suitable fixed, portable or mobile devices. With power-saving, reliable, low-cost, large capacity, security, and many other advantages the ZigBee networks pay the way for its widely applications in various fields of Automatic Control.

Currently, ZigBee mainly used in transmitting information among the various electronic equipment which are within short-distance and data transmission rate is not very high. It mainly targets the markets of PC peripherals (mouse, keyboard, games control rod), and consumer electronics equipment (TV, VCR, CD, VCD, DVD remote control devices and other equipment), the family of Intelligent Control (lighting, gas measurement and Alarm, etc.), toys (electronic pets), health care (monitors and sensors), and industrial controls (monitors, sensors and automation equipment). Usually, any applications which are small space between equipment; low cost, low data rate transmission; small equipment size, inadmissibility of big power module; hard to frequent replace or repeat recharge battery can be considered to use ZigBee technology. It can also complete transmission and exchange of information among physical things, so we can use the technology to complete the same mission in the construction of Internet of Things, then combined with Internet and database technology, we would set up Internet of Things.

IEEE 802.15.4 standard defines Star, Cluster Tree and Mesh networks as possible topologies for the wireless network as shown in Fig. 1. However, mesh networks enable high levels of reliability and longer coverage range by providing more than one path through the network for any wireless link. Note that in any ZigBee network there are three types of ZigBee devices [zhou11]: PAN coordinator: There is only one coordinator in a network that is responsible for starting the network, binding together devices. Also it routes data between different devices. It is a Full Function Device (FFD) and it is usually mains powered device. A router: It cannot start the network however it scans a network to join it. Once it is in the network it can route data between Reduced Function Devices (RFD). It is a FFD and it is usually mains powered device. An end device: It cannot start a network however it scans a network to join it. It can be either a RFD or FFD and it is usually battery powered device [xiolin10].

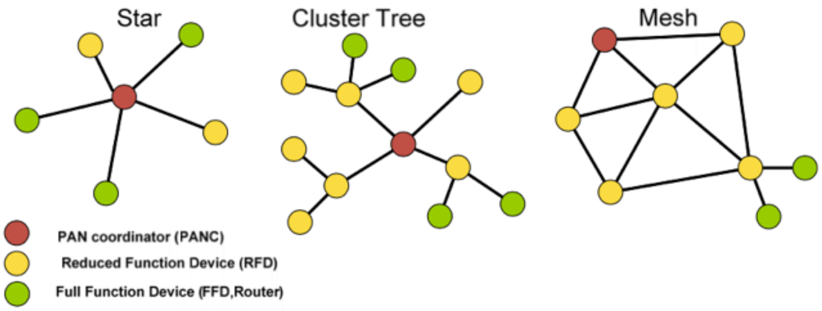

Star
Cluster Tree
Mesh
PAN coordinator (PANC)
Reduced Function Device (RFD)
Full Function Device (FFD,Router)

Figure 1: Star, Cluster Tree and Mesh Topology [zhou11].

2.2 Bluetooth LE

Bluetooth LE is the hallmark feature of the Bluetooth 4.0 specification. It has been designed for ultra- low-power applications, yet keeping similarities with classic Bluetooth [chris15]. Remarkably, a Bluetooth LE implementation can reuse classic Bluetooth circuitry components. Therefore, the upside potential for Bluetooth LE is enormous given that future mobile phones that have a Bluetooth chipset are expected to include Bluetooth LE as well. Nevertheless, in order to achieve the goal of ultra-low-power consumption, major changes have been made to the Bluetooth LE protocol stack.

At the Physical Layer, Bluetooth LE still uses adaptive Frequency Hopping Spread Spectrum (FHSS). The number of channels is reduced from 79 (in classic Bluetooth) to 40 [Kuor11]. The raw data rate of Bluetooth LE is 1 Mb/s. In terms of coverage, Bluetooth LE typically has a range of up to a few tens of meters. The Link Layer specifies, among others, the functionality for bidirectional communication between two devices, which requires them to establish a connection. As defined in [chris15], two roles for connected devices, called master and slave. Prior to connection establishment, the devices that will be in the slave role announce their presence and connect ability, while the device that will be in the master role listens for those announcements and initiates the connection establishment by transmitting a message called Connection Request to each device it attempts to connect to. A master can manage multiple simultaneous connections with several slaves, whereas a slave can only be connected with a single master. Therefore, Bluetooth LE defines a star topology. The connection establishment time between a master and a slave takes less than 3 ms. Once two devices are connected, a Time Division Multiple Access (TDMA) scheme is used by the master for scheduling the start of connection events, in which communication between master and slave takes place. The Connection Request message serves as a reference for synchronization between master and slave [hansen15].

On top of a Link Layer connection, the Logical Link Control and Adaptation Protocol (L2CAP) multiplexes upper layer data and may perform segmentation, retransmission, and detection of duplicate packets, depending on the L2CAP mode in use. Bluetooth LE uses the Basic L2CAP Mode, which does not provide segmentation or reliability services. Above L2CAP, the Generic Access Profile (GAP), Generic Attribute Profile (GATT), and the Attribute Protocol (ATT) allow applications to communicate and/or request data stored in structures called attributes. Using Bluetooth LE for Internet connectivity and applications poses challenges beyond IPv6 packet transport, including gateway operation, application protocol efficiency, and security. A central piece of this solution is the IPv6 over Bluetooth LE specification that is currently being produced by the IETF [chris15] and is expected to become a standard in the near future. It is crucial to understand the capabilities and performance trade-offs of the solution.

