INTERNET OF THINGS UNIFIED PROTOCOL STACK

Jozef MOCNEJ*, Adrián PEKÁR**, Winston K.G. SEAH**, Erik KAJÁTI*, Iveta ZOLOTOVÁ*
*Department of Cybernetics and Artificial Intelligence, Faculty of Electrical Engineering and Informatics,
Technical University of Košice, Slovak Republic,
**School of Engineering and Computer Science,
Victoria University of Wellington, New Zealand,
E-mails: jozef.mocnej@tuke.sk, adrian.pekar@ecs.vuw.ac.nz, winston.seah@ecs.vuw.ac.nz, erik.kajati@tuke.sk,
iveta.zolotova@tuke.sk

ABSTRACT

The Internet of Things (IoT) is a paradigm aimed at connecting everyday objects to the Internet. Given the character of IoT devices, the most popular way of connecting them is using wireless technologies. However, unlike traditional (legacy) networks, the IoT has unique traffic characteristics with specific demands on the used communication protocols. Together with the constrained nature of IoT devices and the diversity in IoT application domains, there is no one network technology that meets all requirements. IoT solutions are based on a variety of protocols that yield concerns about interoperability and mutual compatibility. This article provides a high-level overview of the most popular IoT network technologies and compares them in one unified protocol stack consisting of five layers. The proposed protocol stack is intended to highlight the similarities and differences among IoT network technologies and to provide their compatibility possibilities at different layers.

Keywords: *Internet of Things, IoT network technologies, unified protocol stack, wireless sensor networks, short range networks, long range networks*

1. INTRODUCTION

The Internet of Things (IoT) is a novel paradigm based on interconnecting a tremendous number of heterogeneous end devices and providing the acquired data for all kinds of different digital services. The term 'Internet of Things' was first coined by Kevin Ashton in 1999 while referring to a global network of objects connected to Radio Frequency Identification (RFID) in a supply chain [1]. Since then, many new technologies have emerged, and IoT has spread to other application areas as well. Nevertheless, the primary goal has always remained the same – to empower computers with the ability to monitor/control the physical world and enable them to make decisions without human interference.

IoT extends everyday things with computing power and a connection to the Internet so that they can sense, compute, communicate and control the surrounding environment. [2] These capabilities offer a new point of view on what kind of data should be gathered, how often and from which place in order to get information that was not available before. The possibility to augment the physical world with the information technology has become desirable in various application domains [3].

The communication is crucial in IoT, yet IoT networks have unique traffic characteristics, which are significantly different from traditional (legacy) networks. Since the fundamental feature of IoT is to monitor/control an environment, the message exchange is often based on events, the data flow is rather small and can show signs of irregularity and burstiness. Moreover, IoT devices are often constrained, e.g., have limited computing power, are powered by the battery, and communicate over lossy networks. Due to these reasons, the traditional TCP/IP protocol suite used in legacy networks has not automatically become the fundamental standard in IoT as well, but there is a need for network technologies specifically designed for wireless sensor networks (WSN), which generate less overhead and provide more efficient resources utilization.

However, the heterogeneity of IoT application domains also means that different use cases have different requirements, which can only hardly be addressed with one standard. IoT is so diverse that there is no one-size-fits-all approach. Consequently, we have to deal with interoperability and mutual compatibility issues, which contribute to the significant challenges in IoT.

To better comprehend the position and compatibility possibilities of IoT network technologies, we propose a unified protocol stack consisting of five layers – physical, data link, network, transport, and application. The presented protocol stack depicts the most commonly used IoT network technologies and compares their functionalities at each layer. The aim is to provide a big-picture overview and outlines the interoperability among different network technologies. This is our first contribution.

In addition, we briefly describe each of the depicted network technologies and provide references for more in-depth definitions to ease the selection process of the most suitable network technology for a particular IoT solution. That is the second contribution of this paper.

The content is addressed for readers who wish to begin research in the field of IoT and would like to broaden their knowledge in IoT network technologies. The intended audience is researchers as well as professionals including system and solution architects, technology evaluators, business strategists and decision makers.

2. RELATED WORK

Given the character of IoT devices and their application domains, the most popular way of connecting them is using wireless technologies. Consequently, one of the main IoT building blocks is a Wireless Sensor Network (WSN) or a

Wireless Sensor and Actuator Network (WSAN) comprising sensors and/or actuators called *nodes* which sense and possibly perform some control task/action by cooperating within their communication infrastructure. WSN/WSAN is a perspective topic and has been in the interest of many researchers.

Mainetti, Patrono, and Vilei [4] presented the evolution of WSNs towards IoT and addressed the issues related to the heterogeneity of network technologies. The authors described several network technologies and outlined the communication problems when attempting to interconnect IP based networks with the networks that are non-IP based. Eventually, they proposed a framework that utilized communication gateways to enable message forwarding among different protocols at the application layer. On the contrary, Bello, Zeadally, and Badra [5] discussed how to create interoperability at the network layer. Unlike gateway-centric solutions, compatibility at the network layer can eliminate the drawbacks of message translation and requirement to update gateways whenever a new technology is developed. The latter approach is more suitable for device-to-device (D2D) communication in IoT, although the assumption is that IoT protocols are able to cooperate at the network layer. Both papers analyzed the problem of interoperability in IoT but we missed a comparison which technology is suitable for which approach.

