Lora Nodes in Existing Access Control System Infrastructure: A Feasibility Study

Tomas HYHLIK[1,2], Marek NERUDA[1], Pavel BEZPALEC[1], Lukas VOJTECH[1], Vlastimil BENES[2]

[1]Department of Telecommunication Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague,
Technicka 2, Prague, Czech Republic
[2]Institut of Microelectronic Applications, IMA s.r.o.,
Na Valentince 1003/1, Prague, Czech Republic

[hyhlito1 | marek.neruda | pavel.bezpalec | lukas.vojtech]@fel.cvut.cz, vlastimil.benes@ima.cz

DOI: 10.15598/aeee.v13ix.xxxx

Abstract. *The Wireless Sensor Network (WSN) plays an important role in the Internet of Things (IoT). It is very suitable for intelligent buildings providing a convenient way to collect sensor data and control electronic devices in the building and its surroundings. This paper proposes an extension of the existing access control system with WSN. Design of sensor nodes and gateway connected to the existing RS485 network is performed. The results of a long-term operation measurement in one university floor show the maximum number of sensor nodes simultaneously transmitting data in RS485 network is up to hundreds or thousands in dependence on used RS485 data rate and used reserve of data rate which prevent from malfunction of the access control system. The results prove the WSN can be effectively used in an existing RS485 infrastructure.*

Keywords

Access control system, LoRa, LPWAN, WSN.

1. Introduction

The demands and use cases of Internet of Things (IoT) applications including security, asset tracking, agriculture, smart metering, smart cities, and smart homes as well as the growth of IoT wireless technologies, which require long range, low power consumption, low data rate and low cost are recently increased.

Short-range IoT applications like smart homes are broadly based on Zigbee or Bluetooth technologies that use the 2.4 GHz ISM band [1], [2]. Long-range IoT applications are typically based on a special kind of wireless technology called Low Power Wide Area Network (LPWAN) [3]. Many LPWAN wireless communication technologies appeared during its evolution with unlicensed ISM band, e.g., LoRa and SigFox and licensed band, e.g., NarrowBand-Internet of Things (NB-IoT) and Long Term Evolution-Machine Type Communication (LTE-M). The LPWAN technologies aim to have range up to 10–15 km in rural areas and 2–5 km in urban areas [4] and can have one of the following topologies: star (centralized), star of stars (decentralized) and mesh (distributed) [5]. Very low power consumption should allow sensor nodes a very long battery life, even greater than 10 years. The low cost of hardware (HW) is achieved by fully integrated transceivers and minimized number of off-chip components [6].

The industry of IoT is growing because of its enormous potential. Cisco study [7] says IoT will be combined with other technologies such as artificial inteligence (AI), fog computing and blockchain. Such a combination of technologies will provide greater value of investment for companies. IoT applications in smart cities require a scalable network coverage. This can be achieved by interconnection of multiple gateways as proposed in [8], where all gateways are connected to web server accessible via the Internet. It aims to manage urban street lighting and the implementation of smart metering is also considered as a future work. Similar application is proposed in paper [1] which focuses on assisted real-time automatic meter reading (AMR) in cities, but the scalable range is established by mesh network topology. The IoT applications in a smart buildings concept can be proposed as shown in [2], where nodes exchange data with the cloud via a Wi-Fi router or Bluetooth gateway connected to the

Internet. Similar application is proposed in [9] where nodes are controlled by a master node via Zigbee network that is conncected to a PC via RS232. Basic smart metering systems can be proposed with a gateway connected to a PC where the data are processed as proposed in [10], [11] and [12]. A long-range metering system can be established by multiple gateways connected to a network server from which data are obtained by the application server [13]. Similar network is proposed in Smart Farm application [14] with the difference that nodes can also be connected to the gateway via RS485 which forms a hybrid wired /wireless system.

This paper proposes to extend the access control system to include a low power Wireless Sensor Network (WSN) which can be used for smart metering applications, smart building applications and the building surroundings which is related to smart city applications. The WSN gateway is connected by the same way as a card reader is connected in the access control system, therefore it also has to support the same protocol. This can lead to complications since the reader is ment to transmit a short packets with user ID when the user's credential is attached to it. The WSN gateway is designed and tested in access control system of one university floor. The results show the infrastructure of access control system can manage up to thousands sensor nodes in dependence on used RS485 data rate.