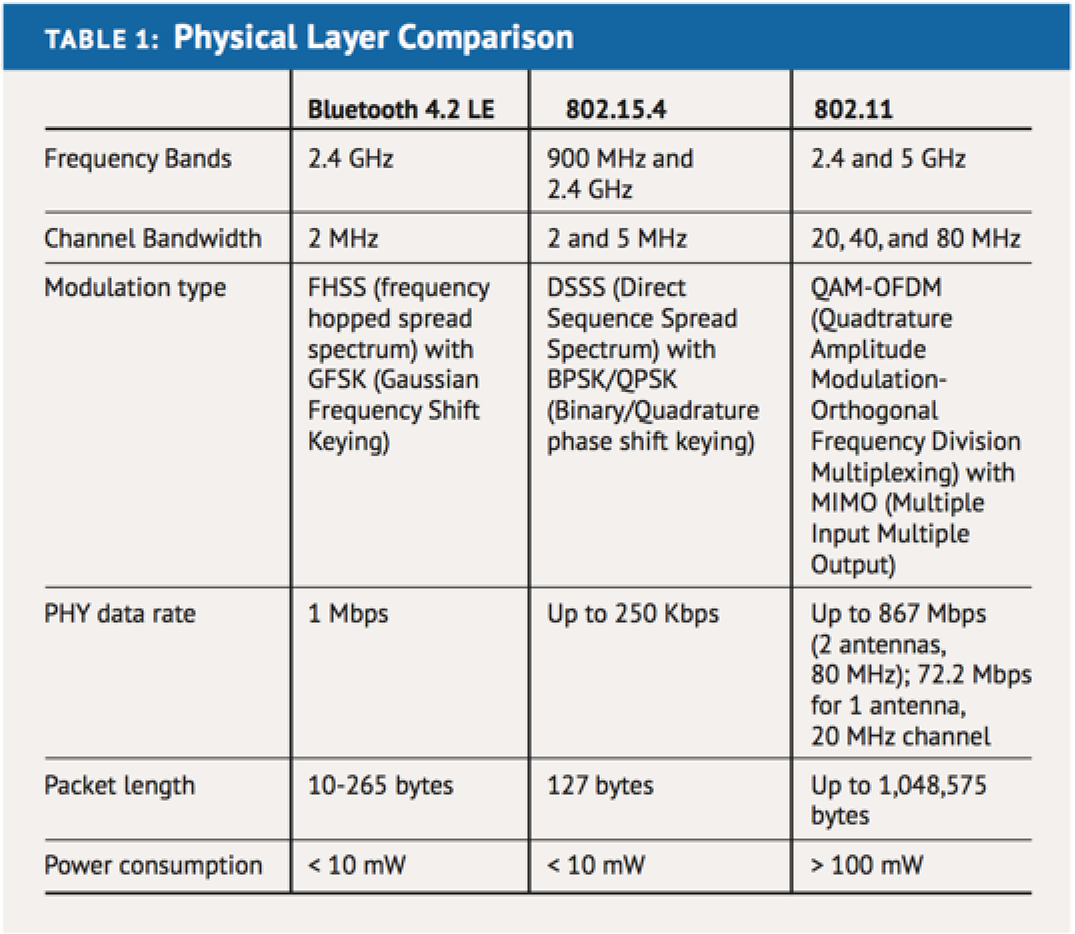


TABLE 1: Physical Layer Comparison

	Bluetooth 4.2 LE	802.15.4	802.11
Frequency Bands	2.4 GHz	900 MHz and 2.4 GHz	2.4 and 5 GHz
Channel Bandwidth	2 MHz	2 and 5 MHz	20, 40, and 80 MHz
Modulation type	FHSS (frequency hopped spread spectrum) with GFSK (Gaussian Frequency Shift Keying)	DSSS (Direct Sequence Spread Spectrum) with BPSK/QPSK (Binary/Quadrature phase shift keying)	QAM-OFDM (Quadtrature Amplitude Modulation-Orthogonal Frequency Division Multiplexing) with MIMO (Multiple Input Multiple Output)
PHY data rate	1 Mbps	Up to 250 Kbps	Up to 867 Mbps (2 antennas, 80 MHz); 72.2 Mbps for 1 antenna, 20 MHz channel
Packet length	10-265 bytes	127 bytes	Up to 1,048,575 bytes
Power consumption	< 10 mW	< 10 mW	> 100 mW

Figure 2: Physical Layer Communication [chris15].

A comparison of the Bluetooth LE physical layer with IEEE 802.15.4 and IEEE 802.11 is given in Table 1. Both Bluetooth LE and 802.15.4 are low data rate PHYs that employ spectrum spreading, which means the bandwidth occupied by the signal over the air is much greater than the transmitted data rate. IEEE 802.11 also employs spectrum spreading at the lower data rates (1 - 2 Mbps) but to achieve high speeds, it employs bandwidth efficient modulations. Spectrum spreading allows uncoordinated, low data rate wireless connections to share the radio spectrum without interfering. Frequency hopped spread spectrum, used by Bluetooth LE, changes the radio frequency in each transmission burst according to a pseudo random pattern [hansen15]. Different networks employ different hopping patterns. Thus, the likelihood of two networks simultaneously sharing a channel is low. If a particular hop results in interference, there will not be interference on the next hop, so any lost data can be re-transmitted without error. Direct sequence spread spectrum works in a different way. It makes data transmissions more immune to noise or interference by modulating the data with sequences that switch much faster than the data's bit rate. The result is a transmitted signal that occupies a wider swath of radio spectrum. The effect for uncoordinated radio links is the same, however. More radio links can share a given slice of radio spectrum without interfering.

In contrast, IEEE 802.11 networks choose to coordinate transmissions at the MAC (media access control) layer. This has an advantage of allowing high speed, bandwidth efficient communications [nieman14]. However, there is a cost in power consumption because all devices must actively sense the medium before transmission. Furthermore, bandwidth efficient communication is inherently more power consuming because the physical layer must be designed to accommodate high dynamic range signals. Two examples are provided for internetworking with Bluetooth LE. The first, shown in Figure 3, is a fixed infrastructure model. A typical home will already have Internet access through one or more Wi-Fi APs. A router gateway can be added to the home to provide connectivity to Bluetooth LE enabled IoT devices. The gateway can either be a stand-alone device or it could be incorporated into another fixed device. In Figure 3, it is shown as a stand-alone device. IPv6 packets over Bluetooth LE are routed by the gateway over either the Bluetooth LE interface or over the Wi-Fi interface, depending on their final destination. An Internet-based application for controlling the lamp or washing machine will employ the 6LoWPAN protocol from the device to the gateway. As with any Bluetooth connection, the devices must first be paired for authentication and for key generation.

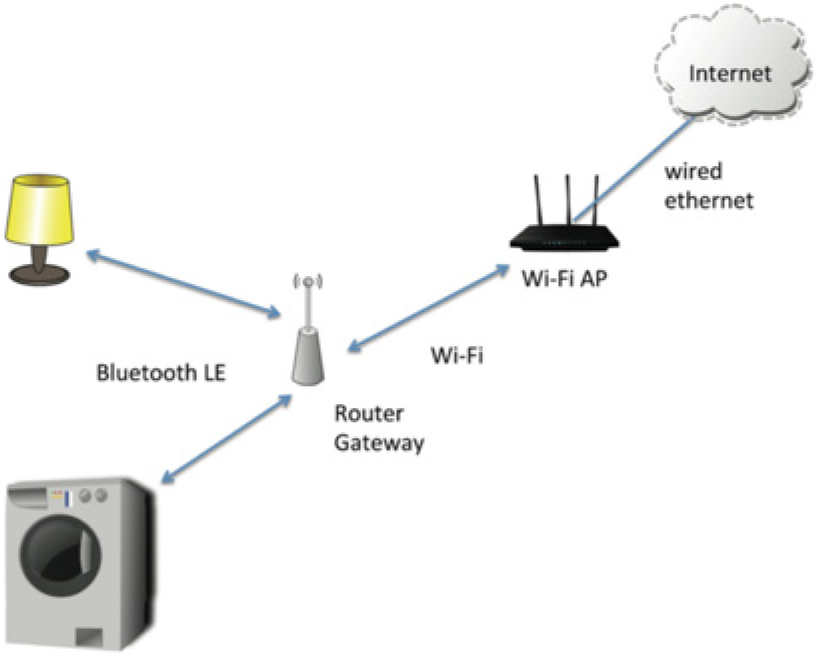


Figure 3: Internetworking with Fixed Bluetooth LE Gateway [hansen15].

2.3 Z-Wave

The Z-Wave protocol was explicitly developed by Zensys for home control applications [zwave15]. It is a proprietary protocol, with two basic types of devices: controlling and slave devices. Slave nodes reply and execute commands sent by controlling devices that initiate messages within the network. There is always a single controller (primary controller) that holds authoritative network topology information. Slave nodes can have several forms depending on their function. Routing slaves forward commands to other. nodes, enabling a controller to communicate with nodes out of direct radio reach as shown in Figure 4. At data frame creation the whole route is known, meaning a source routing is used. Networks can be formed with up to 232 devices. FSK (frequency shift keying) modulation is used at 908.42 MHz in the US and 868.42 MHz in Europe. The RF data rate is advertised as being up to 40 kbit/s and was not tested in this work.

