Communication Capabilities of Wireless M-BUS: Remote Metering within SmartGrid Infrastructure

Pavel Masek*, David Hudec*, Jan Krejci*, Aleksandr Ometov†,
Jiri Hosek*, and Konstantin Samouylov‡

* Department of Telecommunications,
Brno University of Technology, Brno, Czech Republic
†Laboratory of Electronics and Communications Engineering,
Tampere University of Technology, Tampere, Finland
‡Applied Probability and Informatics Department,
Peoples' Friendship University of Russia (RUDN University), Moscow, Russia
`Contact author's e-mail: masekpavel@vutbr.cz`

Abstract. In today's landscape of utility management, the contribution of Internet of Things (IoT) to smart grids has acquired extensive potential. IoT paves a way to virtually control every smart device in almost every domain of society. Contrariwise, the smart grid networks attracted the attention of the universal research community. The idea of merging IoT with smart grid together demonstrates enormous potential. In this work, we investigate the suitability of Wireless M-BUS communication protocol for possible adoption in remote metering by evaluating possible communication range and system stability in future housing estate represented by university campus made of steel and concrete – this living area acts well when it comes to wireless transmissions. Measurements were executed by means of constructed prototype sensor devices utilizing the frequency 868 MHz which is the frequency by far the most used by WM-BUS devices in Europe.

Keywords: Wireless M-BUS, Remote Reading, M2M, Wireless Communication, Industry 4.0

1 Introduction

In 2017, the number of smart devices capable to transmit data through the network infrastructure reached 8.4 billion. By 2020, the studies indicate about 30 billion smart objects capable to establish connection without the human interaction [1, 2]. Following the definition given by European Commission in document Internet of Things – An action plan for Europe, Internet of Things (IoT) stands for "*a network of interconnected computers towards a network of interconnected objects*". In the context of Smart Grid (SG) landscape, IoT opens the doors for a promising future enabled by smart analytics. No doubt this is only feasible to realize owing the analytics data provided from the end users towards utility provider(s). At the end of the day, users' data could potentially enhance the efficiency as well as reduce congestion in the Smart Grid networks [3].

Focusing on the electricity, the transformation of the legacy electric power grid into intelligent bidirectional communication systems had paved the way to the Smart Grid of the "future" where new intelligent grids are supposed to enable interconnections between the already implemented SCADA systems and future implementations. The utilization of smart meters in all residential, commercial, and industrial places allows the utility provider(s) to gain the knowledge of customers' behavior on daily basis [4]. Smart meters, in general, provide end-users with the ability to interact with the utilities and wirelessly monitor, e.g., power consumption providing the assistance to reach the goal of reducing the bills.

1.1 Technologies for Smart Grid

In 2018, we can list many IoT-based technologies which are ready to be utilized for the need for SG applications. One one hand, many communication technologies are possible to use. On the other hand, the current situation does not offer guidelines towards the proper association between technology and SG application [5]. Focusing on IoT technologies, they are used mainly for long-range data transmissions [6]. The SG systems require advanced wireless technologies in comparison with the wired technologies, e.g., Power Line Communication (PLC), optical communication which takes place in case of scenarios when interference occurs or the metering devices are placed in "deep indoor", i.e., the signal attenuation of 60 dB.

Information streams of data within Smart Grid infrastructure can be treated in two ways: (i) the stream between all the smart meters connected in star topology where the Machine-Type Communication Gateway (MTCG) acts as the connecting point for all devices [7]; (ii) data streams between the MTCGs and remote control centers operated at the side of utility. In this work, we focus on the first type of communication where the smart device communicates directly with the MTCG. Owing to the tight and long-term cooperation with industry partners in Czech Republic and Austria, it has been recognized that Wireless M-BUS (WM-BUS) communication protocol is used very often as an alternative for PLC technology in case of mid-range communication indoor scenarios, i.e., for distances of up to 100 m[1].

WM-BUS is based on an open standard for automatic meter readout. The design of the protocol implies a battery-powered communicating device to operate for up to 10 years autonomously. This requirement can be achieved if the radio management module is switched to the low-power mode for as long as possible, and hence the awakening and transmitting procedures are managed and optimized – the summary of standardization activities related to Smart Grid is given in Table 1. Based on the WM-BUS standard, the communication initiation node is always the smart meter and never the concentrator, which is more suitable to extend the lifespan of the sensor battery [8, 9].

