

Comparative analysis of communication standards for Smart City deployment

Đorđe Lukić*, Dejan Drajić*

* School of Electrical Engineering University of Belgrade, Belgrade, Serbia
djordje.lukic92@gmail.com, ddrajić@etf.rs

Abstract — In this paper we discuss the communication standards for Internet of Things applications, with focus on Smart City deployment. Different communication technologies can be used for applications based on the types of devices in the smart environment and their available resources and limitations. A selection criteria for appropriate communication standard also depends on the specific smart environment application. Promising technologies for both indoor and outdoor smart environments are considered. Communication standards comparison is made by considering the various parameters such as throughput, operating frequency bands, nominal range and energy efficiency. Additionally, it was analyzed which standard is the most suitable for appropriate Smart City application.

Keywords — communication standards, comparative analysis, Internet of Things, Smart City.

I. INTRODUCTION

Internet of Things (IoT) has been defined from different perspectives and hence numerous definitions for IoT exist in the literature. The reason for this stems from the fact that it is syntactically composed of two terms – Internet and things. The first term pushes towards a network oriented vision of IoT, while the second tends to move the focus on things (objects). When these terms are put together, IoT semantically means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols. Unique identification of objects and the representation of exchanged information is important issue. This brings the third perspective of IoT – semantic perspective. The routing is based upon the information itself, so as to find sources which can deliver the requested content without having an a priori location for the content. The main concepts of these three visions of IoT are presented in [1]. Semantic oriented IoT visions have been already proposed in many research papers such as [2]. Also, according to IP for Smart Objects (IPSO) alliance, the IP stack is a light-weight protocol that already connects a large number of devices and has all the qualities to make IoT a reality.

The investigation in this paper is based on the IoT perspective of things. The focus is on how to integrate the IoT objects into a common framework using current communication standards. The purpose of the IoT communication technologies is to connect heterogeneous objects together to deliver specific smart service. The network oriented perspective is briefly mentioned just to describe incorporation of communication protocol used by proposed technology into the IP architecture.

Standardization is the most important prerequisite for global deployment of the specific technology. The use of standardized information technology has various benefits to companies, individuals and users. The main motivation of this work is to identify implementation challenges for using different communication standards for IoT applications and to propose the most promising technologies for the standardization of specific Smart City applications. Without a comparative understanding of the standards it is quite difficult both to choose the most appropriate communication technology and then to design it into an application.

In this paper the comparative analysis of communication standards for Smart City deployment is made. The wireless standards such as IEEE 802.11ah WiFi, Bluetooth low energy and IEEE 802.15.4 ZigBee PRO for both indoor and outdoor smart environments are considered. The comparison is based on technology specific parameters including range, topology, security, data throughput, latency, robustness to interference and power consumption. The main goal of this paper is to analyze and present potential technologies which can be applied in IoT applications and propose possible directions for standardization. So far many authors proposed the proprietary solutions, while defining the unique solution for specific IoT application should enable global deployment of IoT and Machine to Machine (M2M) communications.

The rest of the paper is organized as follows. In section II, the wireless technology specific parameters which are relevant for further analysis are defined. Section III contains an exposure of method for communication standards comparison. The main part of this paper is explained in section IV, where the results of comparative analysis are presented and the appropriate communication technology for the specific Smart City application is proposed. Based on obtained results, conclusions are pointed out in section V.

II. WIRELESS STANDARD PARAMETERS

Parameters of wireless connectivity are mutually dependent, so it is important to consider all of them when making a choice of wireless standard. Every application has different requirements, but it is essential for the overall analysis to go through the main technology specific parameters.

A. Range

Range is invariably the first parameter which is considered when choosing a wireless standard. The theoretical range given in product specifications has

always bigger value than in reality, because as soon as a radio is brought inside a building, fading, interference and reflections will reduce the range significantly [3]. Range is closely tied up with throughput and output power. Wireless performance degrades as the distance between transmitter and receiver increases. It is not a linear decrease. Generally, the connection maintains a link that supports a data rate close to the maximum the transmitter and receiver can support, until it reaches a point when it starts to decrease. There is no strict definition of where range stops. In most cases it is considered as the point where throughput falls by 5-10%.

What underlies the decrease in throughput is the fact that data start to get lost in the background noise. As transmitter and receiver move further apart, the strength of signal arriving at the receiver gets smaller, until it becomes impossible to detect the signal from the background noise. Radio signal interference also results in corruption of individual bits within the data stream.

B. Throughput

Throughput is the rate of successful data delivery over a communication channel. It fails as the range increases and the Bit Error Rate (BER) rises. To get the highest throughput, wireless standards attempt to cram more than one bit of information into each bit transmitted. Bluetooth and WiFi maximize throughput by trying to select the most complex coding scheme that the link quality will support. As the link quality declines, they will automatically step down to a less aggressive coding scheme until they achieve a reliable link [4]. It is fairly obvious that the more data crammed into each bit, the more susceptible it will be to noise, so the highest data rates will typically have the lowest range. The important thing regarding range and throughput is to choose wireless standard that works well within the envelope of performance required for specific application.

C. Interference

If two radios within range of each other both transmit at the same time and at the same frequency, this results in signals arriving at the respective receivers that interfere and are likely to be corrupted. Radios using reliable data links will not get an acknowledgement of reception and so they will attempt to retransmit the data. Different radio standards use different techniques to try and ensure that they don't clash with each other on the retransmission, but even if the next transmissions do not overlap and are successful, it means that the throughput will be decreased as a result of retransmission. In a situation where this starts to occur, it will probably happen repeatedly.

Each standard defines a spectral mask for its transmission, which is a set of limits on the output power within and around each transmit channel [3]. These are defined to meet the requirements of global regulatory regimes as well as the practical performance of low-cost radios. In an ideal world, a radio's transmissions would reduce to zero outside the extent of its channel. Real radio implementations are not that perfect, they provide a peak output at the centre of the channel, and the power then falls off gradually at either side. As well as the issue of not interfering with a radio on an adjacent channel, there is generally a tighter requirement at the two ends of the band, where spectrum is allocated for other applications. To help protect them from each other, most standards

incorporate guard bands at either end of allowed spectrum, which, although they lie within the allowed license free band, are set aside to ensure that transmissions do not extend beyond the band edge.

D. Topology

The manner in which the connections are allowed between devices is called the network topology. The first, most straightforward and still most widely used is simple cable replacement, which is also what that particular topology is called. All of the wireless standards can perform it, differing predominantly in their speed of throughput.

Next comes point-to-multipoint topology or the piconet, where one device acts as a master or central device, connecting to several other devices. This is also known as a star network. Different standards allow differing numbers of concurrent live connections in a piconet. The maximum number of connections is determined by the size of the local address field within each standard [4]. Although topologically identical, client server topology is considered as a distinct form of piconet or star-network topology, as it implies a central unit that acts as an access point to provide connectivity to another network. A limitation of the piconet is that a slave is a slave. It can only communicate with its master device. If slave nodes are given the ability to talk directly to each other, the topology develops into a cluster network. Cluster networks have the advantage that some of the workload can be removed from the master, as transactions no longer need to pass through it. However, the master needs to set up the routing tables in the cluster nodes in the first place, which generally increases its complexity.

The next level of complexity comes with the scatternet topology. This is an extension of a piconet, but allows a slave or peripheral device to be simultaneously connected to two or potentially more networks [3]. It has the limitation that although a device may be part of multiple networks, that device generally only functions within one at a time, it is not able to act as a bridge between the two networks. That is the reason for deployment of tree or hierarchical network. The difference is that the backbone nodes of a tree network have routing capabilities, whereas the connecting nodes in a scatternet may only share data. This means that any node connected to the backbone can send data to any other node within the tree.

At the top end of complexity is the mesh network, where individual nodes may be able to talk directly to each other if they are within wireless range, or through a selection of alternative routes. Whereas the tree network uses a single backbone for all inter-cluster routing, mesh networks allow multiple routes throughout the network. This adds redundancy to the network, allowing traffic to be maintained even if some of the nodes or links between nodes fail.

E. Security

Devices connecting through a wireless link need to be sure that they have connected to the correct device. As anyone with a suitable receiver can listen in to the wireless conversation, they also need to encrypt their data, so that an eavesdropper who intercepts it cannot decode it. These two processes are known as authentication and encryption. Each of the wireless standards has a credible approach to security.

F. Power consumption

Many wireless products are designed to be mobile, which implies that they will run on batteries. Because of that, minimizing the power consumption of the wireless link is critical.

A low-power radio enables data to be sent efficiently over the air. It includes power management schemes to ensure that the radio can remain in deep sleep mode whenever possible. Power consumption goes down as the range and throughput decreases. There's a complex relationship between coding schemes and energy efficiency. As more bits are put into each packet, the processing requirements increase, but so does the BER for the link, so although a higher coding rate may be technically more efficient, as it requires fewer packets, this may be offset by the need for a higher transmit power to get a reliable transmission [3].

Most low-power applications are centred around sensors, which only need to communicate their state intermittently. Rather than looking at the energy per bit of transmitted information, the battery life depends on the duty cycle and how quickly radio can move from its sleep state to perform a wireless transaction and then return to sleep. For many radios the current consumption in receive mode is greater than it is in transmit mode. So if a transmission needs to be acknowledged, it is important that it is done as quickly as possible, so that the receiver does not sit around burning current. Also, there are times associated with the device waking up, stabilising and performing its measurement before it can transmit [4].

G. Latency

Wireless connection has finite delay between data being presented at the transmitting end and being received at the other. Latency, which is the measure of this delay, is different for each wireless standard. It is also implementation dependent and may vary for different hardware. Most of the IoT devices use data services instead of voice, so considered IoT applications are not delay sensitive. This technology specific parameter has important role in analysis of real-time IoT applications.

III. COMPARISON METHOD

Wireless standards have more in common than is generally realised. They have evolved from a few basic radio configurations, distinguishing themselves with protocol stack that adapt these radios to particular connection topologies. The focus in this comparison method is on commonalities, explaining where and why the communication standards differ and how these differences affect their use.

The features that are relevant for choosing a radio including range, topology, security, throughput, latency and power consumption are described in previous section. These are the core differences that should be considered as the first step in making a choice which wireless standard to choose for appropriate IoT application. After that comes the essential part of the analysis explaining how to move from a standard to a product and the way in which wireless standards can be used for applications.

This looks at the practical side of the wireless parameters that are mentioned, including topologies, methods for making connections and securing them, managing power consumption, transmitting different types

of data and coexisting with other radios. This approach is also based on the tools and techniques that are needed, along with a discussion of the system design and architecture necessary to embed wireless connectivity into a wide range of devices. Finally, the major opportunities for communication technologies including IEEE 802.11ah WiFi, Bluetooth low energy and IEEE 802.15.4 ZigBee PRO are highlighted, exploring the key IoT applications where it is expected to make its biggest impact.

IV. RESULTS

In this section, results obtained by described comparison method are presented. The aim was to compare wireless standards designed for IoT applications on physical layer. Technology specific parameters have been examined and their influence on wireless technology performances is analyzed.

IEEE 802.11ah is a new wireless networking protocol that operates in the sub-gigahertz license-exempt band (900 MHz), compared to conventional WiFi networks operating in 2.4 GHz and 5 GHz bands [5]. The consequence of using lower frequency band is the extended range. This standard enables single-hop communication over distances up to 1000 m. Relay Access Points are used to extend the connectivity to Access Points that are two-hops away [6]. Bluetooth low energy and ZigBee PRO standards usually operate in unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz band. The usage of higher frequency bands decreases the coverage range for these two technologies (maximum 100 m).

As more devices use unlicensed frequency bands, the specific communication technology have to deal with increased interference level. ZigBee PRO standard is using direct sequence spread spectrum (DSSS) technique which can accommodate data rates up to 250 Kbps. The DSSS technique works on the principle that much of the noise within a frequency band will come from narrowband transmissions. Rather than trying to avoid these, DSSS uses a spreading function to transform its signal across a wider frequency range within the spectrum. At the receiving end, the reverse transformation takes place in a correlator, reproducing the original signal. Any noise arriving at the receiver goes through the same reverse transformation, with the result that it is reduced from being of similar amplitude to the received signal, to an order of magnitude or more lower. Classic Bluetooth standard takes a different approach using frequency hopping (FH) technique. The radios jump from channel to channel in synchronization with each other 1600 times every second. The reasoning behind this is that if a Bluetooth radio encounters interference and packet is lost, then it will be repeated at a different frequency, where there is a good chance that there is no interference. Bluetooth low energy has implemented a modified frequency hopping scheme known as adaptive FH which enables data rates from 125 Kbps to 1 Mbps [7]. Adaptive FH works by scanning the spectrum, looking for channels which are being used. The radios then modify their hopping sequence to avoid these channels. IEEE 802.11ah standard is using orthogonal frequency division multiplexing (OFDM). OFDM is a method of digital signal modulation in which a single data stream is split across several separate narrowband channels at different carrier frequencies. This technique has high spectral

efficiency and ability to cope with narrowband co-channel interference and frequency-selective fading due to multipath propagation. Using OFDM with appropriate modulation and coding scheme, IEEE 802.11ah standard provides data rates from 650 Kbps to 78 Mbps. These techniques differ but they are all good in decreasing interference level in the communication system.

Although Bluetooth low energy and ZigBee PRO standards achieve much lower data rates than IEEE 802.11ah, that is enough for most of the IoT applications which are proposed to be implemented using these two standards. IEEE 802.11ah standard has tree network topology where an access point allows multiple clients to connect to a separate network. Bluetooth low energy has scatternet network topology which is inherited from the classic Bluetooth standard. ZigBee PRO standard has the most flexible network topology. That is mesh topology which provides redundancy and reliable wireless links. From the security point of view, the analyzed wireless standards have similar level of security so they are not competitive regarding to that criteria. The highest data rates provided by IEEE 802.11ah have as a consequence big power consumption comparing to other two standards and requires power suppliers. ZigBee PRO provides long battery lifetime due to low duty cycle so it is the most energy efficient wireless technology. Bluetooth low energy has improved power management algorithm comparing to the classic Bluetooth standard. This technology also achieves the lowest latency due to short distance between the devices. IEEE 802.11ah standard has improved latency comparing to the previous IEEE 802.11 standards. ZigBee PRO has the biggest latency which is approximately 100 ms per one hop, but this latency is not critical for the most IoT applications [8]. Table I gives a point-wise comparison for the analyzed standards.

After technology specific parameters comparison, the most appropriate Smart City IoT applications are proposed for each analyzed wireless standard. The most suitable IoT application which can be implemented by IEEE 802.11ah is one which requires long range and high number of IoT devices. The Relay Access Points can be spread all around the city and detect movement and dynamically turn on lights (Smart Street Lighting) or detect traffic jam and damaged roadways and dynamically propose re-routing for end users (Vehicle Traffic Monitoring and Smart Parking).

Bluetooth low energy standard is the appropriate for IoT applications where devices should be on short distance and constantly measure the physical parameters. Sensors can be put on human body and measure blood pressure and body temperature (Smart Healthcare) or they can measure speed and burned calories for runner (Sport and Fitness Applications). Using this technology, the customer with specific shopping profile in mall can be discovered and the advertisement can be sent to him according to his shopping profile (Smart Advertising).

ZigBee PRO offers full wireless mesh low-power networking capable of supporting more than 64000 devices on a single network. With mentioned properties, this standard is the most suitable for IoT applications which require periodical measurements of physical environment such as water or gas metering (Smart Metering). Sensors can measure humidity of the ground in city parks or air pollution and make actions due to environmental changes (Environment monitoring). They

can be put in bins and detect when rubbish reach certain level (Waste Management). Wireless sensor networks using ZigBee technology can be spread around the city and measure noise level in some part of the day and make urban noise maps which are quite popular nowadays.

TABLE I: TECHNOLOGY SPECIFIC PARAMETERS

Parameter	WiFi 802.11ah	Bluetooth low energy	ZigBee PRO
Frequency range	900 MHz	2.4 GHz	900 MHz, 2.4 GHz
Coverage	1 km	100 m	10-100 m
Throughput	0.65-78 Mbps	0.125-1 Mbps	20-250 Kbps
Interference robustness	OFDM	adaptive FH	DSSS
Topology	tree	scatternet	mesh
Security	WPA2	128 bit AES	128 bit AES
Power consumption	1 mW-1 W	0.01-0.5 W	1-100 mW
Latency	47 ms	6 ms	108 ms

V. CONCLUSION

This paper shows the results of communication standards comparative analysis for Smart City applications. The IEEE 802.11ah WiFi, Bluetooth low energy and IEEE 802.15.4 ZigBee PRO standards are considered in the analysis. The technology specific parameters on physical layer are compared and it was determined which wireless standard can be applied for the specific IoT application deployment. Improvements of IEEE 802.11ah standard in terms of throughput, delay performance and network coverage range makes this standard ideal for large areas with high number of IoT devices. High energy efficiency and mesh network topology defines IEEE 802.15.4 ZigBee PRO standard as the primary solution for IoT applications which require environment monitoring. With low latency for exchanging data, Bluetooth low energy became promising technology for short range real-time IoT applications.

REFERENCES

- [1] D. Bandyopadhyay, and J. Sen, "Internet of Things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, pp. 49–69, May 2011.
- [2] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro, "Named data networking for IoT," *2014 European Conference on Networks and Communications (EuCNC)*, vol. 1, pp. 1-5, June 2014.
- [3] N. Hunn, "Essentials of Short-Range Wireless," 1st ed. New York: Cambridge University Press, 2010.
- [4] C. X. Mavromoustakis, G. Mastorakis, and J. M. Batalla, "Internet of Things (IoT) in 5G Mobile Technologies," *Modelling and Optimization in Science and Technologies Book Series*, vol. 8, Switzerland: Springer International Publishing, 2016.
- [5] S. Sundaram, "A Quantitative Analysis of 802.11 ah Wireless Standard," *International Journal of Latest Research in Engineering and Technology (IJLRET)*, vol. 2, pp. 26–29, February 2016.
- [6] N. Ahmed, H. Rahman, and Md. I. Hussain, "A comparison of 802.11ah and 802.15.4 for IoT," *Information and Communications Technology Express*, vol. 2, pp. 100–102, September 2016.
- [7] K. Cho, C. Jung, J. Kim, Y. Yoon, and K. Han, "Modelling and analysis of performance based on Bluetooth Low Energy," *2015 IEEE Latin-American Conference on Communications (LATINCOM)*, vol. 1, pp. 1–6, November 2015.
- [8] M. Franceschinis, C. Pastrone, M. A. Spirito, and C. Borean, "On the performance of ZigBee PRO and ZigBee IP in IEEE 802.15.4 networks," *2013 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, vol. 1, pp. 83–88, October 2013.