2. System Design

2.1. General System Design

1) Architecture of Access Control Systems

Access control systems are electronic systems controlling the access of users into restricted areas depending on the user identity [15]. A typical system architecture is shown in Fig. 1.

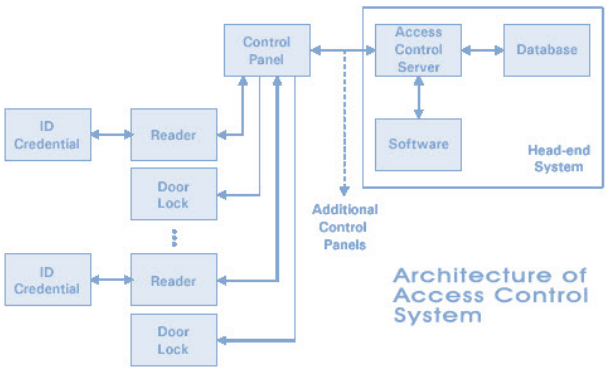

Fig. 1: Example of access control system architecture [15]

The ID Credential represents the user identificaton, provided for instance by RFID tag, fingerprint, QR code. The Reader reads the data from the ID Credential and sends it to the Control Panel. The Door Lock is used to control the physical access of users to the restricted area, e.g., building, room, floor. The Control Panel is the interface between Access Control Server and pairs the Reader with the Door Lock. It typically connects these pairs via RS485 and Access Control Server via Ethernet, i.e., TCP/IP protocol. The main function is the management of these pairs. The Database contains user IDs. The Access Control Server uses Software (SW) to manage the Database and communicates with all Control Panels. The Reader scans data from submitted ID Credential and transmits the data to the Control Panel, which resends it to the Access Control Server. The Access Control Software finds the received user data in the Database and, if found, sends a command to the corresponding Control Panel to switch the corresponding Door Lock.

2) Wireless Sensor Network Design

Wireless sensor network design is based on a popular IoT technology LoRa, which is a LPWAN technology using ISM band, 433 MHz, 868 MHz and 915 MHz (depends on the region) and communicates on multiple frequency channels and uses multiple data rates [16]. The LoRaWAN is an open standard network protocol and system architecture specified by [17] and creates a media access control (MAC) layer on the top of the LoRa physical layer, secured by AES-128 encryption. The LoRaWAN nodes communicate directly with the LoRaWAN gateway [18].

2.2. Specific System Design for Testing Proposes

1) Tested Access Control System Architecture

The access control system to be extended by WSN is designed by IMA company, but it differs from the general architecture shown in Fig. 1 by an added CKP device that creates an interface between the Control Panel and the Reader with the Door Lock. There are several types of CKP devices to connect different types of Readers, Door Locks, barriers and gates, but all of them support the protocol of the IMA company on the RS485 network. The IoT extension of the access control system is done by connecting a WSN Gateway to the Control Panel via the RS485 network, i.e., the same way as CKP device is connected as shown in Fig. 2. Therefore the WSN Gateway has to support the same protocol as CKP device in RS485 network to communicate with the Control Panel. It's a collision proto-