---

[1] See the first complete smart metering project in Austria – a complete model solution for whole Austria, Kamstrup, 2017: `https://www.kamstrup.com/en-us/case-stories/electricity-casestories/case-telekom-austria-system-at`

Table 1. Standardization activities in support of Industrial IoT (IIoT)

Protocol		DDS	CoAP	AMQP	MQTT	XMPP	HTTP, REST	SIP	**WM-BUS**
Service Discovery		mDNS				DNS-SD			**Proprietary**
Infrastr. Protocols	Routing Protocols	RLP							
	Network Layer	6LoWPAN					IPv4/IPv6		
	Link Layer	IEEE 802.15.4, IEEE 802.11, IEEE 802.3							
	Physical Layer	LTE-A; NB-IoT	EPC Global		IEEE 802.15.4	Z-Wave		IMS	

1.2 Wireless M-BUS in IIoT

M-Bus (wired) was developed and first introduced in the early 1990s. It was further extended wireless in 2005 (when the first draft of the EN 13757-4 was published, approved a year later [10]), which is 5 years before the concepts of the IoT and Industry 4.0 started gaining popularity in 2011 and even longer before they captured attention of the mass market in 2014 [11]. Industrie 4.0 is a term coined by the German Federal Government to optimize industrial production and provide smart manufacturing solutions [12]. Accordingly, Wireless M-Bus represents a solid competitor to protocols and networks tailored just for the IIoT, such as Sigfox, LoRaWAN (public or private implementations), or Narrowband-IoT [13]. Since it sets very similar goals (sensor-independence, battery-longevity, meter-automation), but has a few years of advantage, it may be even better established, settled, and stabilized than most of its counterparts [14, 15].

The WM-BUS network topology represents a star, where one or more measuring nodes transmit(s) the data to the aggregator acting as a server. The latter always senses the wireless medium for incoming connections and subsequent data collection. WM-BUS can operate in six communication modes representing specific applications detailed in Table 2. First three modes (i.e., S, T, and R) correspond to the transfer speeds, which are further divided into modes 1 and 2 for unidirectional or bidirectional communication. The remaining three modes (i.e., N, C, and F) are supported only by specific devices [9]:

- In frequent transmit mode (T), the meter sends data periodically or whenever a packet is available. Sub-mode $T1$ defines power saving operation, in which the device transmits to the aggregator and immediately enters power saving mode without waiting for the ACK.

- Stationary mode (S) is designed for unidirectional or bidirectional communication between the stationary or mobile devices. It has three sub-modes, $S1$, $S1M$, and $S2$. Sub-mode $S1$ is for unidirectional communication without the ACK from a server. This mode is primarily to handle the "daily" data transmissions. Sub-mode $S1M$ supports bidirectional communication in predefined cycles without the need for the device to wake up.
- In frequent receive mode (R), the meter is not sending the data periodically but instead is waiting for the aggregation request. Most of the time, the meter is in the power saving mode and awakens only over the predefined intervals for the packet reception. If no valid wake-up frame is received, the meter reenters the power saving mode.

Table 2. WM-Bus protocol transfer modes

	Transfer type	**Frequency**	**Cod. Scheme**	**Speed**
S	Stationary	868 MHz	Manchester	32768 kbps
T	Frequent transmit	868 MHz	Manchester 3 out of 6	100 kbps
R	Frequent receive	868 MHz	Manchester	4.8 kbps
N	Narrowband	169 MHz	NRZ	
C	Compact	868 MHz	Manchester	50 kbps
F	Frequent transmit and receive	433 MHz	NRZ	–

Wireless M-Bus frame structure After the protocol operation modes and the topology were introduced, we focus on the data frame structure to make the reader more familiar with the WM-Bus operational details. This section describes the WM-Bus communication phases (handshakes). In the first step, an over-the-top application at the application layer of WM-Bus sends its data to the RF module as a packet – as demonstrated below [9]:

1 Byte	1 Byte	n Bytes
Length	CI	AppLayer

In the next step, the radio module adds the following fields: (i) Control field; (ii) Manufacturer identification; (iii) Unique address based on parameters saved in the memory of the modules; and (iv) Optional information about received signal strength (RSSI). Therefore, the packet now has the following headers:

1 Byte	1 Byte	2 Bytes	6 Bytes	1 Byte	n Bytes	1 Byte
Length	C	ManID	Address	CI	AppLayer	RSSI

This packet is further encrypted (with AES-128 by default) and transmitted. If the connection is implemented as tunneling (P2P connection) between two

Wireless M-Bus modules, the address field, and the affiliated info is optional – thus allowing for simpler packet structure by sending only the RSSI:

1 Byte	1 Byte	n Bytes	1 Byte
Length	CI	AppLayer	RSSI

The AppLayer field is defined by the M-Bus application layer, which is used as a transition mechanism for the communication from link layer to higher layers. It uses the OMS 3.0.1 specification [16] derived from the EM 13757-4 standard for wireless communication [8]. In this work, we focus primarily on one of the WM-Bus equipped devices – IQRF radio modules. For our implementation, we selected the IQRF TR-72D-WMB module (see Fig. 1) [17]. This module is from the programmable IQRF technology line produced by MICRORISC that allows implementing the Wireless M-Bus or a similar protocol on the fly. It is further equipped with SPI and UART interfaces for communication with the master devices. Its block diagram is depicted in Fig. 2.

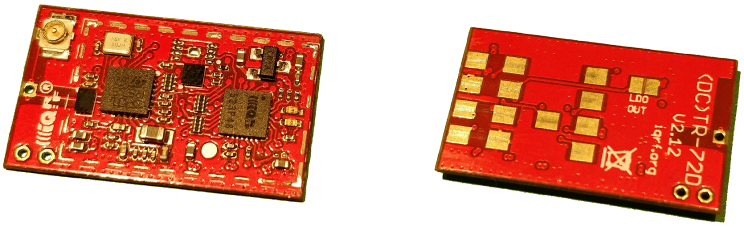

Fig. 1. Utilized IQRF TR-72DA-WMB module.

The said module supports following WM-BUS operating modes $S1$, $S2$, $T1$, and $T2$. The power voltage is in the range from 3.1 to 5.3 V with the maximal current of 1 μA in the sleep mode and 8-22 mA in the transmit mode. This value is based on the output power setting, which caps at 12.5 W. The module itself has support for 169, 433, and 868 MHz frequency bands, whereas the chip supports operation in one of the following modes [9]:

- *Meter*: The module can be connected via UART to the micro-controller, which serves as a data handler, i.e., it could be utilized to build the proprietary measurement devices based on WM-Bus protocol.
- *Multi-Utility Controller*: The module serves as the communication device for the meter data readout. Current firmware only supports bidirectional communication with meters in S and T modes and is still under development.
- *Sniffer*: The module captures all the available communication in the selected transmission mode. Owing to the implementation of the Wireless M-Bus protocol, it can also capture and decrypt the encrypted communication.

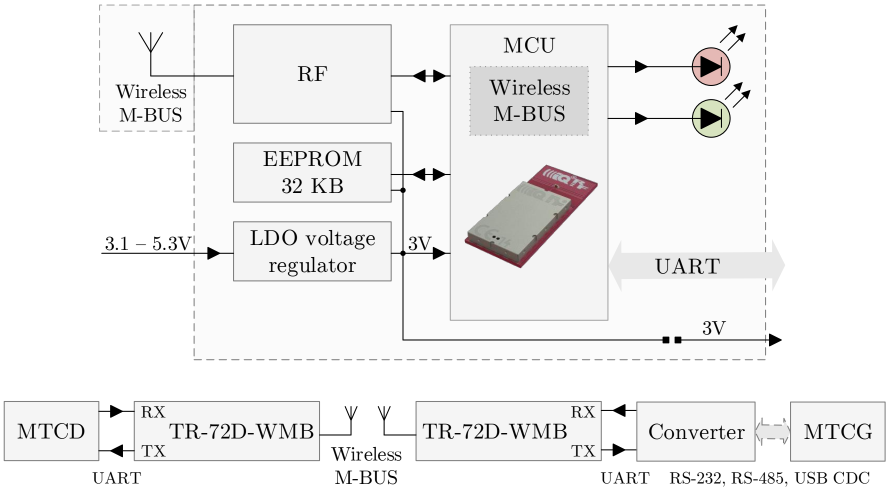

Fig. 2. Block diagram of TR-72DA-WMB module [9].

1.3 Main Contribution

In this paper, we expand our vision of Machine-to-Machine (M2M) communication for embedded devices basing on our previously developed industrial projects [9, 18]. In particular, we consider the situation, when low-cost IQRF radio modules can be configured in the role of Wireless M-Bus receivers. Inspired by that, we analyze and implement a real-world scenario, where the IQRF TR-72DA-WMB module [17] becomes a part of the MTCG device and receives the Machine-Type Communication (MTC) data sent via the WM-BUS communication protocol from electricity meters. What has changed compared to our last trial is the software generator at the side of MTC which was implemented completely from scratch. It is a Java program, which can generate Wireless M-BUS data from both graphical and command-line interfaces. It allows for precise protocol data unit specification and can send these message definitions in the form of telegrams to the Wireless M-BUS network using a supported hardware transceiver. Two device variations supported by the application are a standalone Wireless M-BUS module of IQRF TR-72D-WMB and more complex solution using the UniPi Neuron S103 board [19]. The software-hardware combination, created as a ready-to-use generator solution represents a powerful option in the area of testing Wireless M-BUS networks.

The remainder of this paper is structured as follows. In Section 2, we take a closer look at the measurement scenario where the Wireless M-BUS communication protocol is utilized. Going further, the Section 3 discusses the results obtained from designed test scenario as well as lessons learned originating from development phase.

2 Prototyped Industrial IoT Scenario

To demonstrate the functionality of previously created solution, see the [9], we have recently completed a full-scale implementation of WM-BUS. We investigated the suitability of Wireless M-BUS communication protocol for potential adoption in remote metering by evaluating possible communication range and connection stability in future housing estate represented by university campus made of steel and concrete – this living area acts well when it comes to wireless transmissions. Measurements were executed employing constructed prototype sensor devices utilizing the frequency 868 MHz, i.e., transmitting in Industrial, Scientific, and Medical (ISM) radio band.

2.1 Selected HW Devices

We have selected Raspberry Pi3 with I/O shield for our implementation. The connection between the Raspberry Pi and the mentioned shield is realized via the 26 pin board. The UART bus is escorted to the SIM slot on the shield, which is prepared for the connection. It is equipped with the IQRF TR-72D-WMB module. The said module supports WM-Bus S1, S2, T1, and T2 operating modes. The power voltage is in the range from 3.1 to 5.3 V with the maximal current of 1 uA in the sleep mode and 8-22 mA in the transmit mode. This value is based on the output power setting, which caps at 12.5 W. The module has support for 169, 433, and 868 MHz frequency bands, whereas the chip supports operation in one of the following modes: (i) Meter, (ii) Multi-Utility controller, and (iii) Sniffer.

2.2 Measurement Methodology

For the purpose of our trial, we concentrated on communication distance between two devices transmitting data indoor: (i) Wireless M-BUS transmitter running our proprietary software acting as M2M data generator, and (ii) universal WM-BUS USB Adapter AMB8465-M [20] in role of the receiver i.e., MTCG device – the integrated microprocessor controls the entire data communication as well as block- and checksum-creation. Data packets are built and transmitted according to EN13757-4. The USB-adapter is versatile configurable and supports all operating modes according to the wireless M-BUS specification. The quality of the radio link can be assessed by using the measured field strength (RSSI value).

The realized WM-BUS scenario is shown in Fig. 3 where all the important points are displayed. The "orange circle" represents the Wireless M-BUS data generator equipped by the external planar antenna. The frequency range of the antenna is 824 MHz to 896 MHz which suits well to our scenario where the devices communicate at 868 MHz. The gain added to the system by the antenna (RF part) is set to 6.7 dBi. Going further, the "orange circles" stand for the positions where we placed the RX device and tested one-by-one the parameters of the communication link. The list of possible combinations of power levels on both communicating sides is shown in Table. 3. At each location (Location A, B, C,