Since it is intended for wireless home control applications, Z-Wave radio networking is designed for relatively few nodes (232 maximum, but manufacturers recommend no more than 30-50) that communicate on average every 5 to 15 minutes. Its messages are variable length, with a payload averaging 4 to 6 bytes. Message latency requirements are relaxed to 200 milliseconds or more.

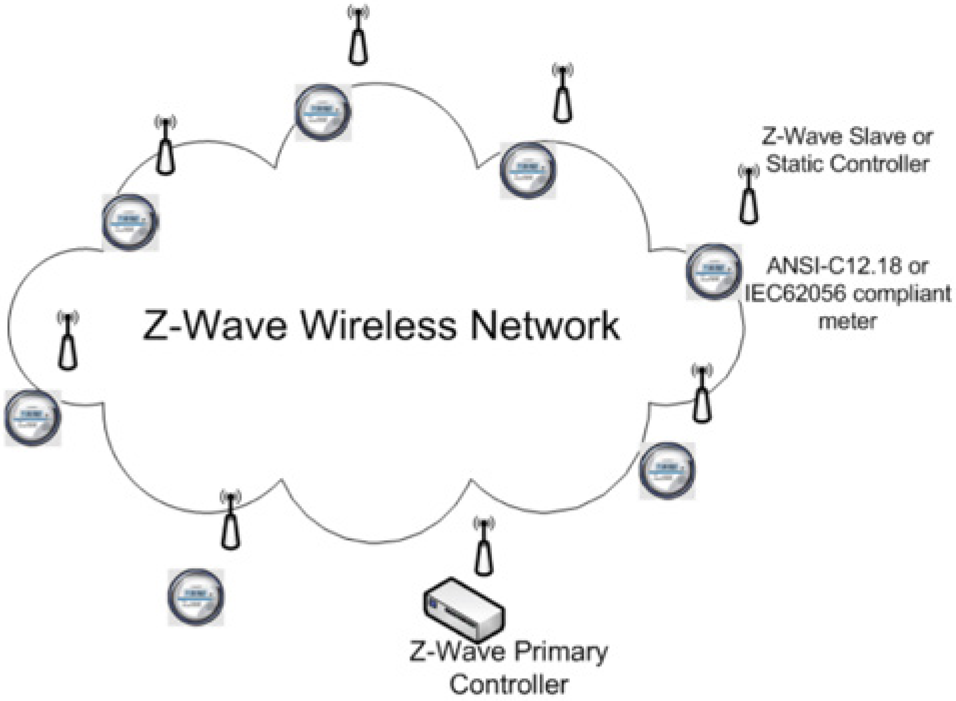

Z-Wave Wireless Network
Z-Wave Slave or Static Controller
ANSI-C12.18 or IEC62056 compliant meter
Z-Wave Primary Controller

Figure 4: AMR infrastructure architecture [zwave15].

The Z-Wave protocol consist of 4 OSI layers as illustrated in Fig 5, the MAC layer that controls the RF media, the Transfer Layer that controls that handles frame integrity checks, acknowledgements, and retransmissions, the Routing Layer that controls the routing of frames in the network and application interface and the application layer that controls the payload in the transmitted and received frames. Most notably, Z-Wave routes its messages through the network using a Source Routing Algorithm (SRA). The SRA requires message initiator devices to know the arrangement of other devices in the network (the topology) so that they can compute the best route for messages to travel. Maintaining and distributing a network topology database is an intricate software task, especially when some devices in the network are mobile. Therefore, to keep costs down, Z-Wave defines different kinds of devices, with the lowest cost devices, called slaves, unable to initiate messages.

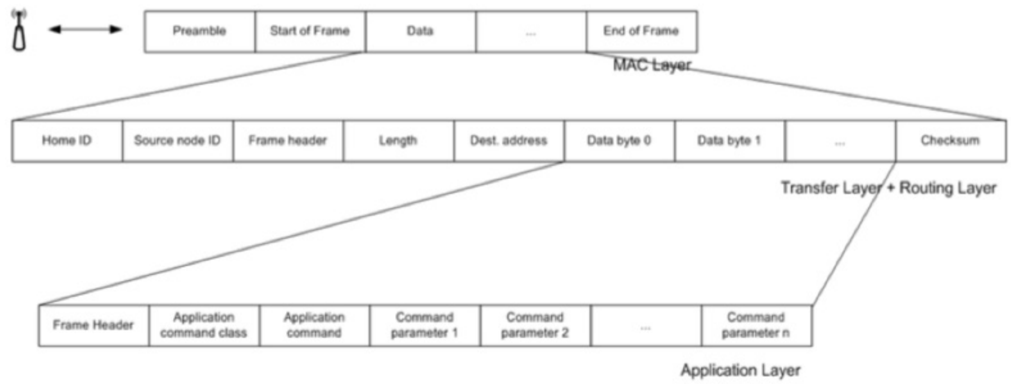


Figure 5: OSI model for Z-Wave Protocol [amaro11].

The minimum length of a properly formatted Z-Wave message is 9 bytes, but a routed message requires 12 bytes plus repeater data plus the payload. The message protocol includes routing, frame acknowledgement, collision avoidance with random back off and a frame checksum with retransmission if necessary. The Z-Wave network is self-organizing and self-healing. To achieve self-organization, Z-Wave nodes have software that discovers the node's neighbors and informs the network's Static Update Controller (SUC) about them. A Source Routing Algorithm (SRA) in devices capable of initiating communication finds message pathways and generates routes based on a network topology database. Self-healing requires software to dynamically generate new routes around temporarily unavailable nodes. Moving nodes have software routines that can request new neighbor searches automatically. This software, which is part of the Z-Wave stack, resides in on-chip memory.

2.4 Near Field Communication (NFC)

The NFC technology was initially developed and standardized by the end of the twentieth century for the transport market. The main idea was to deploy electronic ticketing based on secure microcontrollers (today called secure elements) similar to those used in SIM cards, and remotely feed by inductive coupling. The multiplicity of radio coding schemes leads to the definition of a complex set of standards, supporting three working modes, reader/writer, card emulation and P2P (peer to peer). The NFC forum was founded in 2004, in order to promote the use of NFC technology. It provides a framework for application development, and releases specifications. Some of them like the NFCIP-1 [baldo10], which defines the peer to peer mode, have been endorsed by standardization organizations.

As illustrated by the figure 6, the physical layer is based on ISO14443 (A, B, F) standards [coskun12]. Additional frames have been introduced in order to support read and write facilities for NFC tags. NFCIP-1 stands for "Near Field Communication Interface and Protocol", although compatible with ISO14443-A and ISO 14443-F physical layer; it provides a peer to peer framework that was not previously described by ISO14443 standards. Up to now, many NFC trials are conducted over the world, especially in payment domain. All trials conclude the fact that with the development of NFC technology, mobile phone is subject to become safer, more convenient, speedier and more fashionable physical instrument. NFC technology allows people to integrate their daily-use loyalty cards, credit cards into their mobile phones. In addition to integrating those cards into mobile devices, NFC technology brings innovation opportunities to mobile communications. It enables two users to easily communicate and exchange data simply by touching two mobile phones to each other. Moreover, NFC technology gives NFC reader capability to mobile phones; hence RFID (Radio Frequency Identification) tags can be read.