A more comparative study of emerging network technologies was presented by Rawat et al. [6]. The authors surveyed trending developments in WSN technologies to date and described some of the popular standards. The paper included technical characteristics of those standards to emphasize their similarities and differences. More recently, Al-Sarawi et al. [7] published a similar review of communication protocols but focused on the different set of technologies. The authors also extended the number of characteristics with the aim to create the guideline for researchers to select the right protocol for a particular solution. Our objective is similar, but we perceive the current list of commonly used IoT network technologies to be much broader. In addition, we missed the direct comparison of protocols from the stack hierarchy point of view, which would facilitate comprehension of their possible compatibility at different layers.

Consequently, we still see the gap for a comprehensive review that would cover all popular IoT network technologies and would compare them in a unified protocol stack to show their interoperability possibilities among different layers. This is the key motivation that led us to write this paper and what distinguishes us from other published articles. Our aim is to create a direct comparison of the most commonly used IoT network technologies, highlight which protocols can be interconnected at which layers, and provide a set of recommended literature for every technology should a reader would like to get more information.

3. IOT NETWORK TECHNOLOGIES

The Internet as we know it today is based on the Internet Protocol [8], which is maintained by the Internet Engineering Task Force (IETF). Using IP addresses to identify connected devices and route traffic has become completely natural. Therefore, one might think the similar analogy would be applied in the IoT as well in order to preserve compatibility, but it is not so obvious.

One attempt to resolve the issue of insufficient IP addresses due to the limited IPv4 address space was simply replacing IPv4 with IPv6. However, this created a new problem. The IPv6 packet header presents an unacceptable overhead in constrained environments with battery-powered nodes where every bit counts. This led to the formation of an IETF working group (WG) called 6LoWPAN (acronym of IPv6 over Low power Wireless Personal Area Networks) [9] to define header compression mechanisms so that IPv6 could be used even on devices with highly limited resources. As a result, they managed to define the transport of IPv6 on IEEE 802.15.4 networks. The 6LoWPAN WG evolved into the 6Lo (IPv6 over Networks of Resource-constrained Nodes) WG [10], formed in 2013 to continue in adapting IPv6 for other constrained networks, e.g. IPv6 over Bluetooth Low Energy [11], IPv6 over NFC [12], etc. Another successor is the 6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e) WG [13] that defines IPv6 over the time slotted channel hopping (TSCH) mode of IEEE 802.15.4e.

Concurrently, many other wireless communication and networking technologies have been developed by the industry to meet the needs of IoT applications, leading to numerous interoperability issues. Many began without any support for IPv6 but are slowly integrating IPv6 support. In Fig. 1, we present a detailed protocol stack that aims to consolidate the diverse technologies into a single view, using the five traditional layers: physical, data link, network, transport, and application. In proprietary solutions, where the exact protocols of the technology are not publicly known, we made a decision based on the functionalities they provide. The technologies that share a common protocol at the network layer can be interconnected without the need for translation gateways. The majority, however, still use their own solutions at the network layer, which make the compatibility possibilities more difficult. In these technologies, using the solutions at the application layer is the only option, even though we see the attempts to spread IPv6 to other protocols as well. The protocol stack also categorises network technologies into short and long range groups. The long range group can be further divided into unlicensed and licensed networks.

While the number of technologies may look high at first glance, IoT application scenarios are so diverse that every network technology has found its utilisation. Their similarities and differences are highlighted in Table 1. The comparison is made using the following characteristics:

- *Frequency band* – expresses an interval in the frequency domain.

- *Range* – presents the potential communication distance domains.

- *Data rate* – refers to the number of bits processed per unit of time.

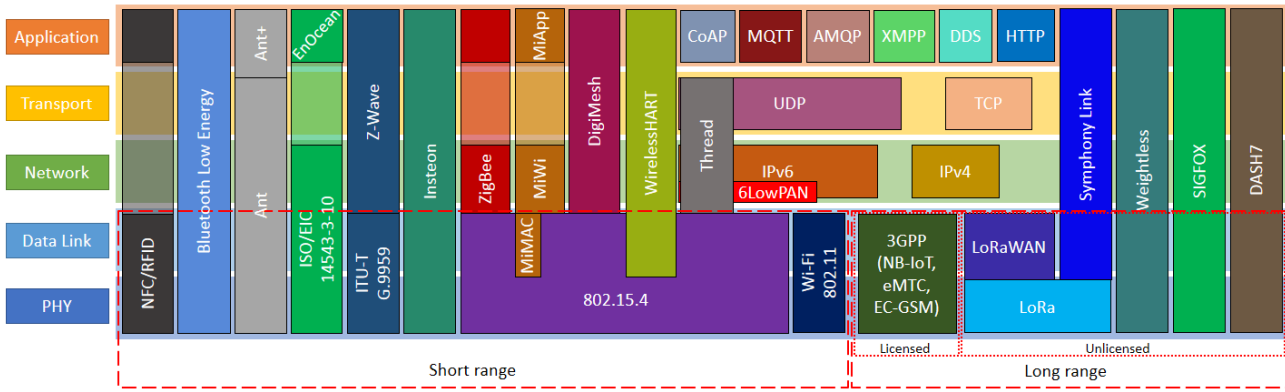- *Battery life* – outlines the power consumption demands.