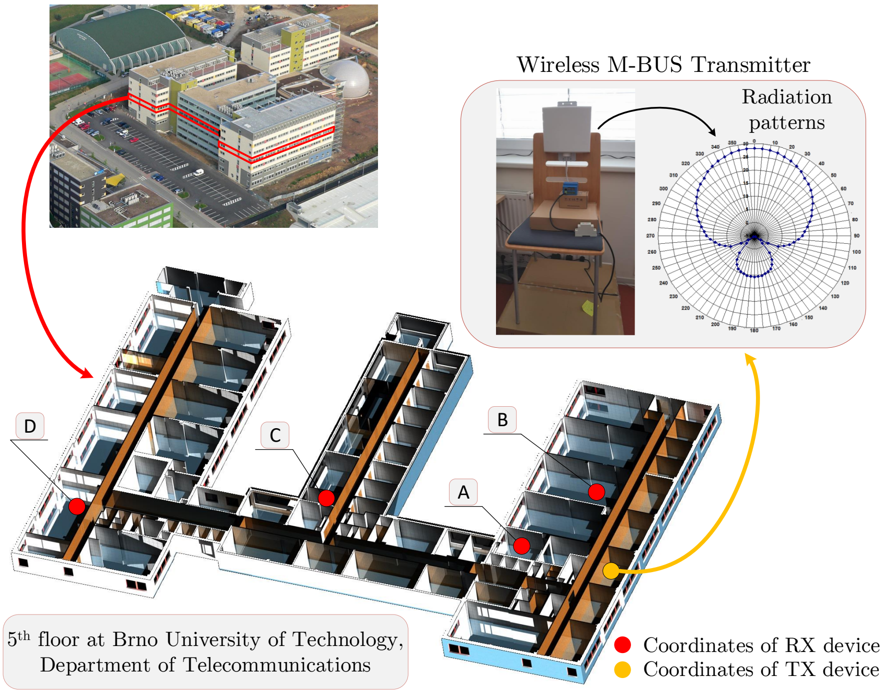

Fig. 3. Implemented WM-BUS scenario at Brno University of Technology, Czech Republic.

and D), all combinations of RF levels discussed in Table. 3 were performed. The data transmission consisted of sending 15 telegrams in a row with the time interval set to 20 s.

Table 3. List of RF levels for both the WM-BUS transmitter and receiver.

	RF Power levels [dBm]
IQRF TR-72D-WMB (Transmitter)	-30; -12; 0; +15
AMB8465-M (Receiver)	-5; 0; Max

3 Lessons Learned and Conclusions

During the development and implementation phases of our work, we have solved a number of challenges and drawbacks: (i) Raspberry Pi 3 uses different access to the serial interface. Hence, modifications on the boot level were needed; (ii) communication between wireless IQRF TR-72D-WMB module and the processing unit via UART had to be redesigned for the target case; (iii) the sniffed packets required re-encryption with the AES key of the IQRF module and were decrypted again to access the data (see our previous work [9] where the process of unencrypted and encrypted communication and following SW implementation is described in detail); (iv) the implementation of the data packets is not identical across the manufacturers and therefore for each device the sniffed data needed to be analyzed separately.

Table 4. Summary of configured RF power levels on both devices together with number of successfully received telegrams for all measured locations. The combinations of RF levels on the side of TX/RX which leads to data transmissions without packet loss are highlighted by grey.

	Location A			**Location B**			**Location C**			**Location D**		
	TX	**RX**	**No.**	**TX**	**RX**	**No.**	**TX**	**RX**	**No.**	**TX**	**RX**	**No.**
RF Levels [dBm]	-30	-5	6	-30	-5	0	-30	-5	0	-30	-5	0
	-12	-5	13	-12	-5	14	-12	-5	0	-12	-5	0
	0	-5	15	0	-5	15	0	-5	0	0	-5	0
	15	-5	15	15	-5	15	15	-5	8	15	-5	11
	-30	0	10	-30	0	0	-30	0	0	-30	0	0
	-12	0	15	-12	0	10	-12	0	0	-12	0	0
	0	0	15	0	0	15	0	0	0	0	0	0
	15	0	15	15	0	15	15	0	9	15	0	11
	-30	Max.	11	-30	Max.	0	-30	Max.	0	-30	Max.	0
	-12	Max.	15	-12	Max.	4	-12	Max.	0	-12	Max.	0
	0	Max.	14	0	Max.	15	0	Max.	0	0	Max.	0
	15	Max.	14	15	Max.	13	15	Max.	12	15	Max.	11

In the course of our development, we have performed practical measurements in all of the above-mentioned locations, see Fig. 3. As the measurements took place indoor, types of used materials play the critical role for the signal propagation. Owing to the possibility to use information from the drawing documentation of the building, the following materials are used: (i) reinforced concrete, (ii) clay block masonry, (iii) autoclaved aerated concrete, (iv) gypsum boards, (v) thermal insulation, and (vi) acoustic insulation.