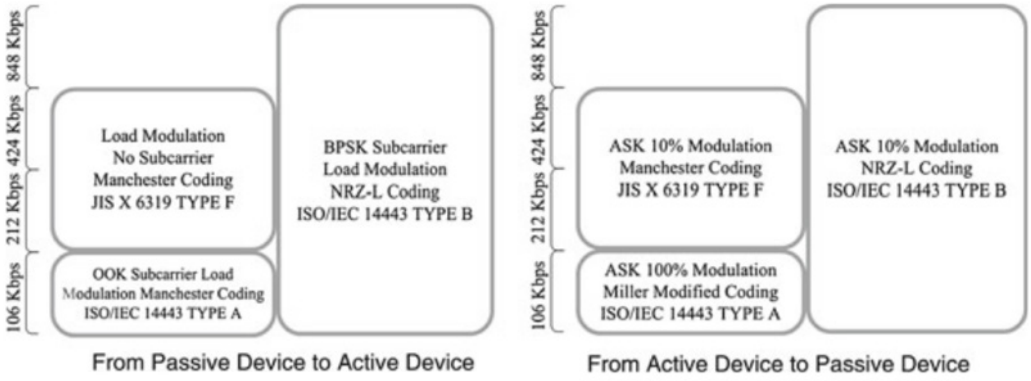

106 Kbps
212 Kbps
424 Kbps
848 Kbps
Load Modulation No Subcarrier Manchester Coding JIS X 6319 TYPE F
OOK Subcarrier Load Modulation Manchester Coding ISO/IEC 14443 TYPE A
BPSK Subcarrier Load Modulation NRZ-L Coding ISO/IEC 14443 TYPE B
From Passive Device to Active Device
106 Kbps
212 Kbps
424 Kbps
848 Kbps
ASK 10% Modulation Manchester Coding JIS X 6319 TYPE F
ASK 100% Modulation Miller Modified Coding ISO/IEC 14443 TYPE A
ASK 10% Modulation NRZ-L Coding ISO/IEC 14443 TYPE B
From Active Device to Passive Device

Figure 6: Modulation and Coding Scheme [coskun12].

In [[coskun12], the RF interface supports communication with data rates of 106, 212 as well as 424 kbps as of today. As mentioned in [nfc15a], NFC uses different modulation schemes such as ASK (Amplitude Shift Keying) with different modulation depth 100 or 10% or load modulation and coding techniques such as NRZ-L (Non-Return-to-Zero Level), Manchester and Modified Miller coding to transfer data. In each NFC transaction, the NFC communication mode of an initiator or target NFC devices (active or passive), the signaling and standards used in RF interface (NFCIP-1, ISO/IEC 14443, JIS X 6319 Type F as FeliCa), and the data transfer rate is important in defining the modulation and coding scheme that is used. The study in [nfc15a] and [vedat13] show the summary of techniques used in NFC transaction depending on the direction of the communication. ISO/IEC 18092 (NFCIP-1) is the combination of ISO/IEC 14443 Type A and JIS X 6319 Type F. Beside that, in [vedat13]deals with the increase of data rates for proximity coupling devices at 13.56MHz and NFC systems, and compares performance of ASK and PSK modulation schemes in a real environment. It shows that PSK performs 23% better in terms of field strength requirement and energy efficiency than ASK (Fig. 6). There are three main operating modes for NFC (figure 7):

- Card emulation mode (passive mode): the NFC device behaves like an existing contactless card conforming to one of the legacy standards.
- Peer-to-peer mode: two NFC devices exchange information. The initiator device (polling device) requires less power compared to the reader/writer mode because the target (listener) uses its own power supply.
- Reader/writer mode (active mode): the NFC device is active and reads or writes to a passive legacy RFID tag.

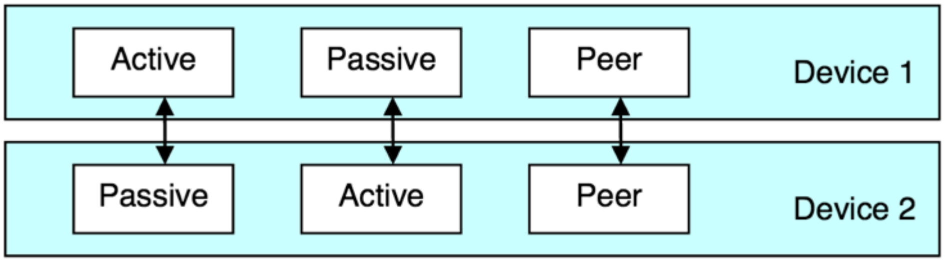


Figure 7: NFC operational modes [coskun12].

2.5 HomePlug GP

The HomePlug Green PHY protocol is chosen for study based on its low power use, its compatibility with existing infrastructure, and its robust error-handling procedures [hpp12]. It is a profile of IEEE 1901-2010 standard for Powerline Networks and is compatible with HomePlug AV and HomePlug AV2. However, it is maintaining compatibility with other HomePlug versions and providing error-handling and error-checking information contributes significant overhead to messages. Considering a network comprised of only HomePlug GP stations, this protocol uses 4 bytes of header information and 4 bytes of Cyclic Redundancy Check (CRC) per 512 or 128 bytes of data. The size of the physical block (PB) depends on the modulation used: for example, the Beacon message is always sent using Mini-ROBO modulation, which is the most reliable and has the lowest data rate (3.8 Mbps), and uses PBs of 136 bytes; the other messages are transmitted using either Standard ROBO (STD-ROBO) or High Speed ROBO (HS-ROBO) modulations, which are less reliable than Mini ROBO and have data rates of 4.9 Mbps and 9.8 Mbps respectively, and use PBs of 520 bytes [hpp05].

The HomePlug GP can chain up to three PBs per message with an additional 128 bits of frame control header. If messages contain less than 128 or 512 bytes of data, the rest of the PB is filled with padding creating wasted space, which will negatively impact the delay performance. Compare this to the Controller Area Network (CAN), which is a commonly used in-vehicle communication protocol standard and uses up to only 8 bytes of data per message [latchman15], and it is clear that for an in-vehicle network there would be much wasted space in using HomePlug GP messages. In order to ensure timely and fair competition for the medium, bus arbitration is accomplished by utilizing a Carrier Sense Multiple Access (CSMA) approach where stations gain access to the channel based on a 4-level priority value (2 bits), followed by a random backoff counter value. Once this backoff counter reaches zero, the station will send its message. This can easily lead to collisions if multiple stations choose the same backoff counter value, which starts off with a range of only 0 to 7. If a PB is received with errors, the entire 136 or 520 bytes PB must be re-sent by the transmitting station. This leads to significant delays if errors or collisions occur [latchman15].

HomePlug GP devices will be restricted to a 10 Mbps peak PHY rate. Given that the required MAC throughput for Smart Grid applications is 250 kbps, this is more than adequate. However, from the perspective of a heterogeneous network comprised of both HomePlug AV devices capable of supporting video distribution as well as HomePlug GP devices supporting Smart Grid applications, 10 Mbps is relatively slow. A 1500 byte Ethernet packet requires a much longer transmission time at 10 Mbps than it does at 200 Mbps. If the slower HomePlug GP devices operating in the presence of heavy HomePlug AV voice or video traffic were able to access the medium in an unconstrained manner, it is possible that HomePlug AV throughput could be adversely affected [hpp05]. Distributed Bandwidth Control (DBC) was included as a mandatory element of the HomePlug GP specification in order to ensure that HomePlug GP devices would not adversely impact existing HomePlug AV services, but still have access to the network [hpp04].