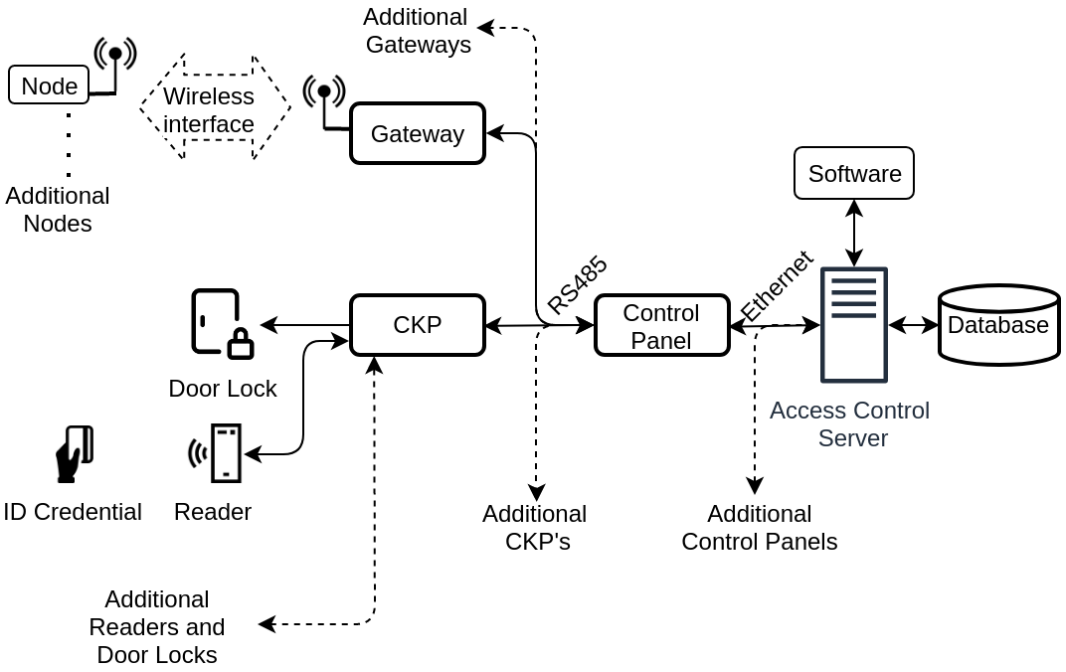

Fig. 2: IMA access control system architecture with WSN extension

col, where all connected devices follow the rule "listen before talk", collisions are detected by integrity check mechanism aplied for all messages. When the device receives a corrupted command, it requests a retry.

The Access Control System operates by obtaining a CKP list of valid cards (ID Credentials) from the Access Control Server. The designed Gateway takes it as a list of valid device addresses in the WSN. When the user presents his card to the Reader and the card ID matches one of the valid cards, the CKP device sends the data to the Access Control Server. The same procedure applies to the Gateway. When the Gateway receives data from a Node and the Node address matches one of the valid device address list, the Gateway sends the data to the Access Control Server.

2) Design of Tested Wireless Sensor Network

The most important requirements for the WSN Gateway are simplicity, low cost and the ability to use third-party nodes. LoRa with the standardized network protocol LoRaWAN is chosen as wireless communication technology, but only in single-channel mode as used in development projects [19], so it is not fully LoRaWAN compliant. Single-channel Gateway communicates only on one channel and data rate at a time, therefore all devices in WSN are configured for one frequency channel and data rate. The advantage of a single-channel Gateway is about ten times cheaper transceiver and lower CPU performance requirements than standard LoRaWAN Gateway transceiver. Third-party LoRaWAN nodes are fully compatible with any LoRaWAN Gateway, so it can be deployed into this system, but it needs to be configured to communicate at the specified frequency channel and data rate. LoRaWAN protocol uses 4-byte device address for nodes. These 4 bytes and node payload are included in the communication protocol between the Gateway and the Control Panel via RS485. In the case of lack of space, the node payload is decoded in the Gateway according to node payload documentation provided by manufacturer [20] and only the required data are transmitted to the Control Panel.

In summary, when the Gateway receives an encrypted LoRaWAN packet, it looks for whether the Node device address is in the list of known device addresses. If this is the case, the packet is encoded in the communication protocol of the Gateway and sent to the Control Panel. If there is not enough space in communication protocol of the Gateway, the packet is decrypted and relevant data, i.e., sensor values, are selected.

In this design the opposite direction of communication direction is not implemented, but it can also be used to control actuators, e.g., switch, motor.

To test the proposed system design, the Gateway is built from one NUCLEO-L073RZ development board [21], RFM95w LoRa Shield [22] and RS485 transceiver [24], Fig. 4.

