Information & Security

M. Brazhenenko, V. Shevchenko, et al.
vol. 47, no. 2 (2020): 172-186
https://doi.org/10.11610/isij.4712

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Adopting Machine Learning for Images Transferred with LoRaWAN

Maksym Brazhenenko [a] (✉), *Viktor Shevchenko* [a], *Oleksiy Bychkov* [a], *Boyan Jekov* [b], *Pepa Vl. Petrova* [b], *Eugenia Kovatcheva* [b]

[a] *Taras Shevchenko National University of Kyiv, Kyiv, Ukraine*
https://pst.knu.ua/

[b] *University of Library Studies and Information Technologies, Sofia, Bulgaria*

ABSTRACT:

LPWAN (Low-power Wide-area network) networks are well-known since the 1980s, but due to low efficiency were not in active use for a long time. Modern LPWAN is a game-changing technology with true power in network coverage, cost efficiency, and low operational expenses. LPWAN services' most frequent market is in smart cities, agriculture, healthcare, and civil defence systems. LoRa is considered one of the market leaders in LPWAN; however, the low bandwidth of its physical layer makes it unsuitable for high-speed transmission. The provision of integrity, availability, and confidentiality in IoT networks is still of major concern. Data accuracy and lack of control over the transmission of personal information prevents the active use of the technology in regulated industries, such as healthcare and civil defence. In this article, we adopt LoRa for the transmission of media content, with an ability to regulate the quality of data and achieve desired level of integrity and availability. This allows the system to self-configure (train) via more reliable machine learning techniques.

ARTICLE INFO:

RECEIVED: 08 JUNE 2020
REVISED: 09 SEP 2020
ONLINE: 22 SEP 2020

KEYWORDS:

IoT, LoRa, Raspberry PI, security, cloud, machine learning

✉ E-mail: mbrazhenenko@gmail.com

Introduction

Internet of Things (IoT) denotes the concept of connected smart devices that communicate seamlessly over the Internet. As the market keeps growing, we can classify IoT solution into several major categories. The most common way to denote them is – mission-critical application and massive IoT, based on the technical and commercial requirements they prioritize. Mission-critical solutions are those which require very low latency levels on ultra-reliable networks, often combined with very high throughput. Massive IoT applications, on the other hand, refers to applications which are less latency-sensitive and have lower throughput requirements but require many low-cost, low-energy consumption devices on a network with excellent coverage.[1] The growing popularity of IoT has driven up the demand for massive IoT technologies and the number of smart devices worldwide continues to increase at a dramatic pace. The key requirements for massive IoT are long battery life, good coverage, low cost, and performance flexibility. The technology category that addressing those requirements is low power wide area network (LPWAN) technologies.[2]

Nevertheless, modern LPWAN networks being actively analysed [3] within past years still do not have appropriate information security solutions. Probably the first complete analysis of threats and vulnerabilities was published recently.[4] They figured out that LoRa devices have coexisting problems with other LoRa networks and devices. Devices using lower spreading factors can corrupt signals from devices using higher spreading factor in the same network. Furthermore, most LoRaWAN security measures such as the key management and frame counters need to be implemented and taken care of by developers or manufacturers. Therefore, poor implementation also may put end-devices and gateways in danger. A series of articles on key management for LoRa based networks [5,6] was published later advocating for key-management solutions. There was also proposed a way to secure communication for healthcare monitoring system.[7] Another great post describe interference vulnerability.[2]

Information security threats should be analysed for many aspects of IoT solutions flow including but not limiting data collection by sensors, data transmission, data transformation, and analysis. All of the described aspects should be considered as sensitive. Threats rate for the given type of system can be classified with the following order for CIA triad (given order of importance from 1 to N) – 1. Integrity, 2. Availability, 3. Confidentiality. This order is driven by the fact, that majority of issues related to confidentiality has human nature, where's integrity and availability are more technology concerns.

In this paper, we adopt image transfer via LPWAN network, with an example of LoRa as hardware, to self-configure the quality of outputs and provide reliable input for Machine Learning algorithms. We advocate for a new way to define integrity within LPWAN networks. Discover and classify existing threats and limitations for media data transfer.

Methods

We used the methodology of building security profiles based on existing standards, image compression/decompression methodologies, processing of statistical and experimental results methods, a theory of probability methods.