2.6 Wi-Fi

The IEEE 802.11 standard, extends the 802 Network Standards to the wireless medium by specifying the operation of Wireless Local Area Network (WLAN) communication within the ISM radio bands. First version was published in 1997. The Physical (PHY) and Media Access Control (MAC) network layers are defined by 802.11. The IEEE 802.11b/g standards use the 2.4Ghz frequency band, whereas 802.11a uses the 5Ghz band, and 802.11n uses a Multiple Input Multiple Output (MIMO) mechanism to utilize both the 2.4Ghz and 5Ghz bands. The 802.11 wireless LAN standard operates in two modes, ad-hoc mode (peer-to-peer) or infrastructure mode (peer-to-AP) [jun11].

In an infrastructure setup, wireless stations (STAs) connect to, or associate with an Access Point (AP). This grouping of devices (STA(s) + AP) is called a Basic Service Set (BSS) where each STA can connect to an outside network (the Internet) via its associated AP [eckehart13]. A BSS uses a Service Set ID (SSID) to identify itself. Multiple APs can be connected via a wired Distribution System (DS) where different BSSs are referred to as an Extended Service Set (ESS). In a scenario where BSSs use different SSIDs, a STA may change association however it must change its association to a different AP which causes a temporary loss of connection. A Basic Service Set ID (BSSID) is the Media Access Control(MAC) address of an AP, this allows a STA to identify a unique BSS AP in an ESS. This research is carried out on a n infrastructure WLAN within one BSS, this is illustrated in Figure 8.

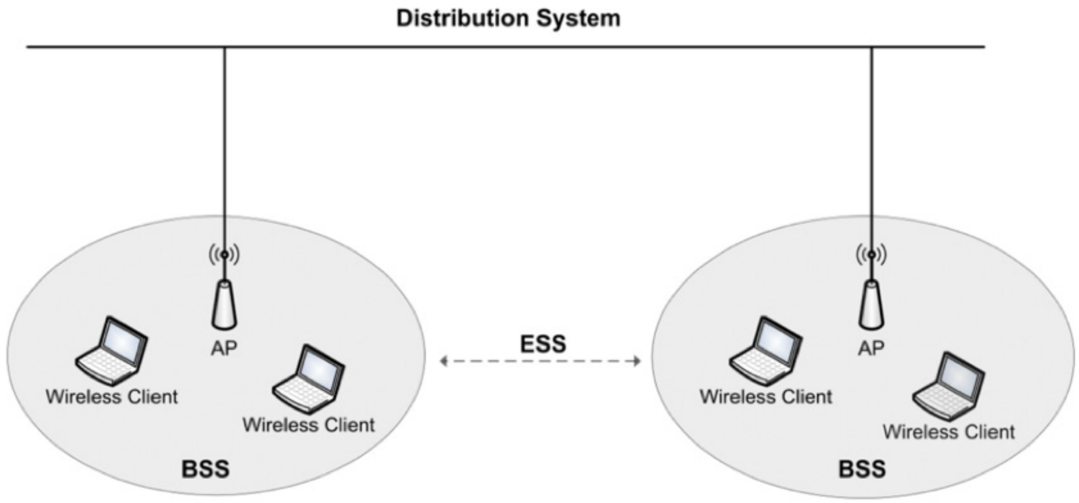


Figure 8 : Infrastructure WLAN [weight15].

In order to associate with an AP, a STA must go through a three-phase setup process as illustrated in Figure 9. These phases are the scan, authentication, and association phases. On waking or power on, a STA must discover nearby APs by using a passive or an active scan. A passive scan involves listening on each channel for broadcast beacons sent from APs. In an active scan, the STA 'actively' sends out a broadcast probe request frame one ach channel and then waits for a response from an AP on that channel [weight15].

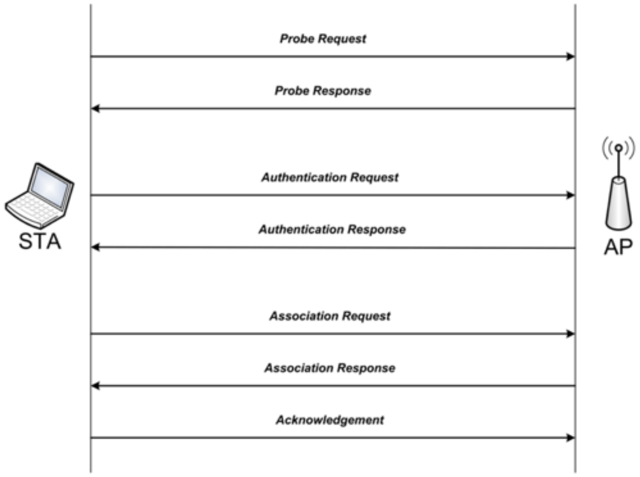


Figure 9 : Request-Response Process [weight14].

After APs are discovered and one AP is selected, the STA starts the authentication process to authenticate itself with the AP. The STA first sends out an authentication frame, to which the chosen AP responds with additional authentication frames. The authentication phase controls what nodes can access the AP. It is a network access control mechanism. After successful authentication, the STA moves to associate with the AP by sending an association/reassociation request frame to which the AP responds with an association/re-association response frame. Finally, the STA sends an acknowledgement (ACK) frame to the AP. Once the AP receives this ACK frame, the STA is associated with the AP and a valid connection is established between the STA and the AP. The infrastructure topology is sometime called an AP topology since the wireless network consists of at least an AP and a set of wireless devices. In this topology, the system is divided into basic cells, where each cell is controlled by an AP. To extend the coverage area, multiple basic cells can be used as shown in Figure 10.