Fig. 1 Protocol stack of IoT network technologies.

- *Topology* – characterizes the layout structure of a network.

- *Standardisation* – describes whether the technology is open or proprietary.

- *Governing body* – identifies who manages the technology.

The characteristics were chosen according to their information potential when selecting a suitable technology for a specific use case. The diversity of IoT solutions demands for different communication distances (*Range*), the volume of transferred data (*Data rate*), as well as energy capabilities of devices (*Battery life*). Moreover, the communication among devices can be single-hop or multi-hop (*Topology*) and we also have to consider whether the utilization of a technology must be licensed or not (*Frequency band*). Besides, the usefulness of a technology also depends on its author(s) (*Governing body*) and who can contribute to new improvements (*Standardisation*).

As the communication network technologies have been described by many researchers in great detail, we shall not repeat the published work. Instead, we present the following subsections with the aim to provide a general overview of the IoT technologies and include the references to other papers where more information can be found.

3.1. Short range networks

Short range networks use wireless technologies that communicate over ranges of a few centimetres up to hundreds of metres. These include close range contactless data transfer technologies, wireless personal area networks (WPANs) as well as, wireless local area networks (WLANs).

- **RFID** – Radio Frequency IDentification forms a critical component of the IoT concept when it was first introduced in 1999 by Kevin Ashton [1]. The falling price of passive RFID tags has enabled the rapid proliferation of this technology into all kinds of tracking and monitoring applications, securing its place in IoT again [35–37].

- **NFC** – based on the technology used for RFID, Near Field Communication [14,38,39] has found its usage

in the IoT paradigm as well. NFC operates in three modes – card emulation, reader/writer, and P2P, offering the information about the objects "by touch".

- **BLE** – Bluetooth Low Energy [15,40,41], also called Bluetooth Smart, has been designed for ultra-low-power applications, which makes it ideal for connecting devices within a small range. In addition, due to the popularity of BLE, the most salient challenges (for instance, communication over IPv6 [11]) are being addressed constantly in order to improve the technology even more.

- **Ant** – Ant is a proprietary protocol designed for long-term monitoring applications [16]. It specifies the physical, data link, and network layers. The application layer is provided by Ant+ [42], the extension that standardises communication between different devices.

- **EnOcean** – EnOcean is an energy harvesting technology for home and building automation, but also adapted to other domains. EnOcean devices can be battery-free and therefore the protocol must be simple and lightweight [17,43].

- **Z-Wave** – intended primarily for the smart home application domain, Z-Wave is a protocol used for home monitoring and control [18,44,45]. Many manufacturers have decided to implement Z-Wave into their products because of its features and wide support.

- **Insteon** – Insteon is a home automation technology based on dual-mesh topology, which is a combination of wireless radio frequency and existing electrical wiring [19,46]. Although the protocol is completely proprietary, it has found its use in many homes.

- **ZigBee** – ZigBee [20,47,48] is a standard-based network protocol built on IEEE 802.15.14 physical and data link layer, and is often incorrectly used as a generic reference to IEEE 802.15.4 radios. Based on the different networking system requirements, Zigbee Alliance offers three specifications – ZigBee PRO, ZigBee RF4CE, and ZigBee IP, all designed

