Optimization of expert methods used to analyze information security risks in modern wireless networks

Sergey Alexandrovich Ermakov, Aleksey Sergeevich Zavorykin, Nikolai Sergeevich Kolenbet, Alexander Grigorievich Ostapenko, Andrei Olegovich Kalashnikov

Voronezh State Technical University, Moskovskiy avenue, 14, Voronezh, 394026, Russian Federation

Abstract. This article is devoted to optimizing the methodical base for improving adequacy of estimates obtained during analysis of information security risks in modern wireless networks. In this work, a method of accounting for risk dynamics indicators is proposed, based on the model of a generalized attack on an IEEE 802.11 wireless network and experimental data about average duration of implementation of various phases of attacks. Necessary adaptation of tools provided within the framework of fuzzy multiple risk analysis of wireless networks has been performed. Based on the proposed approach, forecasts of changes in risk magnitude were obtained, which ensures additional flexibility in choosing measures to protect a wireless network from economic viability point of view.
[Ermakov S.A., Zavorykin A.S., Kolenbet N.S., Ostapenko A.G., Kalashnikov A.O. **Optimization of expert methods used to analyze information security risks in modern wireless networks.** *Life Sci J* 2014;11(10s):511-514] (ISSN:1097-8135). http://www.lifesciencesite.com. 99

Keywords: risk, assessment, attack, wireless network, probability of implementation, damage, expert evaluation, fuzzy sets, fuzzy output, dynamics

Introduction

Currently, the wireless market is experiencing drastic changes due to the customers' increased demand for integrated multimedia services, as well as exponential growth of traffic and requirements to data transfer rate. Wireless IEEE 802.11 networks created in 1997 [1] in course of their development have reached their fifth generation and, due to their increased efficiency, make it possible to address these issues via using innovative technologies that ensure data transmission at speeds of up to 3.5 gigabits per second. [2] This allows Wi-Fi to compete with other wired and wireless solutions in digital data transfer. Intensive development of wireless networks of this type extends the scope of their application, so that the issue of information security for Wi-Fi networks becomes urgent [3].

Modern wireless networks, as an object of study in the context of developing risk models of individual elements, may include expert approaches discussed in monograph [3], but the limiting factor in using this method is the need for iterative analysis, systematization and processing large amounts of expert data, requiring substantial financial and time resources.

The aim of this article is to optimize tools provided within the framework of the concept of fuzzy multiple risk analysis of wireless networks [3] for accounting for dynamics of the risk indicator in choosing optimal protection from the economic point of view.

Methods

Taking into account the specifics of the object of study, we propose to estimate the probability of an attack and damage caused by its implementation by interviewing experts and subsequent processing of the information received. That said, quality scales are used for assessment associated with quantitative values. Then, based on exact input values of threat probability and damage from its implementation, as well as on formulated rules of fuzzy output, risk value is calculated using the fuzzy output mechanism by Mamdani algorithm. Fuzzy numbers obtained from questioning an expert or a group of experts are in many respects similar to the statistical distributions of probability theory, but are free from inherent disadvantages, such as some distribution functions suitable for analysis, the need for their forced normalization, compliance with additivity, difficulty of justifying adequacy of mathematical abstraction for describing behavior of actual values. Compared to the probabilistic method, the fuzzy method makes it possible to reduce the amount of calculations, resulting in a greater speed of fuzzy systems. Developing a model of an attack on Wi-Fi network allows to introduce a temporary component, which makes it possible to take into account dynamics and enhance objectivity of risk assessment.

Main part

Thanks to modeling a generalized attack on a wireless Wi-Fi network using Petri-Markov networks and experimental data about average time required for each stage of the attack on a wireless network Wi-Fi [4], dependence was obtained of the probability of attack implementation on the time

elapsed since its start (Figure 1):

$$P(t) = 1 - e^{-\frac{1}{262}t}, \quad (1)$$

whereby time dependence is taken into account in input data for the fuzzy inference mechanism. To do so, we considered the steps of a typical attack on a Wi-Fi network (from studying coverage and equipment preparation to gaining access to the network), on which a Petri-Markov network had been built. Then we built a system of integral-differential equations that corresponded to the network, using a Poisson approximation, and obtained the average travel time across the Petri-Markov grid from initial position to the final transition, and probability of this travel (1). To estimate time cost of each stage, information was used from literature in this field [4], as well as expert judgment and data obtained experimentally.