Going towards the practical measurements, on top of the redesigned HW, an entirely new software layer has been introduced to generate WM-BUS data traffic (in case of this trial, the data representing the electricity meter is sent periodically) at the side of the WM-BUS transmitter (in the role of a metering device; MTCD) towards the WM-BUS data concentrator (MTCG). The complexity of this solution is further highlighted by the fact that the transmitted data can also be encrypted; re-encryption with the AES key of the IQRF module is implemented.

The obtained data is shown in Table. 4 and depicted in Fig. 4. One can see the results in case of some TX/RX RF level combinations do not follow the the-

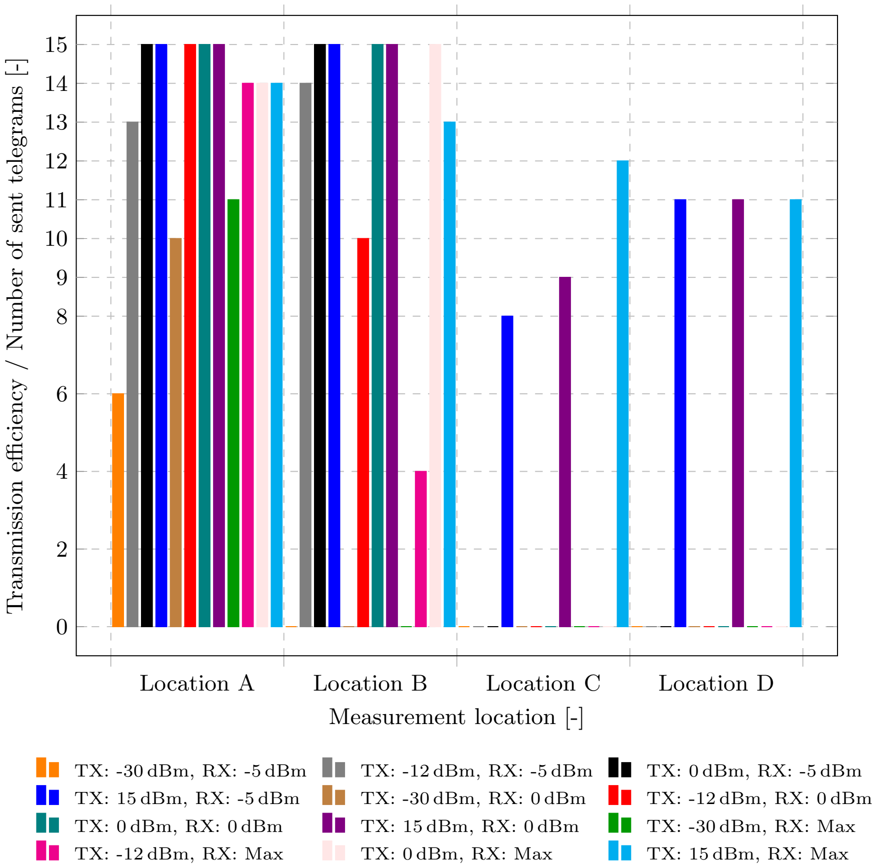

Fig. 4. Transmission efficiency – dependence on RX and TX output RF power levels.

oretical expectations. This behavior has two possible explanations: (i) the measurements were conducted during the working hours at the university. Therefore, the university staff and students influenced the signal propagation. On the other hand, those results stand for the real conditions expected to be met in case of remote metering, e.g., housing estate; (ii) the utilized frequency band is free to use which together with the unique rooms acting as obstacles (EMC chamber, acoustic chamber, etc.) causes unexpected signal propagation while sending the data at 868 MHz.

As mentioned before, this paper was intended as a proof-of-concept hardware implementation that significantly reduces the cost of Wireless M-Bus based communication platform. In our future work, we are planning to expand the functionality of our platform by adding support for more smart-meter vendors, as well as to further work with smart and connected IIoT / Industry 4.0 enablers.

Acknowledgment

The described research was supported by the National Sustainability Program under grant LO1401. For the research, the infrastructure of the SIX Center was used. This work has been developed within the framework of the COST Action CA15104, The Inclusive Radio Communication Networks for 5G and beyond (IRACON).