Table 1 Characteristics of IoT Network Technologies

Technology	Frequency band	Range	Data rate	Battery life	Topology	Standardisation	Governing body
RFID [1]	Low / High / Ultra-high	1 cm – 100 m	1 – 100 kbps	passive: N/A active: 3–5 years	P2P	open standard	no single body
NFC [14]	13.56 MHz	0.2 m	424 kbps	passive: N/A active: 3–5 years	P2P	open standard	ISO/IEC
BLE [15]	2.4 GHz	10 – 100 m	1 Mbps	months to years	P2P / Star	open standard	Bluetooth SIG
Ant [16]	2.4 GHz	30 m	1 Mbps	years	P2P / Star / Mesh / Tree	proprietary	Garmin
EnOcean [17]	sub-1 GHz	30 – 300 m	125 kbps	Self-powered (energy harvesting)	Mesh	proprietary	EnOcean Alliance
Z-Wave [18]	sub-1 GHz	40 – 200 m	100 kbps	months to years	Mesh	proprietary	Z-Wave Alliance
Insteon [19]	sub-1 GHz	30 – 50 m	37.5 kbps	months to years	Mesh	proprietary	Smartlabs
ZigBee [20]	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	months to years	Star / Mesh / Tree	open standard	ZigBee Alliance
MiWi [21]	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	months to years	Star / Mesh / Tree	proprietary	Microchip Technology
DigiMesh [22]	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	years	P2P mesh	proprietary	Digi International
WirelessHART [23]	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	years	Mesh	open standard	HART Communication Foundation
Thread [24]	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	months to years	Star / Mesh / Tree	open standard	Thread Group Alliance
6LowPAN [25]	sub-1 GHz, 2.4 GHz	10 – 100 m	250 kbps	months to years	Star / Mesh / Tree	open standard	IETF
Wi-Fi [26]	sub-1 GHz, 2.4 GHz, 5 GHz	100 m; 1 km	Mbps to Gbps	days to months	Star	open standard	Wi-Fi Alliance
NB-IoT [27]	450 MHz – 3.5 GHz	10 – 15 km	250 kbps	10+ years	Star	open standard	3GPP
eMTC [28]	450 MHz – 3.5 GHz	10 – 15 km	1 Mbps	10+ years	Star	open standard	3GPP
EC-GSM-IoT [29]	850 – 900 MHz, 1800 – 1900 MHz	10 – 15 km	70 – 240 kbps	10+ years	Star	open standard	3GPP
LoRaWAN [30]	sub-1 GHz	10 – 15 km	50 kbps	10+ years	Star of stars	open standard	LoRa Alliance
Symphony Link [31]	sub-1 GHz	10 – 15 km	50 kbps	10+ years	Star	proprietary	Link labs
Weightless [32]	sub-1 GHz (-N and -P), TV white space spectrum (-W)	2 – 5 km	100 kbps (-N and -P), 10 Mbps (-W)	3 – 10 years	Star	open standard	Weightless SIG
SIGFOX [33]	sub-1 GHz	10 – 50 km	100 bps	10+ years	Star	proprietary	Sigfox
DASH7 [34]	sub-1 GHz	2 – 5 km	167 kbps	10+ years	Star / Tree	open standard	Dash7 Alliance

for low-power and low-cost devices. While supposedly an open-standard, Zigbee's concept of application profiles is also a source of incompatibility among Zigbee products.

- **MiWi** – MiWi is a simple networking protocol designed by Microchip Technology Inc. The MiWi stack aims to be an alternative to ZigBee for microcontrollers with constrained memory as its footprint is even smaller. MiWi uses MiMAC at the data link layer to communicate with Microchip RF transceivers and MiApp at the application layer to provide an interface for applications [21, 49, 50].

- **DigiMesh** – DigiMesh is another proprietary technology based on the IEEE 802.15.4 standard. Digimesh networks are represented by a simple topology where all devices are homogeneous and therefore function as end-nodes, routers, coordinators, etc., at the same time. This is a big difference

compared to ZigBee and further distinctions are detailed in [22].

- **WirelessHART** – WirelessHART [23, 51] is an open standard based on the popular Highway Addressable Remote Transducer (HART) protocol and a popular solution for real-time industrial process control [52].

- **Thread** – Thread is an IPv6-based networking protocol for home automation [24, 53]. The technology enables creating mesh networks using IP-addressable devices while keeping power consumption low. Although the full protocol specification is accessible only to the members of Thread Group Alliance, there is an open-source implementation called OpenThread.

- **6LowPAN** – 6LowPAN is a standard providing encapsulation and header compression to allow even low-power devices to send and receive IPv6 packets [25, 54, 55]. The 6LowPAN working group has defined 6LowPAN for the communication over IEEE 802.15.4, albeit the group's successors (6lo and 6TiSCH) work on IPv6 connectivity over other constrained networks as well.

- **Wi-Fi** – Although Wi-Fi was certainly not designed for IoT, it has been utilised in many IoT solutions due to its widespread usage [26, 56, 57]. Several lightweight application protocols, such as CoAP, MQTT, AMQP, etc., have been developed to reduce the unnecessary overhead and to make Wi-Fi suitable even for constrained environments. Moreover, Wi-Fi Alliance has recently introduced Wi-Fi HaLow as a low-power Wi-Fi solution for different IoT use cases [58].

3.2. Long range networks

Long range networks use wireless technology capable of transferring messages up to tens of kilometres to cover large areas. Low-Power Wide Area Networks (LPWAN) represent the specialised type of network technologies designed for interconnecting devices in constrained environments, focusing on energy efficiency and long-range coverage. We differentiate between unlicensed and licensed LPWAN according to the assigned frequency bands.

3.2.1. Unlicensed networks

- **LoRaWAN** – Long Range WAN (LoRaWAN) is a specification designed for wireless communication between constrained devices [30, 59, 60]. The main features of this technology are low data rate and wide communication radius. LoRaWAN, which is the MAC layer defined by the LoRa Alliance, is based on a proprietary spread spectrum modulation technique called LoRa.

- **Symphony Link** – Symphony Link [31] is another wireless specification using LoRa at the physical layer. Unlike LoRaWAN, Symphony Link offers a full protocol stack to ease the process of setting up a network, making the technology interesting especially for enterprise and industrial customers.

- **Weightless** – Weightless [32] is a technology from the global standards organisation called Weightless SIG that defined three open standards: Weightless-N, Weightless-P, and Weightless-W. The standards differ according to their capabilities and requirements. Weightless-N can handle only one-way communication but is also the most lightweight, Weightless-P is the flagship offering the full feature set and two-way communication, whereas Weightless-W has the extensive feature set but also the highest requirements.

