Information Security Threats of Wireless "Smart" Utility Metering Systems

Aleksandr Zhuk [a], Dmitrii Orel [a], Anna Vanina [a] and Tatiana Minkina [a]

[a] *North-Caucasus Federal University, Pushkin street, 1, Stavropol city, 355009, Russian Federation*

Abstract

A current trend is the introduction of "smart" utility accounting systems as one of the components of a "smart city" concept in particular and the development of the "Internet of things" in general. This causes threats to information security when transmitting information from metering devices via wireless communication channels to billing centers. The article is devoted to the analysis of these threats and the forecast of ways to protect against them.

The purpose of the article is to develop additional recommendations for the safe use of narrow-band wireless networks of the "Internet of things", used in wireless automated systems for accounting for resource consumption.

Keywords [1]

Smart City, Internet of Things, utility metering system, information threat, wireless channel

1. Introduction

Since 2010, due to the widespread and continuous spread of wireless networks, the development of cloud technologies, the introduction and development of software-configurable networks, there has been a steady trend in the expansion of the use of information technologies.

Today, the Internet of things is considered not just as a set of different sensors and devices connected by wireless and wired communication channels, but as a link between the real and virtual world, through which it is possible to interact and communicate between people and devices [1].

Currently, the majority of IoT trends are mainly observed only in industrial conditions, in the implementation of the concept of "Industry 4.0", in the transport and utilities sector.

Within the framework of IoT trends, the concept of "Smart city" is gaining quite a lot of popularity and development, which is aimed at integrating information and communication technologies, including IoT systems for managing urban infrastructure [2]. The main goal of the Smart city concept is to improve the quality of life of people using urban Informatics technologies by increasing the efficiency of service and meeting the needs of residents [3].

The British Standard Institution (BSI) describes a Smart city as "the effective integration of physical, digital and human systems in an artificially created environment to ensure a sustainable, prosperous and inclusive future for citizens."

This technology allows the city government to directly interact with communities and urban infrastructure. The use of sensors integrated in real-time mode allows you to process and analyze the accumulated data. Thus, the collected information becomes the key to solving the problems of inefficiency and allows optimizing the processes of urban management, for example, including municipal management, which is implemented by automating the processes of collecting and processing data on consumed municipal resources [4]. Such systems allow reducing the cost of personnel involved in collecting and processing information about accounting for consumed

International Workshop on Data Mining and Knowledge Engineering, YRID-2020, October 15–16, 2020, Stavropol, Russian Federation

EMAIL: alekszhuk@mail.ru (Aleksandr Zhuk); kde.def@gmail.com (Dmitrii Orel); hnykina_anna@mail.ru (Anna Vanina); n.min@mail.ru (Tatiana Minkina)

ORCID: 0000-0003-4280-7489 (Aleksandr Zhuk); 0000-0002-3433-2164 (Dmitrii Orel); 0000-0001-8073-2612 (Anna Vanina); 0000-0002-4163-1154 (Tatiana Minkina)

resources, as well as improving the speed and quality of data collection, maintaining objective statistics, and improving consumer payment discipline [5].

According to forecasts of the International Wireless Research forum, the number of things united in a single network by 2020 will amount to 7 trillion. units. According to Cisco, the cost volume of devices connected to the Internet in the current decade is estimated at 14.4 trillion US dollars. The results of the Cisco review showed that 99 % of physical devices are not yet connected, which opens up huge prospects for growth and development of the concept, and according to some experts – in the future, this will lead to the formation of the Internet of things economy. In general, the maximum value of the number of things that can be linked into a single network is estimated as 3,000-5,000 units per person, which makes it possible to talk about the prospects of combining up to 50 trillion things connected to a unified information exchange network.

2. Problem statement

The introduction of the concept of the Internet of things and its accompanying technologies on one hand opens up undeniable opportunities for modern organizations, and on the other hand generates new threats to information security, some of which are of a specific nature, therefore, is not yet well understood by managers, businessmen and society as a whole.

The main concept of IoT is the ability to connect all sorts of objects (things) that a person can use in everyday life. All these objects should be equipped with built-in sensors or sensors that can process information coming from the environment, as well as controlled objects, exchange it and perform various actions depending on the information received.

Currently in the process of application, the Internet of things poses threats to information security that limit its widespread use. Messages such as hacking of Internet-connected devices, surveillance problems and concerns about personal privacy attract the attention of its existing and potential users [6].

A type of Internet of things technology is resource accounting systems, which are designed to collect data from various devices (sensors) for their accounting. Ensuring the information security of wireless resource accounting systems is a determining factor and a difficult task when creating and operating them [7]. The main vulnerabilities of these systems can be considered as:

- vulnerability of channels to accessing and spoofing messages, since the transmission medium is public;
- not secure nodes, because they are located in open places;
- the lack of infrastructure makes classical security systems inapplicable;
- based on the nature of the radio channel, approaches to ensuring information security in wireless networks differ significantly from approaches to implementing information security in wired networks;
- the lack of a clear topology in wireless networks, so that each node can move freely, which makes it easier for a cybercriminal to attack.

The purpose of the article is to develop additional recommendations for the safe use of narrow-band wireless networks of the "Internet of things", used in wireless automated systems for accounting for resource consumption.

3. Analysis of typical solutions for wireless resource accounting systems

A significant number of IoT devices are connected through gateways based on local and personal networks in radio frequency bands used in a simplified manner. At the same time, the gateways themselves can then be connected via cellular mobile networks or narrow-band wireless IoT networks [8].

Although narrowband wireless IoT networks are not considered the most widespread segment of wireless technologies for IoT, this type of network is intended to connect IoT devices in many industries for a wide range of applications that will be difficult or impossible to implement using other types of wireless communication [9].

Let's highlight the most significant areas of application of the Internet of things [10]:

- Mechanism management (M2M, automated process control system);
- Monitoring of consumption of resources;
- Transport and logistics;
- Security monitoring;
- Smart home appliances;
- Collecting statistics and determining trends.

Let's consider typical solutions for building wireless automated resource consumption accounting systems.

1. Household water meters with built-in radio modem for data transmission to the control room.

This type of device is a combination in a single housing of a device for measuring water consumption and a module for collecting and transmitting data on water consumption over a wireless communication channel [11]. The advantages of this type of device include ease of installation and operation. In addition, there are devices of this type on the market, produced by domestic companies and using proprietary radio modules. These devices can encrypt the transmitted data. For data transmission, both LPWAN (XNB) protocols can be used, which require the deployment of their own base stations for data collection, and NB -IoT protocols, which use the services of mobile operators [12] (SIM-card availability and payment for transmitted traffic are required [13]).

2. Household water meters with the ability to connect wireless data transfer devices to the control room.

This solution requires connecting an external radio module and antenna to the water meter to transmit data using cables of various lengths. RS485 and RS232 protocols can be used for data transmission over the cable. In this type of solution, a connected wireless data transfer device can be used with either one counter or simultaneously with several. However, data can be collected simultaneously from both water meters and gas and electricity meters. For data transmission, both LPWAN family protocols can be used, which require the deployment of their own base stations for data collection, and NB -IoT protocols, which use the services of mobile operators (you need to have a SIM card and pay for the transmitted traffic). Since the data transfer device can collect information from several counters and has a significant price, it is advisable to use this solution in apartment buildings, for example, by combining counters in apartments within a floor of a single entrance. For use in private households, it is necessary to place an outdoor installation cabinet, where the data transmission device and antenna will be located (possibly a backup power supply system). In this case, you will need to connect the meter cables located in the wells to the data transmission device located in the installation cabinet.

3. Household water meters with the ability to transfer data to a nearby device.

The solution of this type includes water meters with Bluetooth Low Energy radio modules, remote displays that can receive data via Bluetooth, mobile applications on consumers' phones, as well as a personal account of the management company on the developer's server, where data is centrally accumulated. In this solution, meter readings are transmitted over the radio channel to the mobile app or to a remote display. The transmission distance is up to 10 meters. The mobile application receives data from the counter via Bluetooth, then the user's phone transmits the information to the personal account of the management company on the developer's server via Internet channels available to it (WI-Fi, GSM). This solution is characterized by the low cost of hardware. No additional technical infrastructure is required to collect information from consumers. However, the terms and prices for registering a personal account on the developer's server for managing companies are not clear. The main share of profit under this business model is earned by the developer on this procedure when interacting with management companies. There is no way to oblige consumers to send counter readings with a certain frequency.

It is worth noting that the Internet of things, as a rule, consists of portable devices with low power consumption, a small form factor and limited capabilities. Also, most often, devices are unmanaged, i.e. they work without the participation of an operator, who could enter credentials or make a decision about how much the team or application is trusted [14], so the devices must independently make such decisions. Therefore, when building the architecture of IoT systems, you should pay attention to the “dangerous features” zones (areas) in these systems where threats to information security can be implemented [15]: for example, a data collection server; a database; a radio channel between the subscriber's transmission device and the data collection base station; interfacing of the mechanical and electronic parts of the counter, etc.

4. Overview of the main threats to the information security of wireless resource accounting systems

The security of the Internet of things becomes a key aspect when building such networks. Having gained access to one device, an attacker can get into the network, and then any confidential information is exposed to threats [16]. Hence, the relevance of information security issues in such networks, where it is necessary to take into account the limitations of devices included in them [17].

Applying traditional methods of protecting IoT devices, such as encryption, identification/authentication, and implementing physical security measures [18], requires significant reengineering and adaptation, as devices have many limitations. The main problem with using IoT networks is that they do not have protection from malicious attacks. This can lead, at best, to damage to the user's property, and at worst – to their health and life. For example, devices that monitor and control the electrical network can be hijacked by an attacker using any device that has access to the Internet and related software. Having obtained full or partial control of the device, an attacker can disable or damage electrical devices, including critical devices (life support systems in hospitals, industrial monitoring systems, security systems, etc.), create short circuits in the network, and even cause a fire or accident, if it is a production. That is why there is an urgent problem of researching the security of the Internet of things and, in particular, the security of the user, his property and personal information that is transmitted, processed and stored in IoT networks.

Due to their portability, IoT devices are physically accessible to hackers, and can be stolen to gain access to confidential data and establish communication with other network devices. To prevent this threat, you need to provide physical protection, for example, by using protective covers on devices or enclosures that restrict direct access to devices.

In addition to direct access, devices can provide remote access to update configuration data or software. To protect against this, you must provide for closing the software ports and applying strong passwords at the download and firmware update level, which will prevent access to the device if it is compromised.

Also, many IoT devices become vulnerable to cyberattacks because their software is not updated in a timely manner [19]. To minimize such risks, we recommend implementing automatic updates by default. In addition, you should pay attention to the organization of data storage on the devices themselves, because often this information is related to the user's personal data, financial transaction data, and data about critical objects in various fields of activity. Safety must be ensured both during the entire time of operation of the product and after its decommissioning.

To protect networks, "strong authentication" methods must be provided, including, for example, two-factor authentication, assigning "hard" unique identification and authentication data, and using modern secure protocols. Cryptographic algorithms must be adapted to the Internet of Things network. In order to minimize the risks of denial-of-service attacks against devices, it is recommended to limit the bandwidth of the Internet of Things network of devices, both at the software and hardware levels. If suspicious traffic is detected, the devices must provide an alarm capability with subsequent analysis of the detected threat. If the device is compromised, it should be possible to immediately erase key information used in cryptographic operations. IoT devices should transmit and process only the information that is necessary for the implementation of their main functions.

In addition to the heterogeneity of networks, a feature of the Internet of Things is that devices have different computing resources, bandwidth, and support different technologies and protocols. The lack of unified standards and protocols remains a serious problem when building a network of "things". Also, many "things" have limited power supply capabilities and must support power-saving modes. These features of the Internet of Things also impose limitations when building a security system on such a network.

The usual methods of protecting information in wireless networks may not be sufficient, or they may not be applicable due to the limitations imposed by the Internet of Things network. Therefore, the security subsystem must be designed to provide protection for devices and gateways, the transmission network, and applications that are deployed to ensure that the devices function.

5. Directions for countering threats to information security

Complex issues of information security, including those applicable to narrow-band wireless IoT networks, are considered in a separate area of implementation of the Digital economy of the Russian Federation program. For this reason, the "Concept of building and developing wireless narrow-band communication networks of the Internet of Things on the territory of the Russian Federation" considers only the key aspects of regulating protection and information security methods necessary for the successful construction and development of narrow-band wireless IoT communication networks. These aspects are illustrated in Figure 1.

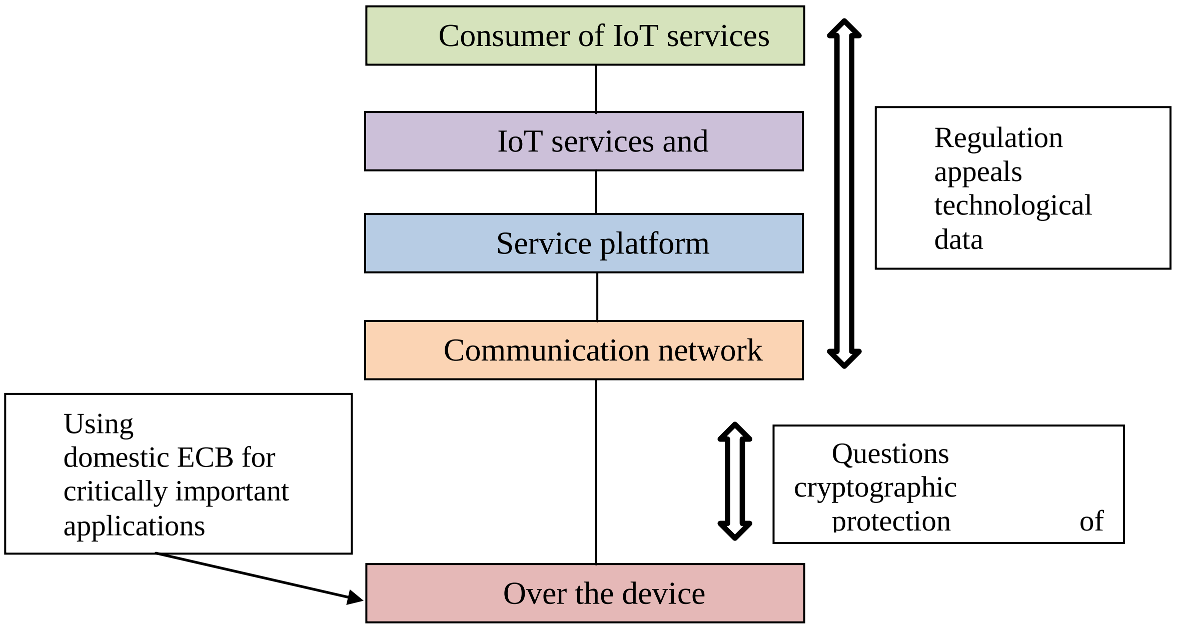
Consumer of IoT services
IoT services and
Service platform
Communication network
Regulation appeals technological data
Using domestic ECB for critically important applications
Questions cryptographic protection of
Over the device

Figure 1: Selected aspects of ensuring information security of narrow-band wireless communication networks IoT

The most global issue of protection and information security methods in narrow-band wireless IoT communication networks is the regulation of storage and processing of huge amounts of data collected from a variety of sensors. If the data is distorted even in the telemetry data, it may later cause the infrastructure to malfunction.

In the framework of the above mentioned concepts the following general guidelines are determined for information security narrow-band wireless networks "Internet of Things", whereas, including the use of existing Russian technologies ensure the integrity, confidentiality, authentication and availability of information and processing [20]:

1. In the organizational part

a) it is necessary to develop a common terminology and classification of objects, methods and tools used in the field of the "Internet of Things" in the territory of the Russian Federation. The lack of a common terminology and classification hinders structured work to create appropriate tools to ensure information security, provokes errors in interpretation;

b) it is necessary to develop specific requirements for ensuring information security for certain areas of application, complementing the General recommendations. General recommendations cannot take into account the technological features of individual applications and guarantee the applicability and sufficiency of such recommendations. A threat model must be developed based on which the cryptographic protection class is selected;

c) it is necessary to ensure regular educational work among operators and users of the Internet of things network aimed at responsible attitude and compliance with information security standards on the entire perimeter of the network.

2. In part of the access network

a) it is recommended to give preference to open, well-documented standards for narrow-band wireless Internet of things networks, for which the stability of embedded information security mechanisms is analyzed by a large community of researchers and developers, thus reducing the risk of undetected vulnerabilities.

3. In terms of the platform and applications

a) it is advisable to consider the possibility of applying cryptographic protection and monitoring the integrity of messages transmitted between the subscriber's device and the Internet of things platform. The implementation of cryptographic protection and integrity control must have the property of having the lowest possible impact on the power consumption of the subscriber's device. At the same time, before introducing this requirement as a mandatory one, it is advisable to conduct a pilot project in a separate region to work out the possible risks of such a replacement;

b) regular internal and external information security audits should be encouraged.

According to the authors of the narrow-band wireless networks of the "Internet of things" used in wireless automated systems for accounting for resource consumption, the following recommendations should also be considered for use:

1 In terms of subscriber devices and embedded software

a) it is recommended to provide a power of attorney for the hardware of terminal devices, by localizing the processes of its development and production, or by declaring their compliance with the established requirements. The greatest attention should be paid to the power of attorney of such hardware components of end devices as the controller and the receiving and transmitting module;

b) it is necessary to ensure the power of attorney of software endpoints, by localizing its development processes;

c) to ensure information security in the networks used in wireless automated resource consumption accounting systems, it is necessary to consider the issue of ensuring the use of cryptographic information protection tools by the subscriber device and the IoT platform.

2 In part of the access network

a) it is necessary to ensure the use for the authentication of subscribers of cryptographic protection of information, certified by the appropriate protection class subject to the protected objects and the set of capabilities that can be used to create methods, training and carrying out attacks on these objects, to the applied information technologies, environments and hardware.

6. Acknowledgements

It should be noted that Russia is still lagging behind the leading countries in terms of promotion of IoT technologies. The globalization of the global economy challenges Russia to quickly introduce innovative IoT technologies that will make everyday life safe and convenient, and will contribute to increasing satisfaction of human needs and society as a whole.

The use of "smart" technologies for the development of ways to manage the city's infrastructure is a necessary condition for maintaining competitiveness, especially in the context of an economic crisis. The world practice of applying these technologies shows that the indicators of efficiency and efficiency of urban economy institutions are significantly increasing.

Based on the general recommendations for ensuring information security of narrow-band wireless networks of the Internet of things for narrow-band wireless networks of the Internet of things used in wireless automated resource consumption accounting systems, the authors propose to additionally use the proposed recommendations in terms of subscriber devices and embedded software and in part of the access network.

This work was supported by the Russian Foundation for Basic Research, project No. 18-07-01020.

7. References

[1] A. P. Zhuk, S. S. Ryabtsev, R. A. Khachkizov, M. G. Ogur, N.D. Dzhamiev, D. A. Sherbakov. “Analysis of the information protection methods in telecommunication systems with channels split by code”. CEUR Workshop Proceedings, 2254. 2018. Pp. 303-310.

[2] A. Prusov, N. Sevryugina, A. Ovsienko. “Smart house: Model of resource management and safety of vertical transport”. E3S Web of Conferences, 97. 2019. Article # 01016, #148595.

[3] A. V. Markeeva. “Internet of things (IoT): opportunities and threats for modern organizations”. Society: sociology, psychology, pedagogy, #2. 2016. Pp. 42-46.

[4] A. Y. Fetisova, Hadi Saleh. “Data collection and processing information systems on sensors of mobile devices”. JSRP. 2016. # 6 (38). URL: https://cyberleninka.ru/article/n/sbor-i-obrabotka-dannyh-s-sensornyh-datchikov-mobilnyh-ustroystv (01.10.2020).

[5] A. Zhuk, D. Orel, E. Nekrasova, O. Krivolapova. “The use of simulation models and game scenarios in the study of radio engineering systems by higher engineering students”. CEUR Workshop Proceedings, 2494. 2019. #154115.

[6] A.A. Gavrishev, A.P. Zhuk, D.L. Osipov. “An analysis of technologies to protect a radio channel of fire alarm systems against unauthorized access”. SPIIRAS Proceedings, 4 (47). 2016. Pp. 28-45.

[7] D. Orel, A. Zhuk, E. Zhuk, L. Luganskaia. “A method of forming code sets for CDMA in communication, navigation and control systems”. CEUR Workshop Proceedings, 1837. 2017. Pp. 158-167.

[8] D. Vlasov, A. Terekhova. “Determination of regularities in the development of intermodal hubs' planning structure in "smart" cities”. E3S Web of Conferences, 97. 2019. Article # 01007, #148595.

[9] D.F. Vydrin, D.R. Sitdikov. “Brief review of main kinds of LPWAN networks”. Academy. 2019. # 2 (41). URL: https://cyberleninka.ru/article/n/kratkiy-obzor-osnovnyh-vidov-setey-lpwan (01.10.2020).

[10] E. Basan, M. Lapina, D. Orel. “Host-based method and system for detecting anomalies in network traffic for a robotic system”. CEUR Workshop Proceedings, 2500. 2019. #154807.

[11] I. A. Gromov. “Influence of digital technologies on the sphere of public and business services in Russia”. Problems of modern economy, # 3. 2018. Pp. 43-47.

[12] I. Zaitseva, O. Malafeyev, N. Poddubnaya, A. Vanina, E. Novikova. “Solving a dynamic assignment problem in the socio-economic system”. Journal of Physics: Conference Series, Volume 1172, Issue 1, 1 April 2019, # 012092I.

[13] Internet of things communication method, network-side device and Internet of things terminal. Russian patent 2019 for IPC H04L12 / 24, RU 2 693 293 C1.

[14] M. Deryabin, M. Babenko, A. Nazarov, N. Kucherov, A. Karachevtsev, A. Glotov, I. Vashchenko. “Protocol for secure and reliable data transmission in MANET based on modular arithmetic”. 2019 International Conference on Engineering and Telecommunication, EnT 2019. Art. # 9030580. doi: 10.1109/EnT47717.2019.9030580.

[15] M. Panteleeva, S. Borozdina, “Mathematical model of evaluating the quality of "smart city" transport interchanges functioning”. E3S Web of Conferences, 97. 2019. Article # 01006.

[16] N. Chervyakov, M. Babenko, A. Tchernykh, N. Kucherov, V. Miranda-López, J.M. Cortés-Mendoza. “AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security”. Future Generation Computer Systems, 92. 2019. Pp. 1080-1092. doi: 10.1016/j.future.2017.09.061

[17] Nayancy, S. Dutta, S. Chakraborty. “IoT-Based Secure Communication to Enhance Blockchain Model”. Lecture Notes in Electrical Engineering, 673. 2021. Pp. 255-264.

[18] Parfenov, D.I., Bolodurina, I.P., Lapina, M.A. “Development of a model for detecting security incidents in event flows from various components in a network of telecommunication service providers” IOP Conference Series: Materials Science and Engineering, V. 873, Issue 1, 7 July 2020, # 012020.

[19] R. Patnaik, N. Padhy, K. Srujan Raju. “A systematic survey on iot security issues, vulnerability and open challenges”. Advances in Intelligent Systems and Computing, 1171. 2021. Pp. 723-730. doi: 10.1007/978-981-15-5400-1_68.

[20] XX Order of the Ministry of digital development, communications and mass media of the Russian Federation No. 113 dated 29.03.2019 "On approval of the Concept of building and developing wireless narrow-band communication networks of the Internet of things on the territory of the Russian Federation".