IOT NETWORKING: TECHNOLOGIES AND APPROACHES FOR A DISTRIBUTED INFRASTRUCTURE-LESS WORLD

Matteo Saloni, Member, IEEE Master degree in Computer
Science, University of Trento, Trento, Italy

Abstract—Internet of things is rapidly becoming a commodi- tized technology: the widespread availability of low cost devices like personal assistants, smart sensors and always connected home appliances has lead to a situation where network access becomes indispensable. While wired connections may provide bandwidth and reliability, wireless networks are the de-facto standard for IoT due to cost, mobility and scalability advantages. Many wireless technologies can offer a distinct mix of performance, adaptability and power consumption, but which is the most suitable for an IoT world where ubiquitous availability, low power operation, device roaming and reliability are the pillars used to support billions of devices?

I. INTRODUCTION

Technological advancements in computer manufac- turing, miniaturization techniques and the development of sensing components have paved the way for the widespread adoption of powerful embedded devices, able to detect and interact with the surrounding environment and communicate over data networks. Nowadays, sensors are deployed everywhere: smartphones, vehicles, factories, landscape or energy monitoring, smart homes are only some of the scenarios which rely on some kind of sensing technology to understand the environment. We take for granted such a pervasive presence of sensors, but a little more than a decade ago they were considered an area of academic and industrial research, mostly unknown to the general public. It was the availability of inexpensive and low powered components, paired with the ability for manufacturers to integrate processors, radios and sensors in a single system on chip that led to the development of Internet of Things.

The Internet of things is the idea of a network where these tiny devices, which are objects in the physical world, are connected together and can communicate both with each others and with end users. First introduced by Kevin Ashton [1] in 1999, in association with RFID tags and supply chains automation, the expression “Internet of Things” (IoT) initially described the idea that computers could collect data about their surroundings by themselves, without a person inserting the information. In that specific scenario, computers could manage and inventor physical objects by autonomously reading their identifiers.

Starting from this early definition, IoT has been described in many different ways, all while being adopted in many different scenarios, resulting in the expansion of the original machine-to-machine focus towards an increasing ability to communicate with humans. Vermesan et al. [2] define the Internet of Things as simply an interaction between the physical and digital worlds. Others, like Pena-Lopez et al. [3], predict a paradigm where every kind of object possesses some kind of computing and networking capability embedded.

Independently from labels, almost all forecasts agree that the IoT is going to be huge, both in terms of numbers of devices sold, predicted to be more than 50 billions by 2020 [4], as in the way it will shape our lives.

What every definition agrees on, is the basic idea of the digital world interacting with the physical one, by means of sensors and actuators. First, data about the surrounding envi- ronment is collected, then an intelligent processing determines a reaction: the way the device should act in response to inputs. The innovation in IoT lies in this reasoning process, which leverages communication with other nodes and controllers, or service providers, to perform a task which would otherwise result complex and resource-hungry when tackled standalone [5]. The ability to communicate and collect information from various sources, analyze data and perform an appropriate action is the key element which makes these tiny appliances smart.

While the networking of devices such as sensors and actua- tors is the basic enabler for machine-to-machine connectivity, more often than not it can also be exploited for machine-to-human interaction. In a scenario where even small, single purpose things are able to sense their state, many of them lack the ability to communicate it to users: humans need visual or audible notifications, like lights or alarms. It is much easier to rely all kind of communication to more powerful and user-friendly devices like smartphones or control panels, than to enrich all IoT systems with components suitable for user interaction.

Things can be connected using wired or wireless technologies, depending on the usage and the deployment environment. While for example industrial scenarios can rely on cabling, thanks to the usage of mostly static systems, the vast majority of situations will require the support of mobility, which results in the adoption of wireless communication.

Traditional infrastructure-based networks can be extended to support IoT devices, either by integrating nodes in the same network, or by bridging a dedicated IoT network.

In the first case, nodes need to employ the adequate com- munication interface (eg. Wi-Fi cards, LTE modems), but they subsequently acquire the ability to directly communicate with computers (and smartphones etc) and thus also access Internet if needed.
In the second case instead, IoT devices can leverage the most suitable wireless technology for their very specific use case, but they depend on the presence of bridges, which are dual-network devices that act as glue between the IoT network and the pc/Internet world.