References

1. A. Nordrum, "Popular Internet of Things Forecast of 50 billion Devices by 2020 is Outdated," *IEEE Spectrum*, vol. 18, 2016.
2. P. Masek, D. Hudec, J. Krejci, J. Hosek, A. Ometov, S. Andreev, Y. Koucheryavy, and F. Kroepfl, "Advanced Wireless M-Bus Platform for Intensive Field Testing in Industry 4.0-Based Systems," in *Proc. of IEEE European Wireless Conference*, vol. 1–6, 2018.
3. J. Bhatt, V. Shah, and O. Jani, "An instrumentation engineer's review on smart grid: Critical applications and parameters," *Renewable and Sustainable Energy Reviews*, vol. 40, pp. 1217–1239, 2014.
4. G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.
5. P. Middleton, T. Tully, J. Hines, T. Koslowski, B. Tratz-Ryan, K. Brant, E. Goodness, A. McIntyre, and A. Gupta, "Forecast: Internet of Things-Endpoints and Associated Services, Worldwide, 2015," *Gartner Inc., Stamford, CT, USA, Tech. Rep. G*, vol. 290510, p. 57, 2015.
6. A. Ometov, N. Daneshfar, A. Hazmi, S. Andreev, L. F. D. Carpio, P. Amin, J. Torsner, Y. Koucheryavy, and M. Valkama, "System-level analysis of ieee 802.11 ah technology for unsaturated mtc traffic," *International Journal of Sensor Networks*, vol. 26, no. 4, pp. 269–282, 2018.
7. J. Hosek, P. Masek, S. Andreev, O. Galinina, A. Ometov, F. Kropfl, W. Wiedermann, and Y. Koucheryavy, "A SyMPHOnY of Integrated IoT Businesses: Closing the Gap between Availability and Adoption," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 156–164, 2017.
8. European Committee for Standardization, "EN 13757-4. Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio Meter reading for operation in the 868-870 MHz SRD band)." http://oldfjarrvarme.unc.se/download/1309/fj, 2003.
9. K. Zeman, P. Masek, J. Krejci, A. Ometov, J. Hosek, S. Andreev, and F. Kroepfl, "Wireless M-BUS in Industrial IoT: Technology Overview and Prototype Implementation," in *Proc. of 23th European Wireless Conference; Proceedings of European Wireless 2017*, pp. 1–6, VDE, 2017.
10. M. Arian, V. Soleimani, B. Abasgholi, H. Modaghegh, and N. S. Gilani, "Advanced metering infrastructure system architecture," in *Proc. of Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific*, pp. 1–6, IEEE, 2011.
11. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

12. P. Lade, R. Ghosh, and S. Srinivasan, “Manufacturing Analytics and Industrial Internet of Things,” *IEEE Intelligent Systems*, vol. 32, no. 3, pp. 74–79, 2017.
13. H. Wang and A. O. Fapojuwo, “A survey of enabling technologies of low power and long range machine-to-machine communications,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2621–2639, 2017.
14. S. Spinsante, S. Squartini, L. Gabrielli, M. Pizzichini, E. Gambi, and F. Piazza, “Wireless m-bus sensor networks for smart water grids: analysis and results,” *International Journal of Distributed Sensor Networks*, vol. 10, no. 6, p. 579271, 2014.
15. E. Kaloudiotis, “A 169 MHz and 868 MHz Wireless M-Bus Based Water and Electricity Metering System,” 2015.
16. OMS-Group, “The Open Metering System specification.” http://oms-group.org/en/oms-group/about-oms-group/, 2016.
17. IQRF – Technology for Wireless, “TR-72D-WMB series.” http://www.iqrf.org/products/transceivers/tr-72d-wmb, 2016.
18. P. Masek, J. Hosek, K. Zeman, M. Stusek, D. Kovac, P. Cika, J. Masek, S. Andreev, and F. Kröpfl, “Implementation of true IoT vision: survey on enabling protocols and hands-on experience,” *International Journal of Distributed Sensor Networks*, vol. 12, no. 4, p. 8160282, 2016.
19. UniPi.technology, subsidiary of Faster CZ spol. s r.o., “UniPi Neuron S103.” https://www.unipi.technology/unipi-neuron-s103-p2, 2016.
20. Wurth Elektronik eiSos GmbH & Co. KG, “Wireless M-Bus USB Adapter 868 MHz.” https://www.amber-wireless.com/en/amb8465-m.html, 2018.