Journal of Modern Technology and Engineering
Vol.6, No.3, 2021, pp.219-229

MODELING AND SELECTION OF OPTIMAL PARAMETERS OF SECURITY GATEWAYS TO PROTECT INDUSTRIAL EQUIPMENT FROM CYBERATTACKS

Igor Sh. Nevludov , Murad A. Omarov* , Sergiy P. Novoselov

Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv National University of Radio Electronics Kharkiv, Ukraine

Abstract. This paper presents the methodology and results of modeling the wireless protective gateway for the industrial automation network. The analysis is carried out for technologies that are the combination of the existing industrial equipment with new modern technologies from cloud computing. The basic components for construction of a network of intelligent devices according to the concept of Industry 4.0 are defined. The requirements to the architecture of building a network of wireless devices using IoT technology are analyzed. To combine with network sensors, it is proposed to use LoRaWAN modems to build as well as a LoRa gateway. The mathematical substantiation of the method of calculation of the gateway bandwidth is given. The description of the principle of the organization of message exchange by means of LoRa modules is given. Modeling and selection of optimal parameters of the IoT gateway, using the tools LoRa Modem Calculator, Channel Activity Detection.

Keywords: Cybersecurity, LoRaWAN, IoT, Security Gateways, Industrial Control Systems.
Corresponding author: Murad A. Omarov, Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv National University of Radio Electronics Kharkiv, Ukraine, e-mail: *murad.omarov@nure.ua*
Received: 2 September 2021; Revised: 12 November 2021; Accepted: 5 December 2021; Published: 30 December 2021.

1 Introduction

Automated control systems of technological process (ACS TP) are an integral part of almost any production process in modern enterprises. As a rule, ACS TPs have higher levels of risk compared to corporate information systems.

It is worth noting the current trend of implementing the concept of Industry 4.0 in enterprises and the widespread use of wireless networks. Industrial Internet of Things (IIoT) is a system of integrated computer networks and connected industrial (production) facilities with built-in sensors and software for data collection and exchange, with the possibility of remote control and management in an automated mode, without human intervention (Boyes et al., 2018).

IoT-devices allow real-time monitoring of production lines, identify problems, obtain information about the necessary preventive measures and maintenance. In order for networked devices to work effectively and generate the information needed for analytics, the company must ensure the connectivity of its operations and machines. That is, operational technologies (OT) must function in harmony with information technologies (IT), and equipment must be connected to the human-machine interface so that professionals can work with information.

The industry uses a variety of equipment that requires separate communication channels to exchange information. Depending on the type of equipment and application, the network transmits different amounts of data. Depending on the type of network, special equipment is used. Gateways, routers, and routers are used in high-load, high-volume networks.

Table 1: Classification of wireless networks by type of transmitted messages

The type of message being transmitted	**The amount of information transmitted**	**Application example**
1. Data stream, streaming video	Large (Megabytes)	Real-time technological equipment management, technological process status monitoring, intelligent video surveillance systems
2. JSON messages, text data	Medium (Kilobytes)	Security systems, smart home system
3. Fragments of the message frame, equipment status.	Small (bytes)	Energy consumption accounting systems, burglar alarm systems, smart home system

Gateways in IoT networks provide the connection of devices and data analytics to IoT devices, which usually do not have these capabilities. Any gateway can use IoT modules to perform analysis or pre-processing before sending messages from slave devices to the Internet of Things.

2 Classification of Wireless Networks Depending on the Volume of Information Transmitted

The industry uses a variety of equipment that requires separate communication channels to exchange information. Depending on the type of equipment and scope, the network transmits different amounts of data (Drobotun, 2017). Table 1 shows examples of the use of wireless networks by various software tools.

As can be seen from Table 1 by the type of messages transmitted, we can distinguish three types of networks used in industry.

The first type of network - large data streams are transmitted. These can be video streams, continuous data streams received from industrial equipment, telemetry. Such networks are used in the management of technological equipment in real time, monitoring the state of the technological process, intelligent video surveillance systems.