The NUCLEO-L073RZ development board with STM32L073RZ microcontroller is suitable for the development purposes because of its parameters,

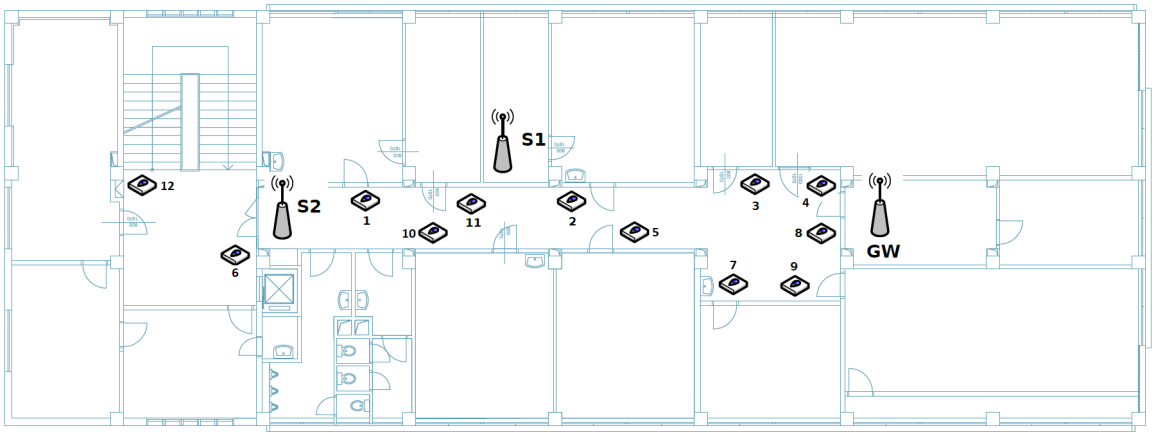

Fig. 3: Location of sensor nodes and CKP devices on the university floor

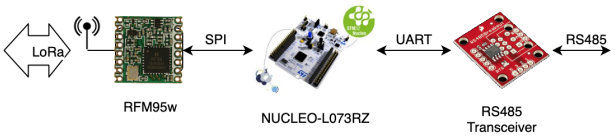

Fig. 4: Gateway block diagram, RFM95w [22], RS485 transceiver [24], NUCLEO-L073RZ [21]

Tab. 1, price and available documentation. LoRa transceiver board RFM95w with SX1276 chip integrated into Dragino LoRa Shield has the same pinout as the NUCLEO-L073RZ development board. RS485 transceiver as an RS485/UART interface enables communication with Control Panel.

Tab. 1: The STM32L073RZ features [21]

Microcontroller architecture	ARM Cortex-M0+ 32-bit RISC
Internal flash memory	192 KB
Internal SRAM memory	20 kB
Internal EEPROM memory	6 kB
CPU frequency	up to 32 MHz
Interfaces	2X SPI, 3x I2C, 4x UART, LIN

3. Measurement Results and Discussion

One floor block of university building is selected to perform the test. It is equipped with twelve CKP devices, each controlling one Door Lock and one Reader. One Gateway is added to the infrastructure, i.e., thirteen devices are connected to one RS485 network. Two temperature/humidity sensor nodes are wirelessly connected to the Gateway. The Gateway and CKP devices are connected via RS485 network as shown in Fig. 1. The specific location of CKP devices, Gateway and two sensor nodes on the floor is shown in Fig. 3.

The long-term operation test is carried out from 21^{st} September to 31^{th} October, i.e., in the period involving the presence of students and employees in the classrooms and offices on the monitored floor of the university. During this period, the Control Panel received 1 876 978 packets (14 074 522 Bytes) and sent 1 101 556 packets (8 295 219 Bytes) from/to RS485 network. The lengths of all 2 978 534 packets, i.e., 22 369 741 Bytes, are recorded in RS485 network during long-term operation test and the frequency analysis method, i.e., the number of packet lengths in monitored period, is performed. Three packets reach the largest value, i.e., 40 Bytes. Considering the total amount of packets, it is negligible quantity, i.e, 1.3E-04%. However, given the nature of the system, i.e., the system with the primary function of access to a restricted area, the worst-case scenario is considered to be an uncrossable limit. Number of sensor nodes that can be wirelessly connected to the Gateway and does not affect the existing access control system, can be calculated in dependence on used RS485 data rate. The reserve of the data rate is considered in order to protect the access control system from malfunction, e.g., a long waiting for the door to open.