- **SIGFOX** – SIGFOX is a technology created by the identically named company that aims at building wireless networks in an unlicensed frequency band. The technology employs the proprietary ultra narrowband (UNB) modulation with a heavily limited uplink connection. The low bit rate enables communication over large distance while using very low transmission power [33, 61, 62].

- **DASH7** – DASH7 Alliance protocol (D7AP) is an open source technology for low power communication [34, 63, 64]. Historically, it was based on the ISO/IEC 18000-7 standard for active RFID but has been significantly extended over the years. D7AP currently defines a full protocol stack from the physical layer up to the application layer.

3.2.2. Licensed networks

- **eMTC** – enhanced Machine Type Communication (eMTC) [28, 65, 66] is an evolution of LTE that has been optimised for IoT. Developed with energy efficiency in the mind, LTE-M is much less demanding than LTE, while still able to work within the normal construct of LTE networks. LTE is a part of the Release 12 and Release 13 specifications published by 3GPP.

- **NB-IoT** – NarrowBand Internet of Things (NB-IoT) has been standardised recently in 3GPP's Release 13 and it is aimed even more energy constrained devices than eMTC. NB-IoT does not require developing any additional networks as it is built from existing LTE functionalities and can be deployed in three different operation modes – stand-alone, in-band, or guard band [27, 67].

- **EC-GSM-IoT** – Extended Coverage GSM IoT (EC-GSM-IoT) [29] is a standard based on eGPRS that enables low power communication over GSM frequency bands. Since the GSM networks require only software updates to connect EC-GSM devices, the existing cellular infrastructures of the network operators can be re-used to offer low power connectivity.

4. CONCLUSION

The IoT paradigm is aimed at connecting everyday devices to the Internet. While communication plays a primary role in IoT, it also represents one of the biggest challenges due to the heterogeneous character of IoT use cases. The communication requirements are being addressed by the whole spectrum of network technologies, which makes it difficult to select the right protocol for a specific solution. Moreover, the diversity in IoT also yields concerns about interoperability and mutual compatibility.

This paper analyzed IoT from the communication perspective and created a comprehensive set of the most popular IoT network technologies to date. We briefly described each of them and provided the recommended list of readings should a reader would like to get more information. In addition, we proposed a unified protocol stack to directly compare all technologies among five layers and to highlight their similarities and differences. The proposed protocol stack outlines what layers every technology cover to better comprehend their interoperability possibilities. It also represents a tool that enables quick understanding of IoT network technologies for the intended audience who wish to begin the research in IoT.

Consequently, the contribution of this paper is twofold – a) the proposed unified protocol stack that depicts IoT network technologies among five layers and b) the comprehensive set of commonly used IoT network technologies to ease the selection of the right technology for a particular solution.

We mentioned that IoT compatibility in communication can be achieved by two approaches. One way is to implement a common protocol at the network layer, which will allow direct D2D communication without the need of intermediate gateways. While this option is certainly beneficial and several research groups are working on it, it is unlikely that all network technologies will implement the same protocol at the network layer.

Another approach is to provide an abstraction of the network technologies at the application layer. This option requires a unifying gateway, but IoT networks often use the star topology anyway. Moreover, when we look at the proposed protocol stack, it is evident that IoT will require both approaches to achieve the desired interoperability and compatibility among all technologies.

In particular, the latter option has become a part of the IoT integration platforms, which provide a foundation for connecting devices to the Internet, acquiring the generated data, and processing it in a meaningful way to get the desired output. In addition to providing the desired interoperability, the IoT platforms also offer standardized management of connected devices, leaving developers to focus on the added value of their solutions. Our research work is actively contributing to this topic, for instance by proposing a decentralized IoT architecture for resources utilization [68]. In the future, we would like to create an IoT platform that will be based on the decentralized architecture and will support the interoperability, compatibility, and scalability by design. We believe the IoT paradigm can be made sustainable, although further research is inevitable.

REFERENCES

[1] K. ASHTON, "That 'internet of things' thing," *RFiD Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] P. PAPCUN, "Dnes je prioritou prepoji ud, technolgie a procesy," *ATP Journal*, no. 9, pp. 54–55, 2018.

[3] M. KOVALČÍK, R. VÁPENÍK, P. FECIĽAK, and F. JAKAB, "Smart home control module as IOT/IOE learning," in *2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA)*. IEEE, 2015, pp. 1–6.

[4] L. MAINETTI, L. PATRONO, and A. VILEI, "Evolution of wireless sensor networks towards the internet of things: A survey," in *SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks*. IEEE, 2011, pp. 1–6.

[5] O. BELLO, S. ZEADALLY, and M. BADRA, "Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT)," *Ad Hoc Networks*, vol. 57, pp. 52–62, 2017.

[6] P. RAWAT, K. D. SINGH, H. CHAOUCHI, and J. M. BONNIN, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[7] S. AL-SARAWI, M. ANBAR, K. ALIEYAN, and M. ALZUBAIDI, "Internet of Things (IoT) communication protocols," in *2017 8th International Conference on Information Technology (ICIT)*. IEEE, 2017, pp. 685–690.