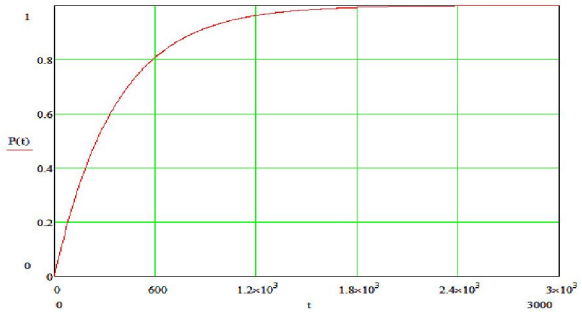

Figure 1. Dependence of probability of an attack on a wireless network on time

In order to use the mechanism of fuzzy sets, it is first necessary to assess the probability of each type of attack and damage from ongoing attacks threats by expertise. This data will be used as input values for fuzzy inference.

The next step is building functions of fuzzy sets belonging, which is also made taking into account experts' opinion. In most cases, it is easier for experts to answer questions about the nature of diffused borders between adjacent terms. Such information may be concentrated in functions of diffused boundaries of terms [mu]i,i+1(x), i = 1, 2, …, n-1. Suppose that a linguistic variable defined by a set of n terms is defined by specifying functions of belonging of these terms [mu]i(x), i = 1, 2, …, n, then assessment of [mu]i,i+1(x) may be performed as follows [5]: each expert specifies an interval [delta]xi on the scale of the universal set X that corresponds to intersection of two adjacent terms Xi and Xi+1. As questions to experts, questions may be used like "specify the interval of changing probability of threat, corresponding to transition from the "very low" to the "low" concept. On the intervals obtained from the survey, bell-shaped functions [phi]ij(x) are built, form of which is chosen from prior considerations (based on the idea of the researcher and preliminary data).

Such processing of the expert group assessments provides information about the nature of diffused boundaries between adjacent terms concentrated in functions [mu]i,i+1(x), representing a generalized solution of the experts.

Then it is necessary, similar to the diffused boundaries of terms function, to normalize functions of terms be-longing by equating their maximum values to unity.

According to the theory of fuzzy sets, let us choose interval [0;1] as the area of variables, and define a set of terms for each of them. For linguistic variable "probability of threat", let us define the following set of terms: "very low", "low", "medium", "high", "very high", and for the linguistic variable "damage from implementation of threat" let's define the term set "insignificant", "low", "medium", "substantial", "significant", and "unacceptable". Then let us use the method of successive intervals that is convenient for expert judgment. To do so, the entire interval [0;1] is divided into 20 sub-intervals. Now, for the two neighboring terms, each expert indicates those of twenty subintervals that corre-spond to the intersection of these two terms, after which the length of the resulting interval (i.e., number of subintervals) is calculated. As five terms had been allocated, we get all in all four intersections of adjacent terms; then in [phi]ij(x), i takes values between 1 and 4. Since the expert group consists of five participants, in [phi]ij(x), j takes values between 1 and 5. From these results, it is necessary to calculate the diffused boundaries function of adjacent terms, after which a belonging function is built for each of the separate terms of the linguistic variable (Figure 2).

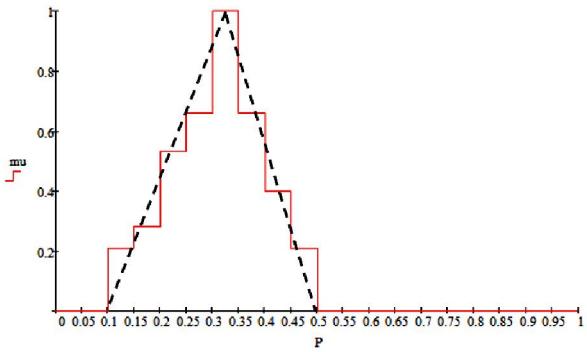

Figure 2. Function of belonging to "low" term

Performing relevant calculations [3] for each term, we obtain belonging function for terms of the "threat probability" linguistic variable (Figure 3).

"very low" "low" "medium" "high" "very high"

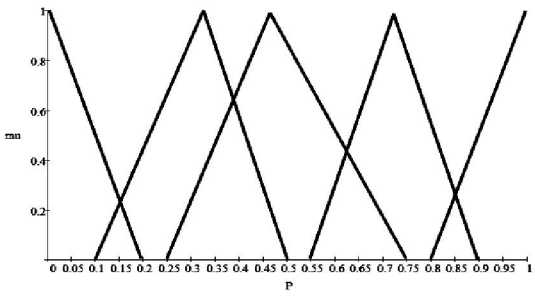

Figure 3. Function of terms belonging to the "probability of threat implementation" linguistic variable

Using the above procedure, we can obtain the function of belonging for remaining linguistic variables. In im-plementation of the fuzzy inference mechanism there is a possibility to select algorithms of individual processing steps. Specific algorithms reflect specifics of the system in question, active relationships, as well as the way of representing the available prior data, on which the inference procedure is built. The most common and convenient fuzzy inference algorithm is the Mamdani algorithm, since it is based on the most commonly used max-min principle and makes it pos-sible to obtain exact output values out of fuzzy input values [3].