Tab. 2: Packet length frequency analysis

Packet length	Count
7	**2 216 098**
8	619 127
9	3
11	58 393
13	58 620
16	1
18	2
19	**26 286**
23	1
40	3

Based on the frequency analysis given in Tab. 2 and IMA know-how, 19 Bytes length packets transmit sensor data, and 7 Bytes length packets are general aknowledgemets of IMA protocol. At least two

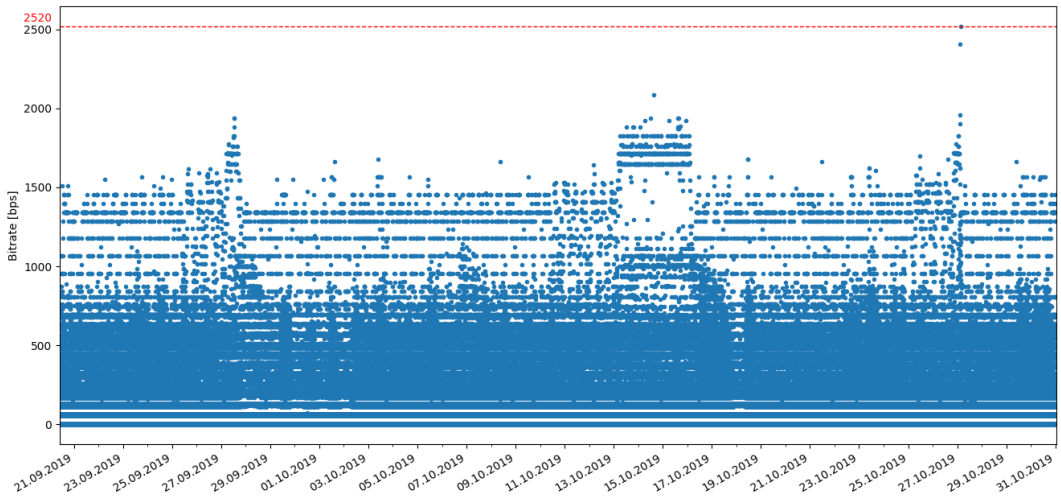

Fig. 5: Measured data rate in [bps] in RS485 network during long-term operation test

packets are required to handle sensor data via RS485 network, i.e., one carrying sensor data and the other with ackowledgement.

During long term operation test, lengths of transmitted packets (l) are captured with the accuracy of timestamps of a thousandth of a second. Then resampled to one second resolution interval using the sum function to easily represent achieved data as a bit rate in bit per second (bps), Fig. 5. Red colored dashed line (with value of 2520 bps) shows one second time interval in which a sum of captured packets is transported in RS485 network. It shows, based on detailed knowledge of the IMA protocol, less than 20% of the RS485 network capacity is used.

To avoid RS485 network congestion the maximum number of sensor nodes S_{MAX} can be calculated as:

$$S_{MAX} = \frac{\frac{v_{485}}{B}}{\frac{l_{MAX}}{P}} - R \qquad (1)$$

where:

v_{485}	485 network data rate [bps]
B	bits to Byte
l_{MAX}	maximal packet length
R	reserve of the data rate [%]
P	number of packets to transmit sensor data

Considering above mentioned limits, desired reserves and RS485 data rates, the maximum number of sensor nodes simultaneously transmitting their data on RS485 network is calculated, Tab. 3.

Values for calculation are:

v_{485}	= RS485 network data rate
B	= 8
l_{MAX}	= 40
P	= 2

Tab. 3: Maximum number of sensor nodes simultaneously transmitting their data in RS485 network with desired reserve

RS485 data rate	**Reserve** R			
v_{485} [bps]	0 %	10 %	20 %	30 %
1200	1	1	1	1
2400	3	3	3	2
4800	7	6	6	5
9600	15	13	12	10
19200	30	27	24	21
38400	60	54	48	42
57600	90	81	72	63
115200	180	162	144	126
230400	360	324	288	252
460800	720	648	576	504
921600	1440	1296	1152	1008

For example, WSN can connect up to 162 sensor nodes that work in RS485 network with a 115200 bps data rate and 10 % reserve, or up to 126 sensor nodes with a 115200 bps data rate and 30 % reserve. The results also show, one floor block of university building, i.e., one RS485 network, can operates dozens of sensors with sufficient reserve protecting the access control system from malfunction.