[8] J. POSTEL, "Internet Protocol," Internet Requests for Comments, RFC Editor, STD 5, September 1981, http://www.rfc-editor.org/rfc/rfc791.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc791.txt

[9] "IPv6 over Low power WPAN (6lowpan)," accessed: 9/12/2016. [Online]. Available: https://datatracker.ietf.org/wg/6lowpan/charter/

[10] "IPv6 over Networks of Resource-constrained Nodes (6lo)," accessed: 9/12/2016. [Online]. Available: https://datatracker.ietf.org/wg/6lo/charter/

[11] C. Gomez, S. M. Darroudi, and T. Savolainen, "IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP," Internet Engineering Task Force, Internet-Draft draft-ietf-6lo-blemesh-02, Sep. 2017, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-6lo-blemesh-02

[12] Y. CHOI, J.-S. YOUN, Y.-G. HONG, D. KIM, and J. CHOI, "Transmission of IPv6 Packets over Near Field Communication," Internet Engineering Task Force, Internet-Draft draft-ietf-6lo-nfc-06, Mar. 2017, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-6lo-nfc-06

[13] "IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch)," accessed: 9/12/2016. [Online]. Available: https://datatracker.ietf.org/wg/6tisch/charter/

[14] V. COSKUN, B. OZDENICZI, and K. OK, "A survey on near field communication (NFC) technology," *Wireless personal communications*, vol. 71, no. 3, pp. 2259–2294, 2013.

[15] K. H. CHANG, "Bluetooth: a viable solution for IoT? [Industry Perspectives]," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 6–7, December 2014.

[16] "ANT Message Protocol and Usage," accessed: 15/12/2016. [Online]. Available: https://www.thisisant.com/resources/ant-message-protocol-and-usage

[17] "EnOcean Technology – Energy Harvesting Wireless," accessed: 15/12/2016. [Online]. Available: https://www.enocean.com/fileadmin/redaktion/pdf/white_paper/WP_EnOcean_Technology_en_Jul11.pdf

[18] B. FOULADI and S. GHANOUN, "Security evaluation of the Z-Wave wireless protocol," *Black hat USA*, vol. 24, 2013.

[19] P. DARBEE, "The details," INSTEON, Whitepaper, 2013.

[20] P. BARONTI, P. PILLAI, V. W. CHOOK, S. CHESSA, A. GOTTA, and Y. F. HU, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards," *Computer communications*, vol. 30, no. 7, pp. 1655–1695, 2007.

[21] D. FLOWERS and Y. YANG, "Microchip MiWi™ Wireless Networking Protocol Stack," 2010.

[22] "Wireless Mesh Networking ZigBee® vs. DigiMesh™," accessed: 16/12/2016. [Online]. Available: https://www.digi.com/pdf/wp_zigbeevsdigimesh.pdf

[23] D. CHEN, M. NIXON, and A. MOK, "Why WirelessHART," in *WirelessHART™*. Springer, 2010, pp. 195–199.

[24] Thread Group, "Thread Stack Fundamentals," July 2015, accessed: 16/12/2017. [Online]. Available: https://www.silabs.com/documents/public/white-papers/Thread-Stack-Fundamentals.pdf

[25] Z. SHELBY and C. BORMANN, *6LoWPAN: The wireless embedded Internet*. John Wiley & Sons, 2011, vol. 43.

[26] L. LI, H. XIAOGUANG, C. KE, and H. KETAI, "The applications of WiFi-based Wireless Sensor Network in Internet of Things and Smart Grid," in *Proceedings of the 6th IEEE Conference on Industrial Electronics and Applications*, Beijing, China, 21-23 June 2011, pp. 789–793.

[27] R. RATASUK, B. VEJLGAARD, N. MANGELVEDHE, and A. GHOSH, "NB-IoT system for M2M communication," in *Proceedings of the Workshop on Device to Device communications for 5G NETWORKS (WD5G 2016) colocated with IEEE WCNC*, Doha, Qatar, 3-6 April 2016, pp. 1–5.

[28] A. RICO-ALVARINO, M. VAJAPEYAM, H. XU, X. WANG, Y. BLANKENSHIP, J. BERGMAN, T. TIRRONEN, and E. YAVUZ, "An overview of 3GPP enhancements on machine to machine communications," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 14–21, June 2016.

[29] "Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT)," accessed: 16/12/2016. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/45_series/45.820/45820-d10.zip

[30] K. MIKHAYLOV, J. PETÄJÄJÄRVI, and T. HAENNINEN, "Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology," in *Proceedings of the 22th European Wireless Conference*, Oulu, Finland, 18-20 May 2016, pp. 1–6.