The second type of network - text messages are transmitted, the so-called JSON-messages which contain information obtained during the operation of industrial equipment. Typically, this amount of information is a few kilobytes of data. Such networks are used in intelligent security systems, smart home systems, and industrial automation in the case of remote adjustment of equipment.

The third type of network - very short messages is transmitted. The amount of data is a few bytes of information. For example, this could be a command to turn on the lights, or turn off the sensor. Such networks are used in the system of the account of the consumed energy resources, the system of the security alarm system, system of the smart house.

3 Simulation of Cyber Threats of ACS TP

The model for protection of the automated system against computer attacks is an abstract (formalized or informal) description of a set of software and hardware or organizational measures of protection (detection, counteraction, elimination of consequences) against computer attacks (Boyes et al., 2018).

In the most general form, the model of the protection process can be represented as shown in Figure 1 (Boyes et al., 2018; Drobotun, 2017; Astakhov, 2002; Cybersecurity of industrial systems: a landscape of threats, 2016; Snitkin, 2015).

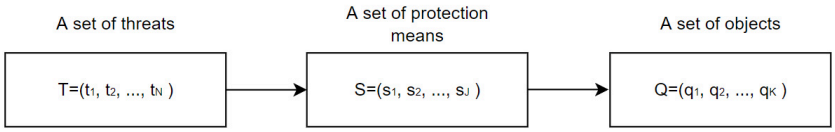

Figure 1: General model of the process of protection against computer attacks

This model is called "formal security model with full overlap". The model considers the interaction of "protected area", "threat area" and "security means":

$T = t_1; t_2; \ldots t_N$ – a set of security threats;

$S = s_1; s_2; \ldots s_j$ – a set of security means;

$Q = q_1; q_2; \ldots q_k$ – a set of protection objects.

The elements of these sets are in a certain relationship, to describe which it is advisable to use a graph representation (Figure 2).

The set of "threat-object" relations is described by a bipartite graph TQ. The purpose of protection is to block all possible edges in the graph. This is achieved by introducing a third set S resulting in a three-part graph TSQ. In a secure system, all edges of the graph are represented as $< t_n; s_j >$ and $< s_j; q_k >$. Any rib $< t_N; q_k >$ identifies an unprotected object.

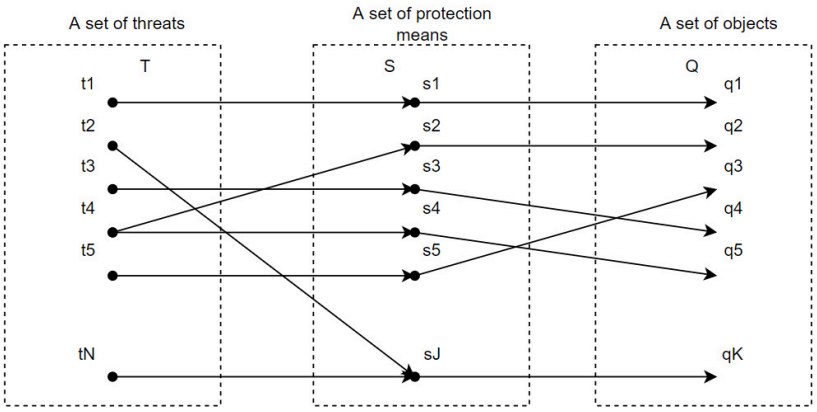

Figure 2: Graph representation of the relationship between the many security threats, security tools, objects of protection

In the security model with full overlap, the condition of full security is met:

$$\forall t_n \in T, \exists s_j \in S, \tag{1}$$

meaning that for each threat tn from the set of threats T there is a means of ensuring s_j from the set S. blocking the path of implementation of this threat to the object of protection q_k.