4. Conclusions

In this paper, the conditions of extending an existing access control system running in an industry standardized RS485 network with a wireless sensor network based on LoRaWAN single-channel mode is discussed. Design of wireless sensor network is performed, i.e., the sensor nodes and one single-channel gateway based on LoRaWAN protocol are designed. The gateway represents a type of CKP device connected to the RS485 network, therefore is supports the existing protocol in the RS485 network. A long-term operation measurement is performed in one university floor infrastructure consisting of twelve CKP devices (pairs of card reader and door lock) and one gateway. Frequency analysis of packet lengths is performed and the biggest value of packet length is considered as well as the reserve of the RS485 data rate in order to protect the access control system from malfunction. Maximum number of wireless sensor nodes simultaneously transmitting data RS485 network is calculated in dependence on RS485 data rate and the reserve of data rate, e.g., 81 sensor nodes that work in RS485 network with a 57600 bps data rate and 10 % reserve. This number of sensor nodes significantly exceeds the actual needs of the sensor nodes on one floor block of university building. Therefore we can state that WSN is suitable for smart metering applications.

Acknowledgment

This work was supported by the TA CR grant "The Multichannel Communication Platform for the Internet of Things (IoT)" TH02010568 and by the the internal CTU grant under project SGS18/183/OHK3/3T/13.

References

[1] H. Ali, W. Y. Chew, F. Khan and S. R. Weller, "Design and implementation of an IoT assisted real-time ZigBee mesh WSN based AMR system for deployment in smart cities," *2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, Oshawa, ON, 2017, pp. 264-270. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8052810 [Accessed: 9-Sep-2019].

[2] T. Malche and P. Maheshwary, "Internet of Things (IoT) for building smart home system," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, 2017, pp. 65-70. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8058258 [Accessed: 9-Sep-2019].

[3] K. Mekki, E. Bajic, F. Chaxel and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment". *ICT Express*, vol. 5, no. 1, March 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959517302953 [Accessed: 9-Sep-2019].

[4] M. Centenaro, L. Vangelista, A. Zanella and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," in *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60-67, October 2016. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7721743 [Accessed: 9-Sep-2019].

[5] A. Lavric and A. loan Petrariu, "High-Density Low Power Wide Area Networks," *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania, 2018, pp. 1-4. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8678997 [Accessed: 9-Sep-2019].

[6] A. Kosari and D. D. Wentzloff, "MURS Band for LPWAN Applications," *2019 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, Orlando, FL, USA, 2019, pp. 1-3. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8711814 [Accessed: 9-Sep-2019].

[7] KRANZ, Maclej. The Internet of Things: 5 Predictions for 2018. CISCO: blog [Online]. Available: https://blogs.cisco.com/innovation/the-internet-of-things-5-predictions-for-2018 [Accessed: 9-Sep-2019].

[8] R. F. Fernandes, C. C. Fonseca, D. Brandão, P. Ferrari, A. Flammini and A. Vezzoli, "Flexible Wireless Sensor Network for smart lighting applications," 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, Montevideo, 2014, pp. 434-439. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6860782 [Accessed: 9-Sep-2019].

[9] W. Huiyong, W. Jingyang and H. Min, "Building a Smart Home System with WSN and Service

Robot," *2013 Fifth International Conference on Measuring Technology and Mechatronics Automation*, Hong Kong, 2013, pp. 353-356. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6493740 [Accessed: 9-Sep-2019].

[10] Luo Hui, "A meter reading system based on WSN," *2010 International Conference on Optics, Photonics and Energy Engineering (OPEE)*, Wuhan, 2010, pp. 311-314. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5508121 [Accessed: 9-Sep-2019].

[11] M. J. Mudumbe and A. M. Abu-Mahfouz, "Smart water meter system for user-centric consumption measurement," *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, Cambridge, 2015, pp. 993-998. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7281870 [Accessed: 9-Sep-2019].

[12] R. K. Kodali, "Radio data infrastructure for remote monitoring system using lora technology," *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, 2017, pp. 467-472. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8125884 [Accessed: 9-Sep-2019].

[13] N. Shah and P. S. Sundar, "Smart Electric Meter Using LoRA Protocols and Iot applications," *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, 2018, pp. 1178-1180. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8474749 [Accessed: 9-Sep-2019].

[14] C. Yoon, M. Huh, S. Kang, J. Park and C. Lee, "Implement smart farm with IoT technology," *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 749-752. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8323908 [Accessed: 9-Sep-2019].