[31] "Symphony Link," accessed: 16/12/2016. [Online]. Available: http://www.link-labs.com/symphony/

[32] "Weightless," accessed: 16/12/2016. [Online]. Available: http://www.weightless.org/about/which-weightless-standard

[33] "SIGFOX - M2M and IoT Redefined through cost effective and energy optimized connectivity," accessed: 28/10/2016. [Online]. Available: https://lafibre.info/images/3g/201302_sigfox_whitepaper.pdf

[34] M. WEYN, G. ERGEERTS, R. BERKVENS, B. WOJCIECHOWSKI, and Y. TABAKOV, "DASH7 alliance protocol 1.0: Low-power, mid-range sensor and actuator communication," in *Proceedings of the IEEE Conference on Standards for Communications and Networking (CSCN)*, Tokyo, Japan, 28-30 Oct 2015, pp. 54–59.

[35] X. JIA, Q. FENG, T. FAN, and Q. LEI, "RFID technology and its applications in Internet of Things (IoT)," in *Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, China, 21-23 April 2012, pp. 1282–1285.

[36] E. WELBOURNE, L. BATTLE, G. COLE, K. GOULD, K. RECTOR, S. RAYMER, M. BALAZINSKA, and G. BORRIELLO, "Building the Internet of Things Using RFID: The RFID Ecosystem Experience," *IEEE Internet Computing*, vol. 13, no. 3, pp. 48–55, May 2009.

[37] S. AMENDOLA, R. LODATO, S. MANZARI, C. OCCHIUZZI, and G. MARROCCO, "RFID Technology for IoT-Based Personal Healthcare in Smart Spaces," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 144–152, April 2014.

[38] K. FINKENZELLER, *RFID handbook: fundamentals and applications in contactless smart cards, radio fre-*

quency identification and near-field communication. John Wiley & Sons, 2010.

[39] P. C. GARRIDO, G. M. MIRAZ, I. L. RUIZ, and M. Á. GÓMEZ-NIETO, "A model for the development of NFC context-awareness applications on Internet of Things," in *Proceedings of the 2nd International Workshop on Near Field Communication (NFC)*, 2010, pp. 9–14.

[40] J. NIEMINEN, C. GOMEZ, M. ISOMAKI, T. SAVOLAINEN, B. PATIL, Z. SHELBY, M. XI, and J. OLLER, "Networking solutions for connecting bluetooth low energy enabled machines to the internet of things," *IEEE Network*, vol. 28, no. 6, pp. 83–90, Nov 2014.

[41] M. COLLOTTA and G. PAU, "Bluetooth for internet of things: A fuzzy approach to improve power management in smart homes," *Computers & Electrical Engineering*, vol. 44, pp. 137–152, 2015.

[42] N. Q. MEHMOOD and R. CULMONE, "An ANT+ protocol based health care system," in *Proceedings of the IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2015, pp. 193–198.

[43] J. PLOENNIGS, U. RYSSEL, and K. KABITZSCH, "Performance analysis of the EnOcean wireless sensor network protocol," in *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA)*, Bilbao, Spain, 13-16 Sep 2010, pp. 1–9.

[44] J. HALL, B. RAMSEY, M. RICE, and T. LACEY, "Z-Wave Network Reconnaissance and Transceiver Fingerprinting Using Software-Defined Radios," in *Proceedings of the International Conference on Cyber Warfare and Security*, Boston, MA, USA, 17-18 Mar 2016.

[45] P. AMARO, R. CORTESÃO, J. LANDECK, and P. SANTOS, "Implementing an advanced meter reading infrastructure using a z-wave compliant wireless sensor network," in *Proceedings of the 2011 3rd International Youth Conference on Energetics (IYCE)*. IEEE, 2011, pp. 1–6.

[46] P. DARBEE, "Compared," INSTEON, Whitepaper, 2013.

[47] "ZigBee Overview - Website," accessed: 28/10/2016. [Online]. Available: http://www.zigbee.org/zigbee-for-developers/zigbee/

[48] S. FARAHANI, *ZigBee wireless networks and transceivers*. newnes, 2011.

[49] M. A. N. AN1283, "Microchip Wireless Media Access Controller–MiMAC," 2009.

[50] M. A. N. AN1284, "Microchip Wireless Application Programming Interface–MiApp," 2009.

[51] D. CHEN, M. NIXON, S. HAN, A. K. MOK, and X. ZHU, "WirelessHART and IEEE 802.15.4e," in *2014 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 2014, pp. 760–765.

[52] J. SONG, S. HAN, A. MOK, D. CHEN, M. LUCAS, M. NIXON, and W. PRATT, "WirelessHART: Applying wireless technology in real-time industrial process control," in *Proceedings of the Real-Time and Embedded Technology and Applications Symposium (RTAS)*, St. Louis, MO, USA, 22-24 April 2008, pp. 377–386.

[53] "OpenThread," accessed: 16/12/2016. [Online]. Available: https://github.com/openthread/openthread

[54] G. MULLIGAN, "The 6LoWPAN architecture," in *Proceedings of the 4th workshop on Embedded Networked Sensors (EmNets)*. Cork, Ireland: ACM, 25-26 June 2007, pp. 78–82.

[55] S. RAZA, S. DUQUENNOY, T. CHUNG, D. YAZAR, T. VOIGT, and U. ROEDIG, "Securing communication in 6LoWPAN with compressed IPsec," in *Proceedings of the International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, Barcelona, Spain, 27-29 June 2011, pp. 1–8.