Expansion of the presented model with full overlap involves the inclusion of many vulnerabilities of objects of the automated system and many barriers, which are ways to implement threats, blocked by means of protection (Cybersecurity of industrial systems: a landscape of threats, 2016). In addition to many vulnerabilities and barriers, the advanced model includes many computer attacks, which are a way to implement threats to ACS.

This model can be represented as a graph $Pr = \{K, T, S, B, V, Q\}$ (Figure 3), where K is the set of computer attacks; T is a set of threats, S is a set of means of protection; Q – a set of objects of protection (components and information resources) of the automated control system:

$$V = KTQ = \{\upsilon_l =< k_m; t_i; q_n >, l = \overline{1; L}\}$$

a set of vulnerabilities of ACS objects, which are a way to implement the i-th threat to the j-th object with the help of the m-th computer attack;

$$B = VS = KYQS = \{b_k =< k_m; t_i; q_n; s_j >, k = \overline{1; K}\}$$

a set of barriers in which protection is required.

For this model, the condition of complete overlap is described as follows:

$$\forall v_l \in V, \exists(b_k =< k_m t_i q_n s_j >) \in B \tag{2}$$

This condition means that for each vulnerability v_{-l} from the set V the barrier b_k from the set B is created by the means of protection s_j from the set S, thereby eliminating the vulnerability v_{-l}, which makes it impossible to realize the threat t_i from the set T by a cyberattack k_m from the set K.

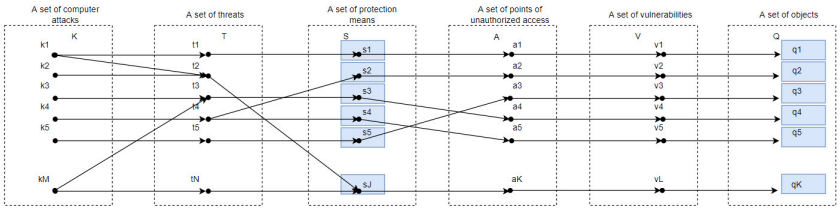

Figure 3: Advanced model of protection against cyber attacks, taking into account vulnerabilities and security gateways

The extended model of protection with full overlap, despite its correctness from the formal point of view, has significant limitations for its practical application, the main of which are (Boyes et al., 2018; Drobotun, 2017; Astakhov, 2002; Cybersecurity of industrial systems: a landscape of threats, 2016):

- the difficulty of identifying the full range of threats and vulnerabilities for a particular automated system;
- lack of possibility to quantify the level of security;
- lack of possibility to conduct a safety analysis on the criterion of "efficiency-cost".

To overcome these difficulties in practice, two approaches are used: regulatory-guaranteed (classification) and based on risk analysis (risk-oriented).

4 Analysis of the Functional Purpose of Iot Device Security Gateway

Gateways in IoT networks provide secure connection of devices and data analytics to IoT devices, which usually do not have these capabilities (Snitkin, 2015; Morris et al., 2015; Brändle & Naedele, 2008; Bhamare et al., 2020; Novoselov, 2018 ; Novoselov & Donskov, 2017).

There are three patterns for using an IoT device as a gateway: transparency, protocol conversion, and authentication conversion.

The main difference between the templates is that the transparent gateway transmits messages between the slave devices and the Internet of Things without requiring additional processing. However, the conversion of the protocol and the conversion of confirmation fragments requires the processing of this data by the gateway to ensure interaction between devices.

Any gateway can use IoT modules to perform analysis or pre-processing before sending messages from slave devices to the Internet of Things.

In the transparent gateway template, devices that could theoretically connect to the Internet of Things can connect to the gateway device. Slave devices have their own Internet of Things

Center certificates and use any of the MQTT, AMQP, or HTTP protocols. The gateway simply provides interaction between the devices and the Internet of Things.

Figure 4 shows the principle of operation of the gateway in the format "Transparent template".

Figure 4: The principle of the gateway in the format "Transparent template"

The protocol conversion gateway is also called an opaque gateway as opposed to a transparent gateway template. In this template, devices that do not support MQTT, AMQP, or HTTP can use the gateway device to send data to the Internet of Things on their behalf.

The gateway understands the protocol used by the slave devices and is the only device with an ID in the Internet of Things Center. All information looks as if it comes from a single device, a gateway.

Slave devices must embed additional credentials in the message if cloud applications need to analyze data for each device separately. In addition, IoT primitives, such as duplicates and methods, are only available for gateway devices (they are not available for slave devices).

Figure 5 shows the principle of operation of the gateway in the format "Protocol Transformation".

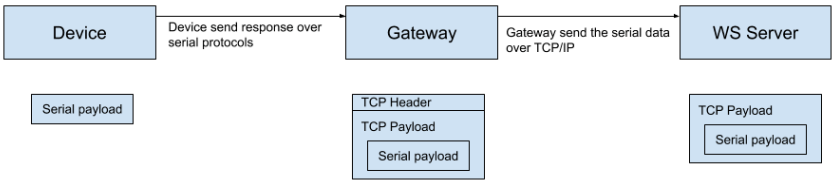

Figure 5: The principle of the gateway in the format "Protocol Transformation"

In the Gateway Conversion Template, devices that cannot connect to the Internet of Things Center can connect to the gateway device. The gateway provides Internet of Things Center credentials and provides protocol conversion on behalf of slave devices. The gateway recognizes the protocol used by the slave devices, provides credentials, and converts the Internet of Things primitives. Slave devices are displayed in the Internet of Things as first-class devices with duplicates and methods.

Figure 6 shows the principle of operation of the gateway in the format of "Translation of certificates".

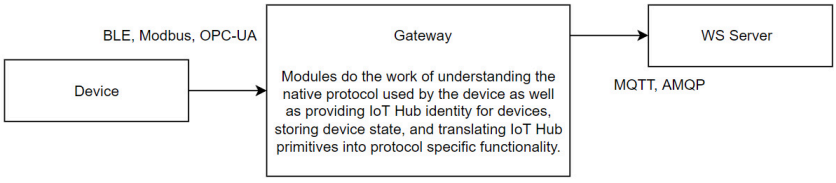

Figure 6: The principle of operation of the gateway in the format of "Transmission of certificates"

5 Modeling and Selection of Optimal Parameters of IoT Gatework Operation

To model the operation of the gateway, it is necessary to determine the principle of packet transmission. The total transmission time and power consumption depend on the change of the module parameters responsible for the transmission and reception modes. By changing these parameters, you can choose the optimal mode of operation of the LoRa module to solve the problem and set the module to the minimum level of energy consumption, which will provide maximum operating time of the device from autonomous power supply (Novoselov & Donskov, 2016; Novoselov et al., 2019; Nevludov et al., 2020; Rubio et al., 2019; Junejo et al., 2021).

To organize messaging at the physical level, data blocks are transmitted between the end device (End Node) and the LoRa gateway (Gateway).

The following steps are performed on the transmitting side:

– receiving a block of data from the upper hardware level (PHYPayload);

– formation of the physical header of the packet (PHDR + PHDR_CRC);

– encoding the physical header of the packet (PHDR + PHDR_CRC) with a fixed speed of 4/8;

– calculation of the checksum of the block of useful data PHYPayload (CRC);

– encoding of a block of useful data (PHYPayload + CRC) with a preset CR speed;

– transmission of the preamble by radio;

– modulation and radio transmission of the physical data block.

The receiving device performs:

– detection of the preamble and determination of the beginning of the physical data block;

– signal demodulation; decoding the physical packet header (PHDR + PHDR_CRC) and checking its checksum; decoding the block of useful data (PHYPayload + CRC) and checking its checksum;

– confirmation of the received data (for the corresponding types of messages);

– data transfer to the upper level of the module for further use by end devices.

The general view of the LoRa package is shown in Figure 7 and consists of three elements (Mumtaz et al., 2017; Leonardi et al., 2018; Blenn & Kuipers, 2017; Yeoh et al., 2018; Debus & Axonn, 2006; Lim & Han, 2018): preamble; optional title; payload. The preamble is used to synchronize the receiver with the input stream. By default, the packet is set to a sequence of 12 characters. This is a programmable variable, so the length of the preamble can be increased, for example, to reduce the duty cycle of the receiver in intensive reception programs. The length of the transmitted preamble can be changed by setting the PreambleLength case from 6 to 65535, obtaining a total preamble length of $6 + 4$ *to* $65535 + 4$ characters. This allows you to pass almost arbitrarily a long preamble sequence.

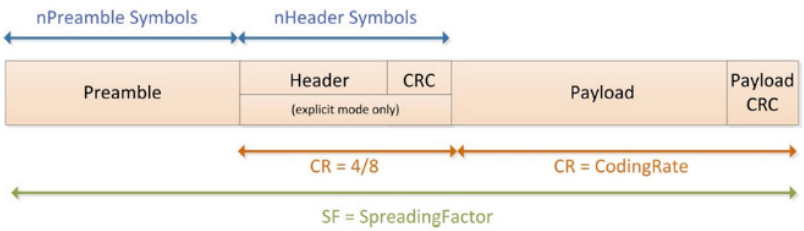

Figure 7: The structure of the data packet of the LoRa package

Next, we will simulate different options for building a data package in order to determine the optimal format for a particular task.

The receiver performs the preamble detection process, which is periodically restarted. For this reason, the length of the preamble must be set identical to the length of the preamble of

the transmitter. If the preamble length is unknown or can vary, the maximum preamble length must be programmed on the receiver side.

Depending on the selected mode of operation of the LoRa module, two types of headers are available: explicit mode; implicit mode.

The principle of transmitting the information symbols of the physical layer data block using the broadband radio signal LoRa is the frequency shift

$$e^{j\cdot\Delta\omega\cdot k\cdot t}$$

relative to the reference signal

$$e^{j\cdot(\omega_n\cdot t+\mu\cdot t^2)},$$

where $k = 0, 1, 2, \ldots, 2SF$ - information symbol, dimension SF bits (Junejo et al., 2021; Hamdi et al., 2021; Amichi et al., 2020; Premsankar et al., 2020; Specification, 2018; Mumtaz et al., 2017; Leonardi et al., 2018; Blenn & Kuipers, 2017; Yeoh et al., 2018; Debus & Axonn, 2006; Lim & Han, 2018).

Thus, the function $x(t)$ is written as follows:

$$x(t) = \begin{cases} A_0 * cos\left(\omega_H * t + \Delta\omega * k * t + \frac{\mu}{2} * t^2\right), & 0 \le t < T_0 \\ A_0 * cos\left(\omega_H * t + \Delta\omega * k * t - BW * t + \frac{\mu}{2} * t^2\right), & T_0 \le t \le T_{sym} \end{cases} \quad (3)$$

where BW is the width of the spectrum of the radio signal; $k = 0, 1, 2, \ldots, 2SF$ - information symbol, dimension SF bits; $T_{sym} = 2SF \,/\, BW$ - duration of the radio signal; $\mu = BW \,/\, T_{sym}$ - rate of change of radio signal frequency; t is the transmission time of the data unit; ω_H is the frequency of the radio signal.

An example of the radio signal frequency dependence on time for the data frame is shown in Figure 8.

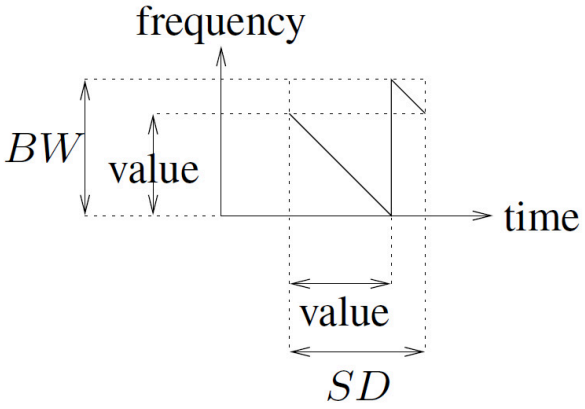

Figure 8: Example of the radio signal frequency dependence on time for the data frame

The work simulation is performed using LoRa Modem Calculator software from Semtech (Junejo et al., 2021). The initial conditions are as follows: transmission $interval = 1\ s.$; $battery\ capacity = 1000\ mAh$; $supply\ voltage = 3.3V$; $operating\ frequency = 433mHz$.

Payload size can vary between $7 - 3$ *bytes*. We performed simulation of the device for these parameters. The simulation results are listed in Table 2.

Figure 9 shows the simulation result in LoRa Modem Calculator for Periodic Receiver mode.

Figure 10 shows the simulation result in LoRa Modem Calculator for Periodic Transmitter mode.

Table 2: Results of simulation of work of the module of receipt / transmission of data at different sizes of the payload field

Payload, byte	**7**	**6**	**5**	**4**	**3**
SF = 12, BW = 125 kHz, CR = 4/5, Header Enabled, Preamble = 10.25 Symb, Payload = 7 Bytes, TR Power = 14 dB					
Time on the air, ms	925,7	761,86	761,86	761,86	761,86
Symbol transmission time, ms	32,77	32,77	32,77	32,77	32,77
Current consumption during transmission, mA	44	44	44	44	44
Receiver sensitivity, dB	-138	-138	-138	-138	-138
Approximate battery life, days	80,54 1,02	80,54 1,24	80,54 1,24	80,54 1,24	80,54 1,24
CAD, ms	61,1	61,1	61,1	61,1	61,1

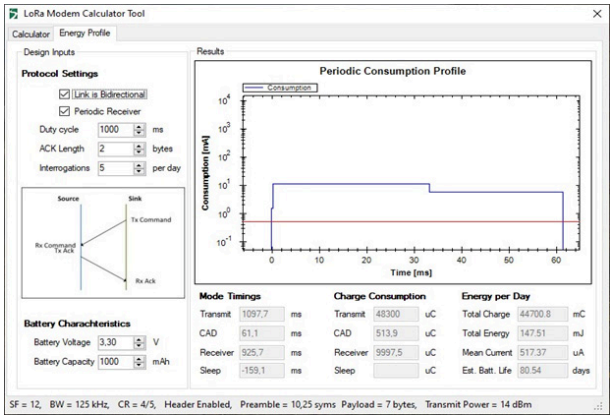

Figure 9: Simulation result in LoRa Modem Calculator for Periodic Receiver mode

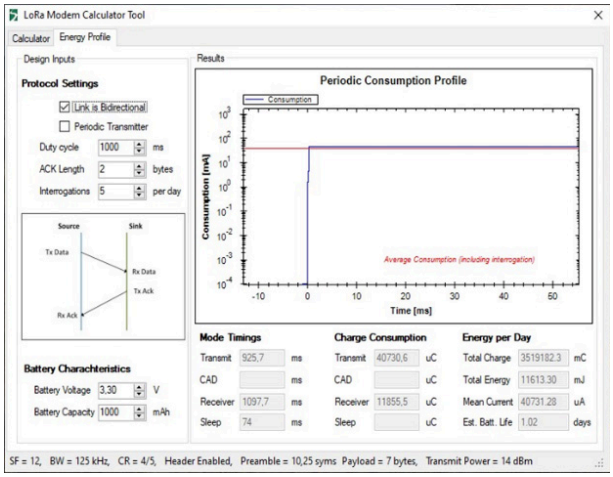

Figure 10: Simulation result in LoRa Modem Calculator for Periodic Transmitter mode

6 Conclusions

Based on the analysis of the data exchange protocol, we can conclude that to reduce power consumption and reduce airtime, you can make a variable frame length. For example, you only need 4 bytes to control the availability of a device (remove empty data fields and cell addresses from the log). By reducing the length of the data field, we reduce the time spent on the air from 925.7 to 761.86 ms. The current consumption does not decrease. Thus, we need to find other parameters that will allow us to extend the battery life.

Another parameter that can change the consumed properties of the module is the presence or absence of header and checksum fields. The influence of these parameters is determined for two values of the data field size: 7 and 4 bytes.

In total, several different simulations were performed: modeling of the module of reception / data transmission at different frame sizes; modeling of the module of reception / data transmission at different values of the CR parameter; simulation of the SX-1278 device for different values of the SF parameter.

As a result of these studies, the LoRa Modem Calculator was used to determine the values of the parameters at which the maximum energy efficiency and speed of the protective gateway are achieved. All studies were performed to transmit a 7-byte packet (Spreading factor = 6; the size of the Payload data field = 7; no header field; no checksum field; encoding type CR = 4/5), and to transmit a packet of 4 bytes (Spreading factor = 6; size of data field Payload = 4; field of header is absent; field of checksum is absent; CR = 4/5). The simulation results were evaluated for three bandwidth values of 125, 250 and 500 kHz.

The simulation results showed that the condition in the air up to 1% of the time of the active cycle for the size of the data field, the size of the data field Payload = 7 or 4 meet the following parameters: $Spreading\ factor\ =\ 6;\ BW >=\ 250\ kHz$; header field is missing; no checksum field; $CR\ =\ 4/5$.This article is written by the development of a protective gateway for IoT devices. This device is actually collected and performs the functions assigned to it.

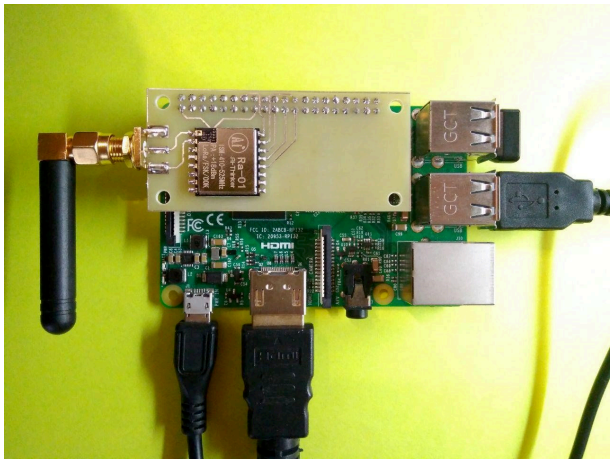

Figure 11: Appearance of a protective gateway layout for IoT devices

The gateway performs the functions of protecting the IoT devices network according to the method of "transformation of protocols" described in the article. That is, the "non-transparent" gateway receives external data packets, analyzes them and removes dangerous inserts from these packages. Further, within the protected sub-network, we can already trust those packages that are distributed from the gateway to the IoT devices and in the reverse side.

Removing the header fields and the control amount at the level of the hardware exchange protocol in the internal protected network segment is a forced effect to reduce the energy consumed by devices and an increase in battery life. This opportunity is provided by the organization of the LoraWAN network and used us for laboratory research. Determination of the correct data is provided on the side analyzing these data using machine learning methods to detect false parameters. There is currently a study for confirmation, or possibly refuting this theory. The results of this study are also planning to publish.

References

Amichi, L., Kaneko, M., Fukuda, E.H., El Rachkidy, N., & Guitton, A. (2020). Joint allocation strategies of power and spreading factors with imperfect orthogonality in LoRa networks. *IEEE Transactions on Communications*, *68*(6), 3750-3765.

Astakhov, A. (2002). Analysis of the security of corporate systems [Electronic resource]. *Open systems. DBMS.,* *7*(8), 1LI: http://www.osp.ni/os/2002/07-08/181720.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, 89, 101677.

Blenn, N., & Kuipers, F. (2017). LoRaWAN in the wild: Measurements from the things network. arXiv preprint arXiv:1706.03086.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, 101, 1-12.

Brändle, M., & Naedele, M. (2008). Security for process control systems: An overview. *IEEE Security & Privacy*, *6*(6), 24-29.

Cybersecurity of industrial systems: a landscape of threats [Electronic resource]. (2016). Kaspersky Lab., URL: https: //seciuelist.m/industiial-cybersecurity-tlueat-landscape/28866 .

Debus, W., & Axonn, L. (2006). RF path loss & transmission distance calculations. Axonn, LLC.

Drobotun, E.B. (2017). Theoretical foundations of building systems of protection against computer attacks for automated control systems. *Science-intensive Technologies*, 120.

Hamdi, R., Baccour, E., Erbad, A., Qaraqe, M., & Hamdi, M. (2021). LoRa-RL: Deep Reinforcement Learning for Resource Management in Hybrid Energy LoRa Wireless Networks. *IEEE Internet of Things Journal*.

Junejo, A.K., Benkhelifa, F., Wong, B., & McCann, J.A. (2021). LoRa-LiSK: A Lightweight Shared Secret Key Generation Scheme for LoRa Networks. *IEEE Internet of Things Journal*.

Leonardi, L., Battaglia, F., Patti, G., & Bello, L.L. (2018, October). Industrial LoRa: A novel medium access strategy for LoRa in industry 4.0 applications. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society* (pp. 4141-4146). IEEE.

Lim, J.T., & Han, Y. (2018). Spreading factor allocation for massive connectivity in LoRa systems. *IEEE Communications Letters*, *22*(4), 800-803.

Morris, T.H., Thornton, Z., & Turnipseed, I. (2015). Industrial control system simulation and data logging for intrusion detection system research. *7th Annual Southeastern Cyber Security Summit*, 3-4.

Mumtaz, S., Alsohaily, A., Pang, Z., Rayes, A., Tsang, K.F., & Rodriguez, J. (2017). Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation. *IEEE Industrial Electronics Magazine*, *11*(1), 28-33.

Nevludov, I., Sychova, O., Andrusevich, A., Novoselov, S., Mospan, D., & Mospan, V. (2020, September). Simulation of the Sensor Network of Base Stations in a Local Positioning System in Intelligent Industries. In *2020 IEEE Problems of Automated Electrodrive. Theory and Practice (PAEP)* (pp. 1-6). IEEE.

Novoselov, S. (2018, October). Wireless Sensor Network for Communication Between Base Stations in the Local Positioning System. In *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)* (pp. 383-386). IEEE.

Novoselov, S., & Donskov, O. (2016, October). Study of mobile device wireless control technology in the visible range of the electromagnetic radiation. In *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)* (pp. 123-124). IEEE.

Novoselov, S., & Donskov, O. (2017, October). Distributed local positioning system using DWM1000 location chip. In *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)* (pp. 489-492). IEEE.

Novoselov, S., Sychova, O., & Tesliuk, S. (2019, May). Development of the method local navigation of mobile robot a based on the tags with QR code and wireless sensor network. In *2019 IEEE XVth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH)* (pp. 46-51). IEEE.

Premsankar, G., Ghaddar, B., Slabicki, M., & Di Francesco, M. (2020). Optimal configuration of LoRa networks in smart cities. *IEEE Transactions on Industrial Informatics*, *16*(12), 7243-7254.

Rubio, J.E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security*, 87, 101561.

Snitkin, S. (2015). Unidirectional Security Gateways Reduce Risk of Industrial Cyber Attacks. *ARC View, Jul.*

Specification, L. (2018). v1. 1 Available at: https://loraalliance. org/resource-hub/lorawantm-specification-v11. *Online Accessed*, *10*.

Yeoh, C.Y., bin Man, A., Ashraf, Q.M., & Samingan, A.K. (2018, February). Experimental assessment of battery lifetime for commercial off-the-shelf NB-IoT module. In *2018 20th international conference on advanced communication technology (icact)* (pp. 223-228). IEEE.