Many different networking techniques can provide the basis for IoT communication, both wired and wireless. Given the current technological landscape as of 2018, we'll try to describe and analyze the most prominent standards, while accounting the peculiar requirements of IoT networking.

II. IOT NETWORKING

Collecting and defining all IoT devices under a single def- inition is a daunting task: hydraulic actuators, alarm sensors, presence beacons, personal assistants, smart TVs, embedded WSN, even autonomous cars are all examples of very different kind of objects, which can coexist inside the IoT world.

Despite the many differences in capabilities and purpose between different classes, all IoT devices depend on network access to fulfill their tasks. In fact, ranging from dumb wireless switches up to personal voice assistants and even smartphones, the need to communicate with other devices, and more often than not towards cloud services over Internet, is a ubiquitous and defining requirement.

In such an hyper-connected environment, guaranteeing In- ternet access, or even LAN/WAN access, to any devices at any given time is a serious challenge for traditional, infrastructure- based networks. Physical constraints, fixed number of ac- cesses, reachability bounds, limited capabilities and expand- ability of core routers or access points pose a real threat on the adoption and massive deployment of IoT both in the industrial and in the consumer space.

A. REQUIREMENTS

Most of IoT devices are small, battery powered and very often they can be moved around by end users. Furthermore, they usually consume a very limited bandwidth, but at the same time they can be sensitive to delays and errors (think for example to valve actuators). As such, the ideal solution should be an ubiquitous wireless network, low power, low bandwidth, which guarantees an adequate level of reliability.
A minimal set of requirements for an ideal IoT network could look like the following.

- **Wireless**: devices are installed at physically, and even geographically dispersed locations;
- **Mobility**: devices can usually be moved by users, or are even mobile by their own means;
- **Scalability**: there could be hundreds of devices under a given area;
- **Low Power:** usually nodes are battery powered;
- **Low Bandwidth**: while a low data rate can be supported by a high-bandwidth network, a specifically designed technology can obtain results more reliable and less resource hungry;
- **Dynamic Configuration:** devices are powered on and off, moved around and should connect as soon as possible, without complex configurations or registration processes;
- **Reliability**: while transmission integrity and minimal packet loss are valuable, messages are the building blocks and thus path discovery, routing and fault-tolerance are more important;
- **Addressability**: devices need to be addressable, both locally (inside the IoT network) and globally when connected over Internet.

Additionally, the following aspects could improve the net- work efficiency and ease the work done by IoT devices [6].

  - **Self Configuration** could lessen the burden associated with first deployments and reconfigurations;
  - **Neighbor Discovery** mechanisms could offer nodes the ability to perform more complex and targeted reasonings, by knowing the surrounding nodes and obtaining a major context awareness;
- No **single-point-of-failure** makes the network more fault resistant and could also improve the performance by offering more routes for packet delivery;
- Node **identification** and **authentication** could be used to provide access control and to secure the communication;
- **Encryption** could provide privacy to the communication channel.

In the following sections we will briefly describe the most prominent and common wireless technologies, and assess their suitability for IoT deployments.

III. WIRED NETWORKS

Wired sensors networks connect devices with fixed cables, providing this way a reliable, stable and predictable commu- nication channel at the expense of mobility (see fig. 1).

Wiring an environment is a complex task: aspects like planning the network, deploying the cables, installing the nodes, setting topology and routing, and even future expandability have to be decided in advance. However, once adopted a wired network offers performance and reliability levels which can not be matched by wireless systems. The adoption of a dedicated medium like a cable which goes from a single device towards the network infrastructure can ensure high bandwidth, low latency and predicable performances, due to the lack of interferences, in straight opposition to systems which adopt a shared medium for communication, like wireless [6].