Security profiles for the system

Based on the existing researches on protection profiles for automated systems [8] and following the proposed way to choose protection profile it is obvious that practically possible should be implemented the following requirements [9,10] for the IoT system (Table 1).

- OR - Objects reuse
- TI - Trusted Integrity
- AI - Administrative Integrity
- R - Rollback
- DEI - Data exchange Integrity
- RI - Registration
- AA - Authorization and authentication
- TC - Trusted channel
- RS - Responsibilities separation
- IPC - Integrity of protection controls
- ST - Self-testing
- AE - Authentication on exchange.
- AS - Authentication of sender
- AR - Authentication of receiver

These five profiles allow us to achieve a majority of requirements for integrity and availability and as result leaving room to evolve into profiles that address confidentiality as well. *Data Exchange Integrity* – is the major concern within a list since media transfer in a low-throughput network is not reasonably possible with a single message and so an intelligent approach for data transfer is necessary. Another complication of integrity is coming from the angle of stream-like data for example temperature or accelerometer sensor, because in LPWAN networks some data loss are expected.

An important thing to note is that the term *integrity* in the scope of IoT communication is meant to be different from other more common web or desktop applications. Data integrity is the maintenance of, and the assurance of the accuracy and consistency of data over its life cycle. We definitely cannot evaluate integrity in the same way for majority IoT solutions due to the fact that expressed quality is not achievable for LPWAN. However, even losing the majority of data might not prevent Machine Learning algorithms to produce exactly the same outputs. Summarizing all of the above we propose to define that data integrity for the signal that was send over LPWAN network is achieved if a client (machinery) interpretation for initial signal and received has no difference.

Table 1. Protection profiles.

Requirement	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
OR				1	1
TI	1	1	1	1	4
AI			2	3	4
R		1	1	2	2
DEI	1	1	2	2	3
RI	2	2	2	3	4
AA	2	2	2	2	2
TC	1	1	1	1	1
RS	1	1	2	2	3
IPC	1	2	2	3	3
ST		1	2	2	2
AE	1	1	2	2	3
AS			1	1	2
AR				1	2

Automated systems transport layer

The transport layer obviously has a significant influence on QoS (Quality of Service) for data transmission. The latest researches in this area demonstrate that[11] TCP (Transmission Control Protocol) is slightly better than UDP (User Datagram Protocol) even in constraint environment. Another research shows that DCCP (Datagram Congestion Control Protocol) is the optimal one for media transfer.[12] Latter research shows that there is no reason to send lost package again because it will not add any value for the end-user. We advocate that this behavior is applicable to IoT (Internet of Things) as well.

The process of data transmission in IoT environment can be represented as a mathematical model of a continuous system Fig.1. One of the obvious conclusion relay in a physical behaviour of $f(t)$, representing variation of environment influence and package losing during data transmission. We propose to take the Heaviside step function[13] for $f(t)$ modelling, where $t \geq 0$ representing successful packet delivery (1):

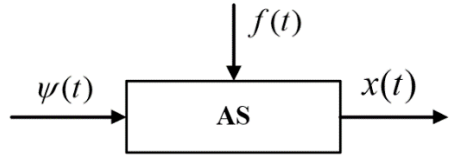

Figure 1: Automated System.

$$f(t) = \begin{cases} 0, t < 0 \\ 1, t \geq 0 \end{cases} \quad (1)$$

This allows us to formulate transformation function $\phi(t)$ (2) and it's a domain $D(\phi)$ (3) for the automated system as well:

$$\phi(t) = \frac{x(t)}{\psi(t)} = \frac{\psi(t) f(t)}{\psi(t)} + a_t f(t)^{-1} = f(t) + a_t f(t)^{-1} \quad (2)$$

where a_t is a fallback value when $t < 0$

$$D(\phi) = (-\infty, 0) \cup (0, +\infty) \quad (3)$$

Experimental data transfer setup

Data send by sensors are different in nature, frequency of sending and quality of measurement. However, the very basic classification still can be applied from the angle of a typical way to transmit data and as a result mathematical models can be created.

- Streaming data – like temperature sensors, GSM (Global System of Mobile Communications). Taking priority for the most recent data over lost packets, make huge sense for this group.
- Packet data – like image, but in a raw format: TIFF (Tagged Image File Format)
- Dynamic streaming data – accelerometer is an example. Losing packet might cause false-positive results on data analysis stage.
- Compressed or Encrypted data – any application-level data, which is encrypted or compressed.

We chose the following scenarios of interaction and $f(t)$ behaviour:
Loosing 5% of data (message sequence is not controlled) (4)

$$\phi(t) = f(t) + a_t f(t)^{-1}, a_t = 0 \quad (4)$$

A. Loosing and mixing 5% of data (message sequence is not controlled) (5)

$$\phi(t) = g(t) \tag{5}$$

B. Loosing 5% of data and replacing it with defaults (message sequence is controlled) (6)

$$\phi(t) = f(t) + a_t f(t)^{-1}, a_t \in \square, a_t \neq 0 \tag{6}$$

Figure 2: Scenario A, B and C with JPEG image.

Each individual packet sends over LPWAN (Low-power wide-area network) due to well-known constraints will not represent an image [14]. In order to compare images we should first aggregate a series of packets into a package that can be compared to the original signal (7), (8).[15]

Figure 3: Scenario C with TIFF image.

$$im = \sum_{t=0}^{n} x(t) \tag{7}$$

$$\xi = Q(im_{in}, im_{out}) \tag{8}$$

The most widely used and common ways to compare images are PSNR [16] (9), (10) and SSIM [17] (11-15) indexes:

$$PSNR = 10 log \frac{s^2}{MSE} \tag{9}$$

$$MSE = \frac{1}{nm} \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} e(m,n)^2 \tag{10}$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{11}$$

$$\mu_x = \frac{1}{\mathrm{T}} \sum_{i=1}^{\mathrm{T}} x_i \quad \mu_y = \frac{1}{\mathrm{T}} \sum_{i=1}^{\mathrm{T}} y_i \tag{12}$$

$$\sigma_x^2 = \frac{1}{\mathrm{T}-1} \sum_{i=1}^{\mathrm{T}} (x_i - \bar{x})^2 \quad \sigma_y^2 = \frac{1}{\mathrm{T}-1} \sum_{i=1}^{\mathrm{T}} (y_i - \bar{y})^2 \tag{13}$$

$$\sigma_{xy}^2 = \frac{1}{\mathrm{T}-1} \sum_{i=1}^{\mathrm{T}} (x_i - \bar{x})(y_i - \bar{y}) \tag{14}$$

$$MSSIM = \frac{1}{p} \sum_{j=1}^{p} SSIM_j \tag{15}$$

where MSSiM - Mean Structural Similarity Index Method:

$$\xi_{PSNR} = PSNR(im_{in}, im_{out}), \xi_{SSIM} = MSSIM(im_{in}, im_{out}) \tag{16}$$

Experimental results

For initial evaluation of image transfer quality and capabilities JPEG (Joint Photographic Experts Group) and TIFF (Tagged Image File Format) images were chosen to represent Zipped and Package data types. (Fig. 2, Fig. 3)

After processing images through basic scenarios, we can easily identify that JPEG being visually identically might be useless for processing engines, TIFF images for scenario A, B can't be opened because image rectangle can't be

constructed without them. Scenario C show much better results, image looks similar to the original and is a good candidate for the next processing steps. The results are outlined in Table 2 and Table 3.

Table 2. JPEG processing results.

Scenario	Description	ξ_{SSIM}	ξ_{PSNR}
A	5% Loss	0.81	11.5
B	5% Loss and Mix	0.54	7.65
C	5% Loss, Sequence Control	0.84	13.15

Table 3. TIFF processing results.

Scenario	Description	ξ_{SSIM}	ξ_{PSNR}
A	5% Loss	N/A	N/A
B	5% Loss and Mix	N/A	N/A
C	5% Loss, Sequence Control	0.96	20.7

Evaluation of ξ clearly shows several things that characterize the image transfer process in LPWAN networks, raw images like TIFF show better performance, but worst file size. Encrypted (compressed) images like JPEG have better file size but cannot tackle package lost issue. Also, it is clear enough that the absence of packet sequence control makes things even worse.

LoRa WAN Limitations and Constraints

Constant sending of huge images through the LoRa network is not really possible due to the following reasons:

- Sensors will be interfering
- Connection latency
- Other technology limitations

Sending data with a high bit rate between end nodes connected to a sensor like camera within a LoRa (Long-Range) network module [18] is highly constraint and limited. This kind of transfer is not suitable for LoRaWAN (Long-Range Wide-area network) first of all due to 1% working time (36 sec per hour) per node limit. LoRa MAC (Media access control) level responsible for data transition due to the size and encryption it uses.[15]

Experimental setups were done recently proving that one-time transfer is possible, even when the consuming node is waiting for all packets,[19] as well as prototyping in real-life environment and research on physical layer setup [15] for compressed images in JPEG format. On the baseline of this researches it is quite clear that we can formulate that data transfer success depends on the following factors:

- Distance
- Data size

Distance growth is reducing the potential maximum size of a packet that can be transferred over the network [20,15] and require increasing of a spreading factor - SF and reducing bandwidth - BW . Let's assume that probability of packet loss is $P(A_x)$, D - distance, $D_{\max}$ - maximum acceptable distance for given SF and BW and k - various factors that increasing signal like end node positioning, absence of natural barriers (17)(18)(19).

$$P(A_x) = 1 - \frac{D}{D_{\max}} + k \tag{17}$$

$$P(B_x) = 1 - P(A_x) \tag{18}$$

$$p_t = C_c^1 P(B_x)^1 P(A_x)^{c-1} = cP(B_x)P(A_x)^{c-1} \tag{19}$$

Then we can define $P(B_x)$ - as a probability of success, and with Bernoulli formula defines p_t - the probability of failure for a single packet for the package and c is a packet count. On the basis of a fact that we are describing sequence of independent events for which probability of success can be taken as the same value, we can conclude that p_t has binomial distribution and mathematical expectation (20):

$$M_p = cP(B) \tag{20}$$

Latter essentially can be re-formulated as increasing distance influence on service quality not only by risk of signal corruption but also through an increasing amount of packets to be send, however individual packet achievement probability mostly depends on other factors k .[15, 19]

JPEG 2000 Experimental results

Previous researches show that compressing with JPEG2000 has much better outputs comparing to other algorithms.[19] However, compression with this algorithm expects data loss and requires more computational time, which negatively influences power consumption. In case the amount of loss will be too huge machine learning algorithms will not be able to recognize objects on a

final image processing stage and it became useless, so a necessary level of quality control should be built.

Figure 4: Scenario C with TIFF image.

For better visibility of JPEG2000 algorithm, we choose an example with toy police machine (Fig.4). The image will be resized to 600x800 and 800x1200 dimension and then compressed to target PSNR (Point to signal noise ratio) provided as an algorithm input parameter. Table 4 and 5 represents results of compression and both ξ_{PSNR}, ξ_{SSIM}.

Keep reviewing initial objective to provide a reliable input to the machine learning algorithms, we can come to conclusion that by manipulation of input PSNR value we can regulate output quality to the necessary degree. Within a machine learning interface image can be described as a set of roots, that can be identified. There are quite a lot of algorithms that allow to perform this kind of control, one example is SURF (Speeded of robust features[21]). On this basis we propose to define number of necessary roots that verify similarity as (21)(22)(23). Roots are used as quality check, allowing to calibrate the system before it is used in intended environment.[22, 23]

Table 4. Compression 600*800.

Scenario	JPEG2000 (kb)	JPEG (kb)	ξ_{PSNR}	ξ_{SSIM}
10	1	2	12	53%
15	1	2	12	53%
25	2	63	24	74%
30	2	82	29	82%
35	21	100	34	92%
40	52	114	37	95%

Table 5. Compression 800*1200.

Scenario	JPEG2000 (kb)	JPEG (kb)	ξ_{PSNR}	ξ_{SSIM}
10	1	2	12	53%
15	1	2	12	53%
25	2	63	24	74%
30	2	82	29	82%
35	21	100	34	92%
40	52	114	37	95%

$$\lambda = \upsilon(x) \;\; \lambda_1 = \omega(\upsilon(x)) \tag{21}$$

$$\eta = Z(\lambda, \lambda_1) \tag{22}$$

$$\xi = \lambda - \eta, \xi \geq 0, \xi \in [0, \lambda], \xi \in \mathrm{N} \tag{23}$$

where λ, λ_1 - functions describing roots before and after compression, $\omega(x)$ - compression function, η - matching roots, ξ - roots loss, then the quality barrier can be set as :(24)

$$p = \frac{\xi}{\lambda}, k_{\min} \leq p \leq 1, p \in [0,1], \lambda > 0 \tag{24}$$

where $k_{\min}$ is either machinery regulated value or human input.