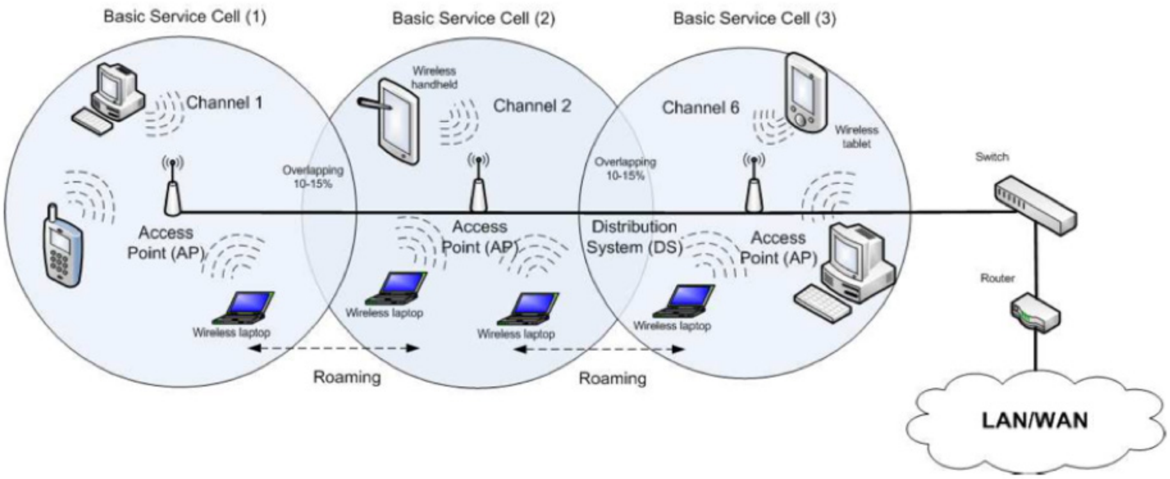
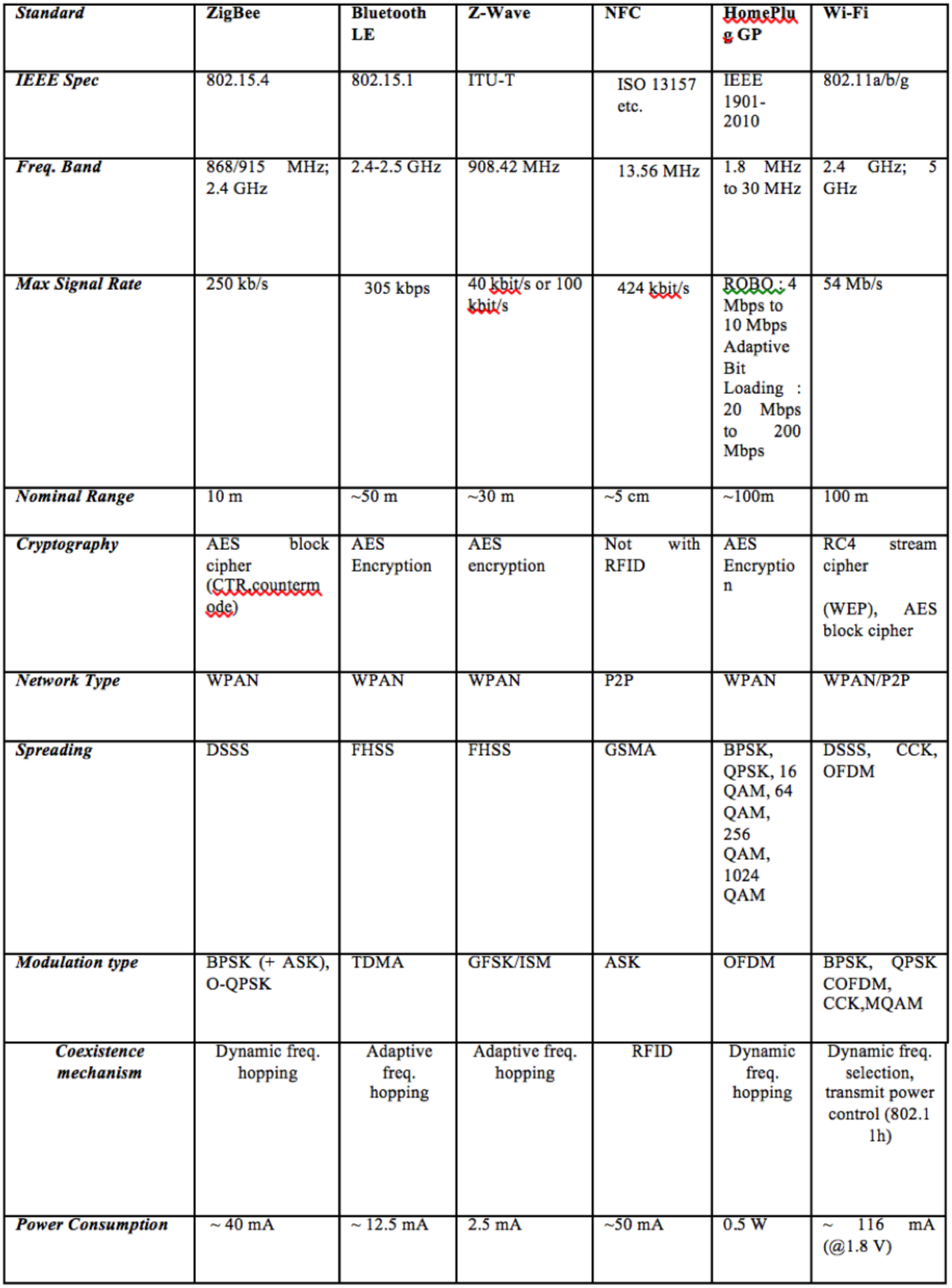


Figure 10 : A typical WLAN [altolin10].

3.0 Comparative Study

Table 1 summarizes the main differences among the six protocols. Each protocol is based on an IEEE standard except Z-Wave. Obviously, Wi-Fi, HomePlug GP and Bluetooth LE provide a higher data rate, while ZigBee and Z-Wave give a lower one. In general, the ZigBee, Bluetooth LE and NFC are intended for WPAN communication (about 20 m), while Wi-Fi is oriented to WLAN (about 100 m). However, ZigBee can also reach 100 m in some applications.

Table 1: Comparison of the ZigBee, Bluetooth LE, Z-Wave, HomePlug GP and Wi-Fi.



Standard	**ZigBee**	**Bluetooth LE**	**Z-Wave**	**NFC**	**HomePlug GP**	**Wi-Fi**
IEEE Spec	802.15.4	802.15.1	ITU-T	ISO 13157 etc.	IEEE 1901-2010	802.11a/b/g
Freq. Band	868/915 MHz; 2.4 GHz	2.4-2.5 GHz	908.42 MHz	13.56 MHz	1.8 MHz to 30 MHz	2.4 GHz; 5 GHz
Max Signal Rate	250 kb/s	305 kbps	40 kbit/s or 100 kbit/s	424 kbit/s	ROBO : 4 Mbps to 10 Mbps Adaptive Bit Loading : 20 Mbps to 200 Mbps	54 Mb/s
Nominal Range	10 m	~50 m	~30 m	~5 cm	~100m	100 m
Cryptography	AES block cipher (CTR,countermode)	AES Encryption	AES encryption	Not with RFID	AES Encryption	RC4 stream cipher (WEP), AES block cipher
Network Type	WPAN	WPAN	WPAN	P2P	WPAN	WPAN/P2P
Spreading	DSSS	FHSS	FHSS	GSMA	BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM, 1024 QAM	DSSS, CCK, OFDM
Modulation type	BPSK (+ ASK), O-QPSK	TDMA	GFSK/ISM	ASK	OFDM	BPSK, QPSK COFDM, CCK,MQAM
Coexistence mechanism	Dynamic freq. hopping	Adaptive freq. hopping	Adaptive freq. hopping	RFID	Dynamic freq. hopping	Dynamic freq. selection, transmit power control (802.11h)
Power Consumption	~ 40 mA	~ 12.5 mA	2.5 mA	~50 mA	0.5 W	~ 116 mA (@1.8 V)

Comparison of the ZigBee, Bluetooth LE, Z-Wave, HomePlug GP and Wi-Fi

ZigBee, Bluetooth LE, and Wi-Fi protocols have spread spectrum techniques in the 2.4 GHz band, which is unlicensed in most countries and known as the industrial, scientific, and medical (ISM) band. Bluetooth LE and Z-Wave use frequency hopping (FHSS) with 79 channels and 1 MHz bandwidth, while ZigBee uses direct sequence spread spectrum (DSSS) with16 channels and 2 MHz bandwidth. Wi-Fi uses DSSS (802.11), complementary code keying (CCK, 802.1lb), or OFDM modulation (802.11a/g) with 14 RF channels (11 available in US, 13 in Europe, and just 1 in Japan) and 22 MHz bandwidth [sikora05].