While sensors and nodes can share traditional Ethernet networks with personal computers, this naive approach doesn't offer a workable solution: many areas are sub-optimal for IoT devices, ranging from deployment costs to network topology, to performance and power consumption. As such, many different sensors-focused technologies have been proposed and developed: X10, CEBus, KNX, Insteon and many others (cfr. [7] and [8]. All those protocols rely on the construction of a bus-like network, where the data communication happens over electrical cables or power lines. This idea, while tempting on the cost side, has proved to be quite problematic on the functional one, with notoriously unstable performance due to power line interferences, network outages and segmentations induced by lines junctions and power switches [7].

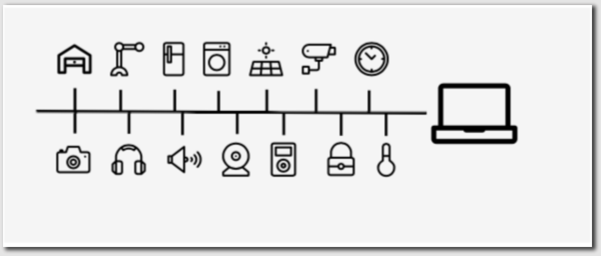


Fig. 1. IoT network - wired connection. Representation of a simplified cabled network, where every device shares the same common bus.

The lack of widespread adoption, paired with the inability of devices to move and the high deployment costs have condemned wired sensors networks to very limited scenarios, with the superseding of wireless connections in the vast majority of fields. As such, also industrial and academic worlds have focused on WSNs, leaving the research for wired sensors networks behind on many advanced topics like device discovery, self configuration, security etc.

However, in situations where safety and security requirements mandate an absolute reliability, wiring will always be preferred, since wireless networks can't offer the same degree of dependability. Among many others, scenarios like process automation control, traffic control systems, alarms, smart energy systems and medical applications are all examples which share the same reliability requirement [9].

One final advantage of wired connections is the ability to deliver power, together with data, to IoT devices over the same cables, avoiding the need to rely on batteries, which should be monitored and changed according to their depletion. This feature can play an important role in many situations, which can not let nodes exhaust their batteries and go off-line for extended periods of time. Anyway, delivering power via cables while leaving data transmission to wireless could be a favorable solution in terms of costs and complexity.

IV. WIRELESS TECHNOLOGIES

Wireless networking leverages radio communication to pro- vide a data connection without requiring dedicated cabling. Radio waves, which are used to transmit data packets, prop- agate freely through space: as such, wireless networking is inherently a technology which supports device mobility and fast changing environments.

In order to communicate, a node has simply to be in range of the radio transmission, and thus it is not tied to a specific place. The usage of a shared medium also means that potentially any device in reach could receive packets and participate in the communication (see fig. 2). Detached from fixed access ports, the limits in large - scale deployments for wireless networks are the enumeration and identification of clients and the time- sharing mechanisms adopted to effectively share the air space in a fair way between all the nodes in the given area.

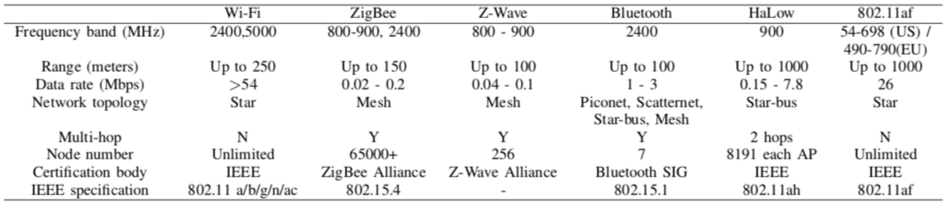
Being wireless, any of the following technologies inherently support node mobility. Anyway, different radio systems may employ different communication and packetization techniques, adopt different frequency bands and as such result in varying limitations on the ability of nodes to move freely around the coverage area. Furthermore, the kind of radio transmission adopted directly reflects on power usage and bandwidth capabilities of the selected technology.

Lastly, reliability of wireless communication is strictly dependent on the lack of electromagnetic interferences during transmission: not only external noise can provoke data loss and disturbance, but also the unregulated access to the shared medium by legitimate devices can result in the inability of receivers to successfully collect data packets. This situation poses a limit on the number of systems supported by dif- ferent wireless technologies, which depends on architectural and technical boundaries balancing performance, latency and reliability of data transmission.