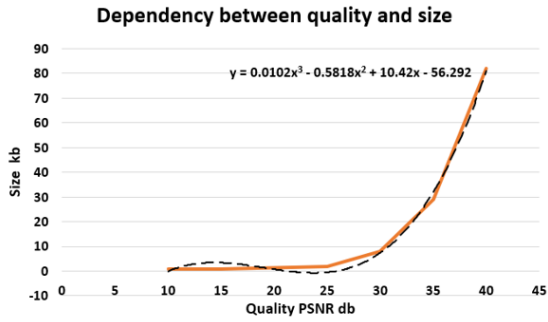

Figure 5: Dependency between quality and size.

Fig. 5 demonstrates how increasing image quality influence on result file size, the most interesting thing is that relation for both image sizes is close to identical. Also, it is quite easy to see that for all $PSNR \in [1,100], PSNR \in \mathrm{N}$ there is such a value that for all less ξ_{SSIM} is growing much faster and for all greater vice versa. This is a clear indication that once you achieve some level of quality, getting more is going to cost doubling network traffic and as a result making whole technology useless. That can be reformulated as increasing file size is decreasing QoS of a system, and so the goal is to keep it at bare possible minimum. Each individual case might have its own optimum value based on particular product, however we already can state that defining that value is an iterative process that can be described in the following way(25).[24, 25]

$$\begin{cases} y_{i+h} = y_i + h, h \in [0,100], h \in N \\ \vec{x}_{y+h} = \dfrac{\xi_{y+h}}{\lambda_{y_0}}, x_{y+h} \geq k_{\min} \end{cases} \tag{25}$$

Conclusions

In this paper we evaluate definition of integrity for IoT networks. We advocate that for IoT solutions integrity could not be achieved within its traditional meaning and so we should apply less restrictive requirement and rely on data similarity – ability of the system to interpreter input and modified signal in a same way. We believe that reliable Machine Learning inputs for image data send over LPWAN networks can be achieved by iterative calibrating of the end-node based on the specific needs of the product, comparing of necessary roots within an image from input and modified signal and validating impact of deviation. Difference between number of roots can be used as a data quality check. We reviewed transport layer of an automatic system and define a mathematical model for signal transformation, interesting point is that compression of data in any manner with stream algorithm increase the probability of losing the whole image, however raw or block algorithms empowered with message sequence technique can accept data losses during transfer.

Acknowledgements

This work is supported by PPNIP-2020-03/09.03.2020 "Extraction, processing and analysis of parametric data from external devices" and Project Bulgarian Supercomputer Centre: A High-Performance Infrastructure for Computer Modelling, Simulation and Research with Application in Industry, Medicine, Pharmaceutics, Energetics, Transportation, Finances and Environment Protection, Contract № D01-30/08.04.2011 with Ministry of Education, Youth and Science. 2011-2012.

References

[1] Galina Panayotova, Georgi Dimitrov, and Dimitar Dimitrov, "Wireless Sensors for Analysis Transport Systems," *Journal of Communications* 13, no. 1 (2018): 40-44,

https://doi.org/10.12720/jcm.13.1.40-44.

2 Kia C. Wiklundh, "Understanding the IoT technology LoRa and Its Interference Vulnerability," *2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, *IEEE,* 2019, pp.533-538, https://doi.org/10.1109/EMCEurope.2019.8871966.

3 Georgi Dimitrov, Galina Panayotova, Eugenia Kovatcheva, Daniela Borissova, and Pavel Petrov, "One Approach for Identification of Brain Signals for Smart Devices Control," *Journal of Software* 13, no. 7 (2018): 407-413, https://doi.org/10.17706/jsw.13.7.407-413.

4 Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence, and Danny Hughes, "Exploring the Security Vulnerabilities of LoRa," *2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, IEEE*, 2017, pp. 1-6, https://doi.org/10.1109/CYBConf.2017.7985777.