3.2 Coexistance

Since Bluetooth LE, ZigBee and Wi-Fi use the 2.4 GHz band, the coexistence issue must be dealt with. Basically, Bluetooth and UWB provide adaptive frequency hopping to avoid channel collision, while ZigBee and Wi-Fi use dynamic frequency selection and transmission power control. IEEE 802.15.2 discussed the interference problem of Bluetooth and Wi-Fi. In [sikora05] provided quantitative measurements of the coexistence issue for ZigBee, Bluetooth, Wi-Fi, and microwave ovens. Other work in [Shuaaib06] focused on quantifying potential interferences between ZigBee and IEEE 802.1lg by examining the impact on the throughput performance of IEEE 802.1lg and ZigBee devices when coexisting within a particular environment. Moreover, Neelakanta and Dighe [neela03] presented a performance evaluation of Bluetooth and ZigBee on an industrial floor for robust factory wireless communications.

3.3 Security

In term of security, all the six protocols have the encryption and authentication mechanisms. ZigBee, Bluetooth LE, NFC, Z-Wave and HomePlug GP use the advanced encryption standard (AES) block cipher with counter mode (CTR) and cipher block chaining message authentication code (CBC-MAC), also known as CTR with CBC-MAC (CCM), with 32-bit and 16-bit CRC, while Bluetooth LE adopt the EO stream cipher and shared secret with 16-bit cyclic redundancy check (CRC). In 802.11, Wi-Fi uses the RC4 stream cipher for encryption and the CRC-32 checksum for integrity. However, several serious weaknesses were identified by cryptanalysts, any wired equivalent privacy (WEP) key can be cracked with readily available software in two minutes or less, and thus WEP was superseded by Wi-Fi protected access 2 (WPA2), i.e. IEEE 802.1 li standard, of which the AES block cipher and CCM are also employed.

3.4 Power Consumption

ZigBee and Bluetooth LE, Z-Wave and NFC are designed for portable devices and limited battery power. Thus, it offers low power consumption and consequently affect battery lifetime. On the other hand, HomePlug GP and Wi-Fi are intended for a longer connection and supports devices with a substantial power supply. ZigBee and RF4CE are virtually the same technology and appear positively power hungry compared with the other radio technologies.Bluetooth LE is the closest competitor and will be competing in the same markets and many others, offering mobile handset manufacturers a route to a larger ecosystem. It also provides the best power per bit requirements of the personal space technologies, beaten only by Wi-Fi. NFC is not seen as a competitor to most low-power wireless technologies, because it brings new use cases to the mobile scene. It is a short range (~5 cm) radio which is ideally suited to "Touch to Action" applications. Wi-Fi is normally intended for bulk traffic transfer at high speed. Work is in progress to enable special Wi-Fi chips to operate in HID equipment. However, currently available chipsets for HID over Wi-Fi are proprietary and require a special driver to be installed on Microsoft WindowsTM 7 PCs. In addition, such systems are likely to consume significant power at the PC end of the link to minimize latency. Obviously, the ZigBee, Bluetooth LE, Z Wave and NFC protocols consume less power as compared with HomePlug GP and Wi-Fi. However, Wi-Fi have better efficiency in energy consumption.

4.0 Summary

This paper gives a broad overview of the six most known IoT data link protocols, with a comparison in terms of specification, frequency band, maximum signal rate, nominal range, cryptography, network type, spreading, and coexistence mechanism. Some of these characteristics, such as frequency band and maximum signal, signal rate, spreading and coexistence mechanism, are stable and well defined by the standards. Others, such as power consumption and security, are open challenges, where the technology is continuously improving, as far as both the standards and their implementations are concerned. This paper is not to draw any conclusion regarding which one is superior since the suitability of network protocols is greatly influenced by practical applications, of which many other factors such as the network reliability, roaming capability, recovery mechanism, chipset price, and installation cost need to be considered in the future.

References

1. [li14] H. Li, Z. Weishi, and Z. Weifu, "A Novel Vulnerability Detection Method for ZigBee MAC Layer," in IEEE 12th International Conference on Dependable, Autonomic and Secure Computing, 2014. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6945675. The paper describes a detection method of ZigBee in MAC Layer.
2. [shyan13]] L. J. Shyan, S. Y. Wei, and S. C. Chou, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), 2013 pp 5-8. http://www.seekdl.org/nm.php?id=1364. The paper compares some wireless protocols and do some performance evaluation.
3. [zhou11] Z. Zhou, Kista, W. Zhiqang, W. Fan, and W. Yuexin, "A middleware of Internet of Things (IoT) based on Zigbee and RFID," in IET International Conference on Communication Technology and Application (ICCTA), 2011, pp. 34-41. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6192962. The paper describes a middleware of Internet of Things (IoT) based on Zigbee and RFID.
4. [xiolin10] Y. Xiolin, J. Zhiqang, Z. Wenjun, and W. Zhingning, "The Research and Implementation of ZigBee Protocol-Based Internet of Things Embedded System," in International Symposium on Information Engineering and Electronic Commerce (IEEC),

2010, pp. 7-10. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5533200. The paper describes a ZigBee protocol based on IoT.

5. [kuor11] C. H. Kuor, "Bluetooth : A Viable Solution for IoT?," in IEEE Wireless Communications, vol. 21, no. 6, 2011, pp. 6-7. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7000963. The paper describes a Bluetooth.
6. [chris15] J. H. Christophher, "Internetworking with Bluetooth Low Energy," in Mobile Computing and Communications," 2015 pp 34-38. http://dl.acm.org/citation.cfm?id=2817774. The paper describes a Bluetooth LE.
7. [nieman14] . Niemen, C. Gomez, M. Isomaki, and T. Savolainen, "Networking Solutions for Connecting Bluetooth Low Energy Enabled Machines to the Internet of Things," in IEEE Network, vol. 5, no. 4, 2014 pp. 83-90. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6963809. The paper describes a Bluetooth LE based on IoT.
8. [hansen15] C. J. Hansen, "Internetworking with Bluetooth Low Energy," in Mobile Computing and Communications, vol. 19, no. 2, 2015, pp. 34-38. http://dl.acm.org/citation.cfm?id=2817774. The paper describes a Bluetooth LE and its explain its specification.
9. [zwave15] Z-Wave "Understanding Z-Wave Networks, Nodes & Devices" http://www.vesternet.com/resources/technology-indepth/understanding-z-wave-networks, 2015. The online article explain about Z-Wave.
10. [amaro11] P. Amaro, R. Corteso, R. Landeck, and J. Santos, "Implementing an Advanced Meter Reading infrastructure using a Z-Wave Compliant Wireless Sensor Network," in Proceedings of the 3rd International Youth Conference on Energetics, 2011. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6028316. The paper describes an implementation of Advances Meter Reading using a ZWave.
11. [zhengguo14] C. S. Zhengguo, Z. Chunseng, and C. M. Victor "Surfing the Internet-of-Things: Lightweight Access and Control of Wireless Sensor Networks Using Industrial Low Power Protocols," in EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, vol. 1, no. 1, 2014. http://www.researchgate.net/publication/271725260_Surfing_the_Internet-of-Things_Lightweight_Access_and_Control_ofWireless_Sensor_Networks_Using_Industrial_Low_Power_Protocols. The paper describes a Lightweight WSN.
12. [baldo10] D. Baldo, G. Beneelli, and A. Pozzebon, "The Siesta Project : Near Field Communication," in Proceedings of 7th International Symposium on Communication Systems Networks and Digital Signal Processing, 2010, pp. 721-725. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5580332. The paper describes a NFC and how it operates.
13. [coskun12] V. Coskun, K. Ozdinici, Near Field Communicatioin (NFC), Wiley, 2012. http://www.wiley.com/WileyCDA/WileyTitle/productCd-1119971098.html. This book describes everything about NFC.
14. [urien13] P. Urien, "LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things," in IEEE Consumer Communications and Networking Conference (CCNC), 2013, pp. 845-854. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6488560.