It is of crucial importance to adequately evaluate the pro and cons of each wireless technology, in order to adopt the one most suited for the kind of IoT deployment envisioned for a given use case. For example, home automation environments may favor low power and wide coverage, while multimedia devices like smart speakers or TVs will adopt a short-range, high-bandwidth network, and maybe personal devices or smart tags could rely on quasi-near field technologies.
The following subsections briefly present the various avail- able technologies, and highlight their suitability for IoT in relation to the previously mentioned requirements, leaving to detailed studies (cfr. [10] [11] [12]) a more formal comparison.

Fig. 2. IoT - wireless connection. Exemplification of a wireless network, highlighting the lack of data cables and the ability for all devices to freely communicate in the given area.

The relevant specifications for the various candidate technologies are reported in table I, where a detailed recap of performance and technical



	Wi-Fi	ZigBee	Z-Wave	Bluetooth	HaLow	802.11af
Frequency band (MHz)	2400,5000	800-900, 2400	800 - 900	2400	900	54-698 (US) / 490-790(EU)
Range (meters)	Up to 250	Up to 150	Up to 100	Up to 100	Up to 1000	Up to 1000
Data rate (Mbps)	>54	0.02 - 0.2	0.04 - 0.1	1 - 3	0.15 - 7.8	26
Network topology	Star	Mesh	Mesh	Piconet, Scatternet, Star-bus, Mesh	Star-bus	Star
Multi-hop	N	Y	Y	Y	2 hops	N
Node number	Unlimited	65000+	256	7	8191 each AP	Unlimited
Certification body	IEEE	ZigBee Alliance	Z-Wave Alliance	Bluetooth SIG	IEEE	IEEE
IEEE specification	802.11 a/b/g/n/ac	802.15.4	-	802.15.1	802.11ah	802.11af

TABLE I
COMPARISON OF NETWORK PROTOCOLS

aspects helps the reader quickly confront the protocols and highlight their strengths or weaknesses.

A. NEAR FIELD COMMUNICATION (NFC)

Near Field Communication is a very short range com- munication technology, aimed at direct interaction between devices in close proximity. Adopted standards rely on RFID communication, which uses magnetic fields to transmit data packets between two devices. Transmission ranges are thus very limited, but this kind of technology provides a passive mode, where only one of the parties generates the magnetic field, thus avoiding the need for a battery on the second one. While useful for sensor reading by measurements devices, or for asset tags and contact-less payments, the many dis- advantages of NFC result in a very limited applicability on general-purpose scenarios.

B. BLUETOOTH

Bluetooth (IEEE 802.15.1) is a network technology targeted towards short range communication, with low data throughput and (relatively) low power consumption. Bluetooth networks support a limited number of nodes, and are primarily developed for providing communication sockets for data. While earlier versions lacks many features dedicated to *device and service discovery*, new revisions of the standard encompass a wide degree of additional scenarios by providing specifications for low power transmission, broadcast and anycast/multicast communication and also privacy and anonymization. **Bluetooth Low Energy,** introduced with version 4 of the standard, is an evolution of Classic Bluetooth, targeted at low power communication, with reduced range and data throughput, and improved power savings paired with extended advertisement and discovery functions. The recent introduction of **Bluetooth 5** offers significant enhancements in the area of range, speed and broadcasting, while also offering new features dedicated to network topology and message routing [13].

Bluetooth has many features which can satisfy the commu- nication needs of IoT: *low power transmission, low- to mid-bandwidth, node discovery* via broadcast, *message encryption.* It also supports various network topologies which could eliminate the *single-point of failure* represented by access points or gateways.

However, only the latest revisions of the Bluetooth standard demonstrate an attention towards device power consumption, which is a concern of great importance in an IoT world pop- ulated by battery-powered devices. Earlier Bluetooth versions designate different classes of devices to regulate the power emission and the coverage range. Starting with *Bluetooth LE* [14], radio duty-cycles, operating modes and connections types have been revised to allow nodes to preserve energy and thus extend their operative life.