5 Weitao Xu, Sanjay Jha, and Wen Hu, "LoRa-Key: Secure Key Generation System for LoRa-Based Network," *IEEE Internet of Things Journal* 6, no. 4 (2019): 6404-6416, https://doi.org/10.1109/JIOT.2018.2888553.

6 Jinyu Xing, Lu Hou, Kuan Zhang, Kan Zheng, "An Improved Secure Key Management Scheme for LoRa System," *2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, China,* IEEE, 2019, 296-301, https://doi.org/10.1109/ICCT46805.2019.8947215.

7 Anto Merline Manoharan and Vimalathithan Rathinasabapathy, "Secured Communication for Remote Bio-Medical Monitoring System Using LoRa," *Sensor Letters* 17, no. 11 (2019): 888-897, https://doi.org/10.1166/sl.2019.4146.

8 Vladimir Tolubko, O. Kurchenko, and Alina Shevchenko, "Stabilization of the Functional Stability of the Information System by Controlling the Dynamics of Security Profiles," *Modern Information Security* 3 (2018): 51-57, https://doi.org/10.31673/2409-7292.2018.035157.

9 "Classification of Automated Systems and Standard Functional Profiles for the Protection of the Processed Information from Unauthorised Access," ND TZI 2.5-005-99, Special Telecommunications Systems and Information Protection Department, Security Council of Ukraine, 1999 (in Ukrainian).

10 "Criteria for Assessment of the Protection of Information in Computer Systems from Unauthorised Access," ND TZI 2.5-004-99, Special Telecommunications Systems and Information Protection Department, Security Council of Ukraine, 1999 (in Ukrainian), p. 22.

11 Fahad AL-Dhief, Naseer Sabri, Abdul Latiff, Nik Noordini Malik, Musatafa Albader, Mazin Mohammed, Rami AL-Haddad, Yasir Salman, Mohd Ghani, and Omar Obaid, "Performance Comparison between TCP and UDP Protocols in Different Simulation Scenarios," *International Journal of Engineering & Technology 7,* no. 4.36 (2018): 172-176, https://doi.org/10.14419/ijet.v7i4.36.23739.

12 Shahrudin Awang Nor, Raaid Alubady, Wisam Abduladeem Kamil, "Simulated performance of TCP, SCTP, DCCP and UDP protocols over 4G network," *Procedia Computer Science* 111 (2017): 2-7, https://doi.org/10.1016/j.procs.2017.06.002.

13 Duangkamon Baowan, Barry James Cox, Tamsyn Hilder, James Hill, Ngamta and

Thamwattana, "Mathematical Preliminaries," In: *Modelling and Mechanics of Carbon-Based Nanostructured Materials* (Elsevier, 2017), 35-58, https://doi.org/10.1016/B978-0-12-812463-5.00002-9.

[14] TheThingsNetwork, "The Things Network 2016 Update," https://speakerdeck.com/wienke/the-things-network-2016-update.

[15] JAkram Jebril, Aduwati Sali, Alyani Ismail, and Mohd Fadlee Rasid, "Overcoming Limitations of LoRa Physical Layer in Image Transmission," *Sensors* 18, no. 10 (2018): 3257, https://doi.org/10.3390/s18103257.

[16] PSNR, https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[17] Zhou Wang, Alan Bovik, Hamid Rahim Sheikh, and Eero P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Transactions on Image Processing* 13, no. 4 (2004): 600-612, https://doi.org/10.1109/TIP.2003.819861.

[18] LoRa, https://www.semtech.com/lora.

[19] Ruslan Kirichek, Van-Dai Pham, Aleksey Kolechkin, Mahmood Al-Bahri, and Alexander Paramonov, "Transfer of Multimedia Data via LoRa," *Lecture Notes in Computer Science,* vol. 10531, Springer, Cham (2017): 708-720, https://doi.org/10.1007/978-3-319-67380-6_67.

[20] Alexandru Lavric, "LoRa (Long-Range) High-Density Sensors for Internet of Things," *Journal of Sensors,* Special Issue (2019): 1-9, https://doi.org/10.1155/2019/3502987.

[21] David G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," *International Journal of Computer Vision* 60, no. 2 (2004): 91-110, https://doi.org/10.1023/B:VISI.0000029664.99615.94.

[22] Galina Panayotova, Georgi Dimitrov, Pavel Petrov, and Bychkov Os, "Modeling and data processing of information systems," *2016 Third International Conference on Artificial Intelligence and Pattern Recognition (AIPR), Lodz, Poland,* 2016, pp. 1-5, https://doi.org/10.1109/ICAIPR.2016.7585229.

[23] Georgi Dimitrov, Galina Panayotova, Eugenia Kovatcheva, Daniela Borissova, and Pavel Petrov, "One Approach for Identification of Brain Signals for Smart Devices Control" *Journal of Software* 13 no. 7 (2018): 407-413.

[24] Georgi Dimitrov, Bychkov Os, and Pavel Petrov, "One Approach for Analysis of Fuzzy Linear Hybrid Automata," *Izvestia, Journal of the Union of Scientists - Varna*. *Economic Sciences Series* 7 no. 2 (2018), pp. 234-240.

[25] Georgi P. Dimitrov, Magdalena Garvanova, Eugenia Kovatcheva , Kristian Aleksiev, and Inna Dimitrova, "Identification of EEG Brain Waves Obtained by Emotive Device," *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, 5-7 June 2019, https://doi.org/10.1109/ACITT.2019.8779861.

About the Authors

Maksym. **Brazhenenko,** software engineering consultant, working on different products last 15 years. Brazhenenko is Student of Information Technology

Faculty National University of Kyiv. Research interests: Internet of Things, Internet of Everything, mathematical modelling, Machine Learning, Data Processing, Algorithms. https://orcid.org/0000-0002-0036-6470.

Viktor **Shevchenko**, Dr.Sc., Professor of Software System and Technologies Department of Taras Shevchenko National University of Kyiv. Was a Director of Educational Scientific Institute of Defence of Information in State University of Telecommunication; Head of National Scientific Research Centre for Defence Technologies and Military Security of Ukraine; Head of scientific support of the implementation of a number of information-analytical systems of defence planning and management of defence resources (6 of which have been adopted in Armed Forces). Research interests: Internet of Things, Internet of Everything, mathematical modeling, cybersecurity, sensors.

Oleksiy **Bychkov**, Dr.Sc., Associated Professor, Head of Software System and Technologies Department of Taras Shevchenko National University of Kyiv. Proposed a new algorithm for studying the stability of stationary states of hybrid automata. Solved an open problem about the necessary and sufficient conditions for the existence of a positive matrix, which is the solution of the matrix Lyapunov equation on a cone. Research interests: Internet of Things, Internet of Everything, mathematical modelling of physics of natural phenomena, computer science.

Pepa Vl. **Petrova**, Dr., Assistant professor at University of Library Studies and Information Technologies. Her interests are in Data Analytics, Data Storages, Data Visualization, Business Intelligence, Artificial Intelligence, Machine Learning and Information Systems. She has more than 10 years of experience in real business projects. She is a certified trainer on ERP systems and Business Intelligence. She has been a visiting lecturer at universities in UK and Spain. She leads the ICT sector at Youth Academy for Knowledge Management at ULSIT.
Scopus Author ID: 57192371738.

Boyan **Jekov**, PhD eng., Associated Professor in Informatics and Computer Science in "Computer Science" department, Vice-dean of "Information Science" faculty at ULSIT - University of Library Studies and Information Technologies, Sofia, Bulgaria, Bulgarian program committee member (PCM) of Information and Communication Technologies (ICT) at EU science program Horizon 2020. Scientific areas – Applied ICT in public sector and business, Internet of things, cyber security.

Eugenia **Kovatcheva**, Assoc. Prof. at the University of Library Study and Information Technologies. She is a Research policy Director. Her areas of interest are Interdisciplinary applied research and innovation, Digital Repository, Information, Knowledge and Innovation Management, and Cyber Security. Dr. Kovatcheva has participated in more than 70 EU and National projects for transfer of innovations in ICT in education and smart services. In more than 70 papers and seven students' textbooks, she has shared her experience in applying the ICT under the specific objectives. Eugenia has been a visiting lecturer at universities in Japan, Kazakhstan, UK, Italy.