[15] Know about Access Control Systems and Their Types with Features. *Electronics projects focus* [Online]. Available: https://www.elprocus.com/understanding-about-types-of-access-control-systems/ [Accessed: 9-Sep-2019].

[16] D. Singh, O. G. Aliu and M. Kretschmer, "LoRa WanEvaluation for IoT Communications," *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, 2018, pp. 163-171. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8554713 [Accessed: 9-Sep-2019].

[17] LoRa Alliance, "LoRaWAN 1.1 Specification", version 1.1, October 11, 2017 [Online]. Available: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf [Accessed: 9-Sep-2019].

[18] A. Zourmand, A. L. Kun Hing, C. Wai Hung and M. AbdulRehman, "Internet of Things (IoT) using LoRa technology," *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, Selangor, Malaysia, 2019, pp. 324-330. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8825008 [Accessed: 9-Sep-2019].

[19] N. H. Abd Rahman, Y. Yamada, M. H. Husni and N. H. Abdul Aziz, "Analysis of Propagation Link for Remote Weather Monitoring System through LoRa Gateway," *2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN)*, Kuching, 2018, pp. 55-60. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8580479 [Accessed: 9-Sep-2019].

[20] RisingHF, "Outdoor IP64 Temperature and Humidity LoRaWAN sensor RHF1S001", version 1.2, 2015 [Online]. Available: http://www.objenious.com/wp-content/uploads/2016/10/RHF-DS01588Outdoor-IP64-Tempratrure-and-Humidity-LoRaWAN-Sensor-RHF1S001_V1.3.pdf [Accessed: 9-Sep-2019].

[21] *NUCLEO-L073RZ.* ST Microelectronics [Online]. Available: https://www.st.com/en/evaluation-tools/nucleo-l073rz.html [Accessed: 20-Sep-2019].

[22] *RFM95/96/97/98(W) - Low Power Long Range Transceiver Module.* HopeRF electronic. V1.0. [Online]. Available: http://wiki.dragino.com/index.php?title=Lora_Shield [Accessed: 20-Sep-2019].

[23] *Lora Shield.* Dragino. [Online]. Available: http://wiki.dragino.com/index.php?title=Lora_Shield [Accessed: 20-Sep-2019].

[24] *SparkFun Transceiver Breakout - RS-485* Sparkfun. [Online]. Available: https://www.sparkfun.com/products/10124 [Accessed: 20-Sep-2019].

About Authors

Tomas HYHLIK was born in Pardubice, Czech Republic. He received his Bc. degree from the Czech Technical University in Prague, Faculty of Electrical Engineering in 2017. His research interests include Internet of Things.

Marek NERUDA was born in Hradec Kralove, Czech Republic. He received the M.Sc. and Ph.D. degree in electrical engineering from the Czech Technical University in Prague, Faculty of Electrical Engineering, Czech Republic in 2007 and in 2014, respectively. Currently, he works as an assistant professor at the Department of telecommunication engineering, CTU in Prague. His research interests include RFID technology, the Internet of Things and electrically conductive textile materials.

Pavel BEZPALEC was born in Prague, Czech Republic. He received the M.Sc. and Ph.D. degree in electrical engineering from the Czech Technical University in Prague, Faculty of Electrical Engineering, Czech Republic in 1998 and in 2007, respectively. Currently, he works as an assistant professor at the Department of telecommunication engineering, CTU in Prague. His research interests include networking, (cyber)security and telephony technology.

Lukas VOJTECH was born in Nachod. He received the M.Sc. degree in electrical engineering from the Czech Technical University in Prague, Faculty of Electrical Engineering, in 2003. In 2005, he received the bachelor degree engineering pedagogy from the Masaryk Institute of Advanced Studies in Prague. In 2010, he received the Ph.D. degree from Czech Technical University in Prague, Faculty of Electrical Engineering. Currently, he works as an assistant professor at the Department of telecommunication engineering, CTU in Prague. His research interests include wireless technologies, technology RFID and mainly EMC in area of shielding materials.

Vlastimil BENES received the M.Sc. degree in electrical engineering from the Czech Technical University in Prague, Faculty of Automated control systems, Czech Republic in 1986. His research interests include RFID technology, access control systems and the Internet of Things.