Furthermore, *Bluetooth 5* [15] delivers operating modes specifically developed for IoT scenarios, which offer data rates lower than the usual 1 Mbps by employing coding techniques which improve data integrity by using more symbols for each transmitted bit. The result is a more robust transmission, which can achieve longer distances than before without requiring additional transmission power.

Nowadays, Bluetooth 5 appears as a viable wireless tech- nology for any kind of IoT deployment.

C. WI-FI

Conventional Wi-Fi (defined by IEEE 802.11 various stan- dards) is widely used to connect any kind of device to the Inter- net, *via access points* bridging wireless nodes with cabled net- works like LAN or WAN. Radio frequencies for 802.11b/g/n standards are provided by the 2.4GHz ISM band and are freely usable in many countries. Wi-Fi provides dedicated modes for connecting together two devices, but is not tailored towards direct access between a group of IoT devices, given the commitment to an inherently *infrastructured* approach. In fact, **Wi-Fi Direct**, an 802.11 extension for infrastructure-less scenarios, relies on one of the nodes acting like an access point which coordinates the communication between all the peers [16].

While the presence of Wi-Fi is ubiquitous, it lacks many features tailored to low power transmission, and also offers little capabilities in term of network topologies alternative to the centralized one. As such, it seems a sub-optimal choice for IoT networks. Ultimately, in the majority of situations Wi-Fi will still be used to provide *upstream* connectivity towards Internet and computers to IoT dedicated networks.

Additionally, Wi-Fi remains a suitable technology when long range communication is needed, thanks to the high power levels employed for radio transmission. Furthermore, the standardization body responsible for Wi-Fi, *IEEE*, has developed dedicated variants, which aim at providing a communication channel more suited for IoT needs, one which is able to compete with Bluetooth. Some of these will be explored in the following sections of this document.

D. ZIGBEE

ZigBee (IEEE 802.15.4) is a networking technology devel- oped for machine-to-machine communication, tailored directly at Internet Of Things scenarios where multiple nodes may connect together in a mesh-network to enable distributed com- munication [17]. Performance, range and power consumption are minimal, and ZigBee also delivers reasonably low latency and low duty cycle.

On paper, ZigBee offers coverage ranges up to 100 meters, similarly to Bluetooth, but it also provides an unique advan- tage: it supports multiple frequency ranges for radio communi- cation. The net result is the avoidance of the congested 2400 MHz range, which promotes better network communication due to the lack of collisions with packets sent by devices adopting one of the many technologies operating in the same range. The technology is intended to be both simpler and less expensive than Bluetooth or Wi-Fi, also thanks to the adoption of network topologies alternative to the usual *star*, like *mesh* and *tree*, which eliminates the cost associated with access points [10]. Furthermore, the very low data rates (less than 100 kbps) offered by ZigBee ensure that even devices with little computational capabilities, like the majority of low cost nodes, can successfully communicate within the network. At the same time, low power consumption greatly benefits from low data rates and long sleep cycles.

However, ZigBee low power design makes the technology ill suited in presence of highly mobile nodes, because long operating intervals excel in supporting fairly static situations where peers and routes rarely change. When a device moves across the area, the communication is temporarily disrupted and network topology has to account for the new position of the node, an expensive operation which could require many logical ticks. In ZigBee, this inconvenience would produce a sizable latency during data transmission.

E. Z-WAVE

Z-Wave is a proprietary wireless protocol used primarily for home automation, designed to provide low-latency trans- mission of small packets at a low data-rate [18]

Similarly to ZigBee, it employs a mesh topology, where nodes participate in the forwarding of packets. Z-Wave delivers both low- power and device-to-device communication, but the nature of the standard, more closed than both Bluetooth and ZigBee, when taken together with the requirement of certifications for interoperability, depict it as a *industry-oriented* technology.