15. [nfc15a] Analogue Specification Draft, Technical Specification, NFC Forum, 2015. http://certification.nfc-forum.org/docs/NFC_Forum_Device_Requirements.pdf. The technical report describes a NFC.
16. [nfc15b] Analogue Specification Draft, Technical Specification, NFC Forum, 2015. http://link.springer.com/article/10.1007%2Fs11277-012-0935-5#/page-1. The paper surveys an NFC implementation.
17. [vedat13]] C. Vedat, O. Busra, and K. Karim, A Survey on Near Field Communication (NFC) Technology. Springler, 2013.
18. [hpp12] HomePlug Powerline Alliance, HomePlug Green PHY 1.1, the standard for in-house smart grid powerline communications: an application and technology overview White paper, October 2012, 17p. http://www.homeplug.org/media/filer_public/92/3f/923f0eb3-3d17-4b10-ac75-03c3c2855879/homeplug_green_phy_whitepaper_121003.pdf. The white paper describes a HomePlug Green PHY 1.1.
19. [latchman13] H. Latchman, S. Katar, L. Yonge, and A. Amarsingh, "High speed multimedia and smart energy PLC applications based on adaptions of HomePlug AV," in Proc. 17th Int. Symp. on Power-Line Communications and its Applications, Johannesburg, South Africa, March 2013, pp. 143-148. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6525840. The paper describes a High speed multimedia and smart energy PLC applications based on adaptions of HomePlug AV.
20. [hpp05] HomePlug Powerline Alliance, HomePlug AV White paper, 2005, 11p. http://www.homeplug.org/media/filer_public/b8/68/b86828d9-7e8a-486f-aa82-179e6e95cab5/hpav-white-paper_050818.pdf. The white paper explains a HomePlug Powerline Alliance, HomePlug AV.
21. [hpp04] HomePlug Powerline Alliance, HomePlug 1.0 Technical white paper, September 2004, 13p. http://www.solwise.co.uk/downloads/files/hp_1.0_technicalwhitepaper_final.pdf. The white paper explains a HomePlug Powerline Alliance, HomePlug 1.0.
22. [antionali15] R.P. Antonioli, M. Roff, S. Zhengquo, and L. Jia, "A Real-Time MAC Protocol for In-Vehicle Power Line Communications Based on HomePlug GP", in IEEE 81st, Vehicular Technology Conference (VTC Spring), 2015. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7145642. The paper describes a Real-Time MAC Protocol for In-Vehicle Power Line Communications Based on HomePlug GP.
23. [jun11] H. Jun, Qingdao, M. Zheng, S. Chungseng, "Energy-efficient MAC Protocol Designed for Wireless Sensor Network for IoT," in Seventh International Conference on Computational Intelligence and Security (CIS), 2011. http://www.eecs.harvard.edu/~mdw/course/cs263/papers/smac-infocom02.pdf. The paper describes a Energy-efficient MAC Protocol Designed for Wireless Sensor Network for IoT.
24. [eckehard13] S. Eckehard, K. Matthias, A.N. Anas, D. Stefan, A. Moller, R. Luis, S. Florian, "Advances in Media Technology Internet of Things," technical report, Technische Universitat Munchen Institute for Media Technology, 2013. http://www.eislab.fim.uni-passau.de/files/publications/hsmt/HSMT-Proceedings_WS201213.pdf. The report describes media technology in IoT.

25. [weight15] IoT "New Weightless 2-Way Communication IoT Standard launches" http://www.weightless.org/news/new-weightless-2way-communication-iot-standard-launches, 2015. The paper describes a new weightless 2-Way communication in IoT.
26. [sikora05] A. Sikora and V. F. Groza, "Coexistance of IEEE 802.15.4 with other systems in the 2.4 Ghz-ISM-Band,' in Proc. IEEE Instrumentation & Measurement Technology Conference, May 2005, pp. 1786-1791. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1604479. The paper describes coexistence of IEEE 802.15.4 with other systems in the 2.4 Ghz-ISM-Band.
27. [shuaib06] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, "Coexistance of ZigBee and WLAN: A performance study," in Proc. IEEE Int. Conf. Wireless & Optical Communication Network, April 2006. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4135336. The paper describes Coexistance of ZigBee and WLAN and conducted some performance study.
28. [neela03] P. S. Neelakanta and H. Dighe, "Robust Factory Wireless Communication: A performance appraisal of the Bluetooth and the ZigBee collocated on an industrial floor," in Proc. IEEE Int. Conf. ind. Electron. (IECON'03), November 2003, pp. 2831-2386. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1280617. The paper describes a performance appraisal of the Bluetooth and the ZigBee collocated on an industrial floor.

List of Acronyms

- AES - Advanced Encryption System
- AP - Access Point
- ASK - Amplitude Shift Keying
- BSS - Basic Service Set
- CAN - Controller Area Network
- CCK - Complementary Code Keying
- CO - Coded
- CRC - Cyclic Redundancy Check
- DBC - Distributed Bandwidth Control
- DS - Distribution System
- DSSS - Direct Sequence Spread Spectrum
- DVD - Digital Video Decoder
- FHSS - Frequency Hoping Sequence Spread Spectrum
- Ghz - Gigahertz
- GP - Green PHY
- GFSK - Gaussian Frequency SK
- BPSK/QPSK - Binary/Quadrature phase SK
- HID - High Intensity Discharge
- IEEE - Internet Engineering Task Force
- IPv6 - Internet Protocol Version 6
- IoT - Internet of Things
- ISM - Industrial, Scientific and Medical/li>
- kbps - Kilobit per second
- LE - Low Energy
- mA - milliamps

- MAC - Media Access Control
- MIMO - Multiple Input Multiple Output
- NFC - Near Field Communication
- OFDM - Orthogonal Frequency Division Multiplexing
- RFID - Radio Frequency Identification
- RF4CE - Radio Frequency for Consumer Electronics
- QPSK - Quadrature Phase Shift Keying
- SSID - Set ID
- STAs - Wireless Stations
- TV - Television
- TDMA - Time Division Multiple Access
- V - Volt
- VCR - Video Cassette Recorder
- WEP - Wired Equivalent Privacy
- WLAN - Wireless Local Area Network
- WPA - Wi-Fi Protected Access
- Wi-Fi - Wireless Fidelity

Last modified on November 30, 2015
This and other papers on recent advances in networking are available online at
http://www.cse.wustl.edu/~jain/cse570-15/index.html
Back to Raj Jain's Home Page