Let us assess the risk of threats to information security caused by unauthorized access directly to the infor-mation that circulates in a wireless network, and to segments of wired network services provided by competitors, by disclosing a simple PSK using a brute force or a dictionary attack. For risk assessment based on fuzzy logic with pre-liminary estimation of two input parameters (threat probability for a wireless Wi-Fi network and damage from this threat), a fuzzy inference mechanism was used.

Probability of threat implementation is:

$$P_{\text{p.y.}} = P_{\text{p.y.}} \cdot P(t), \quad (2)$$

where $P_{\text{p.y.}}$ = 0.48 is expert opinion about probability of the threat of unauthorized access using an attack with disclosing a simple PSK using the exhaustive search method or a dictionary attacks;

P(t) is time component.

Suppose that 1 hour (60 minutes) elapsed since the attack, then

$$P(t) = 1 - e^{-\frac{1}{36_2}t} = 1 - e^{-\frac{1}{36_2}\cdot 60} \approx 1 - 0{,}85 = 0{,}15,$$

consequently,

$$P_{\text{p.y.}} = 0{,}48 \cdot 0{,}15 \approx 0{,}07.$$

The damage caused by the attack strongly depends on characteristics of the organization in question, its information flows, network structure and economic parameters, so it should be assessed through questioning experts that are familiar with the company business. Suppose that after processing survey results, and converting them into a quantitative scale (0 to 1), we obtained U=0.8.

The Fuzzy Logic Toolbox software suite makes it possible to obtain a three-dimensional graph of information security risk on the likelihood of threat implementation and the damage from its implementation. [3] Let us make calculations for similar conditions, but after 10 hours (600 minutes) since the beginning of the attack:

$P(t) = 1 - e^{-\frac{1}{36_2}t} = 1 - e^{-\frac{1}{36_2}\cdot 600} \approx 1 - 0{,}19 = 0{,}81;$ $P^{*} =$ 0.48 • 0.81 ≈ 0.39.

Discussion

Thus, as a result of these calculations we can conclude that one hour after the attack for disclosing a simple PSK using brute force or a dictionary attack, the risk of information security for the wireless Wi-Fi network in question had been 0.366, and after another nine hours of attacks it reached 0.567.

Conclusions

The proposed method of risk assessment makes it possible not only to obtain its value, but also to take into account the time factor, i.e., it takes into account the dynamics of the considered value changing over time, which makes it possible to predict the risk of change, and, taking into account assessment of relevance and confidentiality of information in the company, makes it possible to more flexibly select measures to protect a wireless network from the point of view of economic viability. Also, the time component makes it possible to reduce subjectivity of expert assessing the probability of threat implementation, which ultimately leads to less biased risk assessment [6-10].

Corresponding Author:
Dr.Ermakov Sergey Alexandrovich
Voronezh State Technical University
Moskovskiy avenue, 14, Voronezh, 394026, Russian Federation

References

1. Official IEEE 802.11 Working Group Project Timelines. IEEE, September 19, 2009. Date

Views: 2014-04-13 http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm.
2. Nagarajan, V., 2012. 5G WiFi: Introducing a Wi-Fi Powerful Enough to Handle Next-Gen Devices and Demands. Date Views: May.14, 2012 http://blog.broadcom.com/wireless-technology/5g-wifi-introducing-a-wi-fi-powerful-enough-to-handle-next-gen-devices-and-demands/.
3. Shcherbakov, V.B. and S.A. Ermakov, 2010. Wireless Networks Security: IEEE 802.11 standard. Moscow: RadioSoft, pp: 255.
4. Ramachandran, V., 2011. BackTrack 5 Wireless Penetration Testing. Begin-ner's Guide. Birmingham: Packt Publishing Ltd., pp: 207.
5. Novoselov, A.A., 2001. Mathematical modeling of financial risks. Measurement theory. Novosibirsk: Nauka, pp: 212.
6. Kalashnikov, A.O., Y.V. Yermilov, O.N. Choporov, K.A. Razinkin, N.I. Barannikov, 2013. Ensuring the Security of Critically Important Objects and Trends in the Development of Information Technology. World Applied Sciences Journal, 25(3): 399-403.
7. Menzhulin, R.V., G.A. Ostapenko and L.V. Parinov, 2011. Risk assessment and security management of a distributed payment system based on ATMs. Information and Security Journal, 3: 359-380.
8. Yurasov, V.G., D.M. Kovalenko, G.A. Ostapenko and M.A. Balenko, 2011. