Internet of things networks predictive risk assessment method and security management

A A Bolgov\(^1,2\), S A Ermakov\(^1,2\), L V Parinova\(^1\) and V N Kostrova\(^1\)

\(^1\)Voronezh State Technical University, 14, Moscow ave., Voronezh, 394026, Russian Federation
\(^2\)JSC «Concern «Sozvezdie», 14, Plekhanovskaya str., Voronezh, 394018, Russian Federation

E-mail: csit@bk.ru

Abstract. The methodology of predictive security violation risk assessment based on the use of fuzzy logic is offered. Demonstrates one risk assessment methodology use for IoT-network in presence of data about protocols used in network wireless devices. Alternative methodology for risks predicting when at the initial stage experts estimate input parameters, with subsequent data processing using the hierarchical methodology based on fuzzy inference systems that can reduce the influence of subjective expert evaluations of the researched object is offered. Numerical estimates of risk, despite qualitative character of expert estimates of input parameters are received.

1. Introduction

In connection with the widespread use of wireless technologies and machine-to-machine exchange, began to develop quickly concepts of the Internet of Things (IoT). There is an intensive development of the self-organizing communication networks, in which subscribers not only people, but also various automatic devices which carry out information exchange with each other without direct participation of the person within machine-to-machine communication. Also today it is possible to notice prompt development of the industrial Internet of things (IIoT) market by which concept, there was an introduction of mechanisms of an exchange of information on important industrial facilities or in the industrial centers where the accuracy and speed plays an important role in production life cycle [1-4].

Currently, the concept of the classical definition of risk difficult to apply in real systems the Internet of things because of its demands the availability of statistical data on the damage. In this case, only experts are able to qualitatively assess these options. However, these qualitative estimates of experts hard to predict. This leads to the fact that when you build any IoT-network, we are unable to give an accurate assessment of possible risks of the entire network as a whole [5-6].

Relevance of this work is defined by a contradiction between rapid growth of popularity of introduction of the IoT technologies, lack of uniform approach to a risk assessment, as well as weak legal support of this technology [7-11].

Thus the purpose of this work is to develop a methodology of predictive risk assessment in the conditions of lack of statistics of damage of an IoT-network, as well as developing of the technique of regulation of risks based on obtaining recommendations for decrease in risk.
2. Risk assessment methodology IoT-networks

For calculation of numerical evaluation of risk in network of the Internet of things, the technique which considers the used protocols of safety in wireless devices of the studied network can be applied [12]. Imagine IoT-network in which there are eight devices of the Internet of things working on different wireless technologies (table 1). They can have different versions of security protocols.

| Used equipment                  | Wireless connection | Protocol | Number of devices |
|--------------------------------|---------------------|----------|------------------|
| 1 IP video camera              | Wi-Fi               | WPA      | 2                |
| 2 IP video camera              | Wi-Fi               | WPA2     | 1                |
| 3 Sensor of protection of window | Bluetooth         | V3.0     | 3                |
| 4 Sensor of protection of window | Bluetooth         | V4.0     | 1                |
| 5 System of protection of the house | Z-Wave            | S2       | 1                |

Table 1. Descriptions of protocols of safety of necessary devices.

Having found out, what wireless technologies and protocols of safety use devices of the studied IoT-network, it is necessary to estimate security of each protocol of all connections. This is done on the basis of expert estimates by means of the fuzzy logic toolbox of the Matlab software.

On the basis of the received values of security, the table with quality assessments on all to possible combinations of protocols is formed. Then according to the received quality assessments of level of security of different combinations in network, it is possible to compare quality assessments of indistinct risk for the set combinations. It is necessary for task of rules of functions of accessory. After that there is description of the rules necessary for defuzzification stage in Matlab.

As in the set network, there are some devices belonging to the same type of wireless connection, but working at different protocols of safety it is necessary to calculate input values for calculation of fuzzy risk of network. Obtaining input values for not the particular case is carried out using:

\[ x = b_1 + \frac{b_2 - b_1}{p_1 + p_2} \]

where \( b_1 \) and \( b_2 \) - values of abscissa axis of tops of functions; \( p_1 \) and \( p_2 \) - number of versions of protocols; \( x \) - required input value (figure 1).

Having the original and calculated values for the membership functions of the devices of the technologies Wi-Fi and Bluetooth, as well as knowing the number of devices working on these wireless technologies, it is possible to calculate the input values for these networks, necessary for receiving numerical assessment of indistinct risk of the selected network.

Having obtained all necessary data, we will enter input values into Mamdani’s fuzzy inference algorithm and we will receive value of fuzzy risk equal 0.327 (figure 2).

The above method will be working only in that case when there is necessary information on the devices used in IoT-network, namely what protocols will use these or those wireless devices of this network. But as mentioned before, IoT of technology begin to penetrate the industrial and commercial centers in which it can already not appear information necessary for us on devices, and also they can be both wire, and wireless. Therefore, the alternative method of risk assessment is offered.

As input parameters were chosen the metrics that are captured in regulatory documents, namely: assessment of the attacker, assessment of security, vulnerability assessment, impact assessment.

These parameters are estimated by experts and processed by the fuzzy inference system according to the scheme presented in figure 3 by means of software environment of Matlab with the built-in packet of Fuzzy Logic Toolbox.

As a result of execution of modeling we receive the three-dimensional diagram, and also visual representation of rules of fuzzy set, for receiving numerical evaluation of risk (figure 4).

The proposed method was verified by comparing with the statistical data. Method of testing was the test U of Mann-Whitney test [6]. This coefficient serves for assessment of reliability of distinctions on sign level in two independent samples. Calculating \( U_{emp} \), compared to the tabular \( U_{krit} \) for the
significance level of 0.05, was obtained $U_{\text{emp}} > U_{\text{krit}}$. This means that the values of calculated risk is not significantly different from values obtained in practice, which proves the validity of the developed risk assessment methodology.

**Figure 1.** The given membership functions of devices operating over Wi-Fi and Bluetooth respectively.

**Figure 2.** Graphic interpretation of Mamdani’s fuzzy inference algorithm.

**Figure 3.** The scheme of processing parameters.
3. Risk management
Applying the offered risk assessment technique, quantitative values of risk have been received, leaning on which the conclusion has to be drawn on strategy of its regulation. Obviously, it is possible to allocate three zones of risk:

- area of risk taking;
- the area of redistribution of risk;
- area of risk insurance.

The greatest interest is the area of redistribution of risks, because risk management is carried out by the organization itself. Risk management usually represents the selection and implementation of a range of famous remedies, followed by re-analysis of the risk to ascertain the effectiveness of its use. In ideal conditions of iteration of this cycle repeat until required value of risk is reached. In this case, the problem arises of choosing the optimal from the point of view of reducing risk of complex remedies, in the absence of any recommendations for networking technologies of IoT [13].

In this case, it is expedient to address to foreign experience, for example, the Agency ENISA (The European Union Agency for Network and Information Security) released a document containing a section on threats and risk analysis. This section is presented in the form of a table that contains the category of threat, the threat directly, its description, and also affected the company's assets.

The second way in choice of recommendations for safety it is possible to call binding to private models of devices. For example, knowing the devices that are on a network, you can open databases of vulnerabilities to find out what are the recommendations to eliminate or reduce the impact of current vulnerabilities. There are a large number of databases of vulnerabilities, some of them open, part – closed. The choice of recommendations when using databases of vulnerabilities can be a little complicated as it is necessary to know precisely the models of devices involved in system, the operating systems and the software functioning on the IoT platforms. However thus it is possible to receive effective recommendations for specific case [14].

4. Conclusion
Thus, it is possible to draw conclusion that the offered technique of risk analysis allows to predict numerical value of risk on the basis of estimates of experts. This technique has a flexible configuration system, it is easy to implement and does not require huge amount of computing resources of the system, which allows its use in systems of any complexity. For adaptation to specific systems, it is necessary to fully assess the company's assets and to prepare questions for the experts.

As the parameters evaluated by experts are characterized by the subjectivity, implementation of mathematical apparatus of fuzzy sets is necessary. Having a fuzzy expert assessment, were able to
obtain numerical estimates for the group of devices used in the IoT-network. The essence of this method lies in the consistent application of fuzzy interface for the parameters.

The main difference of the presented method from others is that it can help to assess a complex network consisting of different heterogeneous wireless devices with different number and types of security protocols.

References
[1] Lvovich I Ya, Lvovich Ya E, Preobrazhenskiy A P and Choporov O N 2019 Management of the internet of things system based on decision-making and optimization approaches Conference of Open Innovations Association, FRUCT 24 688-96
[2] Ermakov S A, Zavyrkin A S, Kolbenet N S, Ostapenko A G and Kalashnikov A O 2014 Optimization of expert methods used to analyze information security risk in modern wireless networks Life Science Journal 11(10s) 511-4
[3] Addo I D, Ahamed S I, Yau S S and Buduru A 2014 A reference architecture for improving security and privacy in internet of things applications IEEE 3rd International Conference on Mobile Services 108-15
[4] Lvovich Ya E, Lvovich I Ya, Preobrazhenskiy A P and Choporov O N 2019 Forecasting and optimization internet of things system Communications in Computer and Information Science 1083 321-33
[5] Neisse R, Steri G and Baldini G 2014 Enforcement of security policy rules for the Internet of Things IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications 165-172.
[6] Carruthers K 2016 Internet of Things and Beyond: Cyber-Physical Systems IEEE Internet of Things Newsletter 62-4
[7] Kravets O Ja, Preobrazhenskiy A P, Kochegarov A V, Choporov O N and Bolnokin V E 2018 Development of algorithms for complex numerical optimization of objects with modular structure International Journal on Information Technologies and Security 10(4) 45-56
[8] Tsaregorodtsev A V, Kravets O Ja, Choporov O N and Zelenina A N 2018 Information Security Risk Estimation for Cloud Infrastructure International Journal on Information Technologies and Security 10(4) 67-76
[9] Lvovich I Ya, Lvovich Ya E, Preobrazhenskiy A P, Preobrazhenskiy Y and Choporov O N 2019 Managing developing Internet of things systems based on models and algorithms of multi-alternative aggregation International Seminar on Electron Devices Design and Production (Prague, Czech Republic) 1-6
[10] Vasilyev V I and Shamsutdinov R R 2019 Intelligent system of information security incident analysis (based on the methodology of siem-systems using immunocomputing mechanisms). Modeling, optimization and information technology 7(1) doi: 10.26102/2310-6018/2019.24.1.011
[11] Gavrishev A A 2019 Generalized computational method to compare the accuracy of quantitative estimates of security of wireless security systems. Modeling, optimization and information technology 7(3) DOI:10.26102/2310-6018/2019.26.3.002
[12] Bolgov A A, Ermakov S A and Mokrousov A N 2019 Evaluating the effectiveness of IoT-network protection on the example of smart home technology implementation. Journal on Information and Security 22(1) 130-3
[13] Oladko V S 2019 Formalization of the access control audit procedure in the information system. Modeling, optimization and information technology 7(3) DOI:10.26102/2310-6018/2019.26.3.018
[14] Kashirina I L and Fedutinov K A 2018 Application of Fuzzy ArtMap network in intelligent systems of invasion detection Modeling, optimization and information technology 6(3) https://moit.vivt.ru/wp-content/uploads/2018/07/KashirinaFedutinov_3_18_1.pdf