[56] G. R. MENDEZ, M. A. M. YUNUS, and S. C. MUKHOPADHYAY, "A WiFi based smart wireless sensor network for monitoring an agricultural environment," in *Proceedings of the IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, Graz, Austria, 13-16 May 2012, pp. 2640–2645.

[57] S. TOZLU, M. SENEL, W. MAO, and A. KESHAVARZIAN, "Wi-Fi enabled sensors for internet of things: A practical approach," *IEEE Communications Magazine*, vol. 50, no. 6, 2012.

[58] W.-F. Alliance, "Wi-Fi HaLow," 2016, accessed: 16/12/2016. [Online]. Available: http://www.wi-fi.org/discover-wi-fi/wi-fi-halow

[59] L. VANGELISTA, A. ZANELLA, and M. ZORZI, "Long-Range IoT Technologies: The Dawn of LoRa™," in *Proceedings of the 1st International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures*, Ohrid, Macedonia, 23-25 Sept 2015, pp. 51–58.

[60] L. Alliance, "A technical overview of LoRa and LoRaWAN," *White Paper, November*, 2015.

[61] "Sigfox Technology Overview," accessed: 28/10/2016. [Online]. Available: http://www.sigfox.com/en/sigfox-iot-technology-overview

[62] G. MARGELIS, R. PIECHOCKI, D. KALESHI, and P. THOMAS, "Low Throughput Networks for the IoT: Lessons learned from industrial implementations," in *Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, 14-16 Dec 2015, pp. 181–186.

[63] G. ERGEERTS, M. NIKODEM, D. SUBOTIC, T. SURMACZ, B. WOJCIECHOWSKIi, P. De MEULENAERE, and M. WEYN, "DASH7 Alliance Protocol in Monitoring Applications," in *Proceedings of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Krakow, Poland, 4-6 Nov 2015, pp. 623–628.

[64] "DASH7 Alliance," accessed: 16/12/2016. [Online]. Available: http://www.dash7-alliance.org/

[65] "LTE evolution for IoT connectivity," accessed: 31/10/2016. [Online]. Available: http://resources.alcatel-lucent.com/asset/200178

[66] "3GPP standards for IoT," accessed: 31/10/2016. [Online]. Available: http://www.3gpp.org/ftp/information/presentations/presentations_2016/3GPP_Standards_for_IoT.pdf

[67] "NB-IoT: A sustainable technology for connecting billions of devices," accessed: 31/10/2016. [Online]. Available: https://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2016/etr-narrowband-iot.pdf

[68] J. MOCNEJ, W. K. SEAH, A. PEKAR, and I. ZOLOTOVA, "Decentralised IoT architecture for efficient resources utilisation," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 168–173, 2018.

BIOGRAPHIES

Jozef Mocnej was born on 28.08.1992. He graduated (MSc) from the Department of Cybernetics and Artificial Intelligence, Faculty of Electrical Engineering and Informatics, the Technical University in Košice. Since 2015, he has been pursuing a Ph.D. at the same university. His research is related to the Internet of Things (IoT), Wireless Sensor Networks (WSN), and IoT architectures.

Adrián Pekár received the Ph.D. degree in computer science from the Technical University of Košice (TUKE), Slovak Republic, in 2014. For two years (2015–2016), he was a Data Centre, Systems and Network Engineer at the Institute of Computer Technology, TUKE. Since 2017, he has worked as a Postdoctoral Fellow for the Victoria University of Wellington, New Zealand. His current research areas of interest include network traffic classification and management, network traffic measurement data reduction and visualisation, machine learning, cloud computing, and software-defined networking.

Winston K. G. Seah received the Dr.Eng. degree from Kyoto University, Kyoto, Japan, in 1997. He is currently Professor of Network Engineering in the School of Engineering and Computer Science, Victoria University of Wellington, New Zealand. Prior to this, he has worked for more than 16 years in mission-oriented industrial research, taking ideas from theory to prototypes, most recently, as a Senior Scientist in the Institute for Infocomm Research, Singapore. His latest research interests include Internet of Things, wireless sensor networks powered by ambient energy harvesting, wireless multi-hop networks, software defined networking, and 5G access protocols for machine-type communications.

Erik Kajáti was born on 21.03.1991. He graduated (MSc) from the Department of Cybernetics and Artificial Intelligence, Faculty of Electrical Engineering and Informatics, the Technical University in Košice. Since 2017, he has been pursuing a Ph.D. at the same university. His research is focused on the Industry 4.0, Cyber-Physical Systems (CPS) and Industrial Internet of Things (IIoT).

Iveta Zolotová graduated from the Department of Technical Cybernetics of the Faculty of Electrical Engineering, Technical University of Košice, Slovakia in 1983. She defended her CSc. in the field of hierarchical representation of digital image in 1987. Since 2010 she has been working as a Professor at the Department of Cybernetics and Artificial Intelligence, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Slovakia. Her scientific research is focused on Smart Industry/Industry 4.0, Internet of Things, intelligent systems, networked control and information systems, supervisory control, data acquisition, human machine interface and remote labs. She also investigates issues related to vision and robotics.