Z-Wave operates on the 800 - 900 MHz frequency range, a desirable feature aimed at avoiding the congested 2400 MHz space. Despite being based on a mesh topology for device- to-device communication, Z-Wave nodes usually rely on a central hub acting as a coordinator and upstream (Internet) provider, thanks to dual radio or via a wired connection. Communication distance is quite limited, usually in the 30 - 50 meters range due to the adoption of energy saving policies, while the nominal range goes up to 100 meters. Data rates are similar to those provided by ZigBee, in the 10 - 100 kbps range. Z-Wave is optimized for battery-powered devices, and by design does not support node mobility: it works under the assumption that all devices in the network remain in a specific position. The mesh network will relay all messages to any node, with a scheduling for duty cycles specifically tailored towards the maximization of battery life.

Z-Wave is a strong candidate for IoT networking, but its application scope is limited *by design* to smart home scenarios, with a very narrow focus. This approach makes it a suitable contender for Bluetooth and ZigBee in its own scenario. The need to account license acquisition with specific investments is a barrier for companies to enter the market, a problem which could eventually favor the adoption of different technologies over the long term.

F. 802.11AH HALOW

The 802.11 protocol with its different variants is the most widespread and adopted wireless technology in the world. Almost everywhere Wi-Fi is a recognized term. Acknowledging the need for a low-power variant, the *IEEE Standards Committee* formed a working group tasked with the extension of 802.11 towards low-power applications. Released in 2017, 802.11ah is an amendment of 802.11 which uses the 850 - 900 MHz license-exempt bands to provide low power, shared networks aimed at *machine-to-machine* deployments, such a sensors and actuators. Low data rates for channel, long- range data transmission and the implementation of *target wake time* to regulate device activity are some of the IoT friendly properties of the new standard (cfr. [19] and [20]). Additionally, the adoption of somehow low frequencies, when compared to Wi-FI or Bluetooth, helps in wall penetration. A peculiar aspect of HaLow is the layout of stations, which can be grouped together to minimize contention of the radio medium and optimize wake-up periods: the ability of nodes to act as *relays* enables optimized operation and also extends the network coverage.

On paper, HaLow appears as a strong contender for the IoT networking scene: specifically designed for the task, it offers many features targeted towards huge IoT deployments. Anyway, the adoption of a different-than-usual frequency space requires the usage of different radio chips, resulting in the inability to leverage existing designs and thus requiring high investments from companies willing to adopt the new standard. Furthermore, the frequency space varies between different countries, producing a fragmented scenario which further increases development and adoption costs.

G. 802.11AF

At the core, 802.11af is another extension of 802.11 Wi- Fi, released in 2014. Originally aimed towards low-power and wide-area communication, it bases its operation on the adoption of unused television spectrum frequencies between 54 MHz and 790 MHz [21]. Since this range is usually dedicated to television UHF and VHF bands, 802.11af is also nicknamed White-FI.

Sharing many improvements over 802.11 with HaLow, 802.11af can also be successfully used for the construction of IoT networks. The long range coverage and the wall penetration guaranteed by the chosen frequencies are positive points for a sensors network. Additionally, the protocol envisions the ability for devices to utilize several channels at once. Thanks to the wide hypothetical frequency range this feature can result in successful transmissions over many kilometers with high data rates.

However, the need to utilize only frequencies not already in use by television results in a very fragmented support: not only the various countries differ in adopted channels, but even local states or districts could present operators occupying different channels. As such, the adoption of 802.11af by the general public is unfeasible, leaving its application space limited to big television or cellular operators, which are established players in the communication field and also have the resources required to develop and support such a specific deployment within their organizations.

V. CONCLUSION

The Internet of Things is already a successful reality, with several millions of devices deployed in a variety of different scenarios all over the world. Influential studies [4] predict an unstoppable growth of the sector, towards billions of things delivered each year to consumers. In such an hyper-connected scenario, it appears obvious that wired technologies have little to no place: given the growth rate and the sheer number of devices, the burden of cabling alone relegates wired connections to very specific use cases. On the opposite field of wireless technologies, the competition for becoming the IoT communication standard is fierce and rich of candidates. The market potential is huge, and many parties are ready to provide adaptations or brand new implementations of standards suitable to IoT needs.

Given the analysis portrayed in this work, Bluetooth 5 emerges as the natural candidate for IoT deployments in 2018. Its capabilities, joined with the market presence and the widespread adoption pose it as the most suitable wireless technology for a variety of scenarios. Anyway, the fast-pacing nature of the technological landscape inhibits our ability to make long-term predictions: a shift in usage or a technical break-trough could rise another wireless protocol to the role of IoT favorite network technology.

VI. ACKNOWLEDGMENT

This project is supported by a student grant of the IEEE Smart Cities Initiative.

REFERENCES

[1] K.Ashton,“That’internetofthings’thing,”http://www.rfidjournal.com/ articles/view?4986, Jun. 2009.

[2] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer et al., “Internet of things strategic research roadmap,” Internet of Things- Global Technological and Societal Trends, vol. 1, no. 2011, pp. 9–52, 2011.

[3] I. Pena-Lopez et al., “Itu internet report 2005: the internet of things,” ITU Internet Reports, 2005.

[4] D. Evans, “The internet of things: How the next evolution of the internet is changing everything,” Cisco Internet Business Solutions Group (IBSG), vol. 1, pp. 1–11, 01 2011.

[5] P. Sethi and S. R. Sarangi, “Internet of things: architectures, protocols, and applications,” Journal of Electrical and Computer Engineering, vol. 2017, 2017.

[6] T. K. Hui, R. S. Sherratt, and D. D. Sanchez, “Major requirements for building smart homes in smart cities based on internet of things technologies,” Future Generation Computer Systems, vol. 76, pp. 358– 369, 2017.

[8] C. Withanage, R. Ashok, C. Yuen, and K. Otto, "A comparison of the popular home automation technologies," in Innovative Smart Grid Technologies-Asia (ISGT Asia), 2014 IEEE. IEEE, 2014, pp. 600–605.

[9] M. Li and H.-J. Lin, "Design and implementation of smart home control systems based on wireless sensor networks and power line communications," IEEE Transactions on Industrial Electronics, vol. 62, no. 7, pp. 4430–4442, 2015.

[10] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi," in Industrial Electronics Society,2007.IECON2007.33rdAnnualConferenceoftheI-EEE. Ieee, 2007, pp. 46–51.

[11] D.Thomas,E.Wilkie,andJ.Irvine,"Comparisonofpower-consumption of wifi inbuilt internet of things device with bluetooth low energy," Intl J Comput Electrical Automation Control Inf Eng, vol. 10, no. 10, pp. 1837–1840, 2016.

[12] M. Elkhodr, S. Shahrestani, and H. Cheung, "Emerging wireless tech- nologies in the internet of things: a comparative study," arXiv preprint arXiv:1611.00861, 2016.

[13] M.Collotta,G.Pau,T.Talty,andO.K.Tonguz, "Bluetooth5:aconcrete step forward towards the iot," arXiv preprint arXiv:1711.00257, 2017.

[14] Bluetooth SIG, "Bluetooth core specification v4.2, 2014."

[15] ——, "Bluetooth core specification v5.0, 2016."

[16] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, "Device-to-device communications with wi-fi direct: overview and experimentation," IEEE wireless communications, vol. 20, no. 3, pp. 96–104, 2013.

[17] ZigBee Alliance, "IEEE 802.15. 4, ZigBee standard," 2009.

[18] Z-Wave Alliance, "Z-wave protocol overview," 2007.

[19] S.Aust,R.V.Prasad,andI.G.Niemegeers,"Ieee802.11ah:Advantages in standards and further challenges for sub 1 ghz wi-fi," in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 6885–6889.

[20] E. Khorov, A. Lyakhov, A. Krotov, and A. Guschin, "A survey on ieee 802.11 ah: An enabling networking technology for smart cities," Computer Communications, vol. 58, pp. 53–69, 2015.

[21] A. B. Flores, R. E. Guerra, E. W. Knightly, P. Ecclesine, and S. Pandey, "Ieee 802.11 af: A standard for tv white space spectrum sharing," IEEE Communications Magazine, vol. 51, no. 10, pp. 92–100, 2013.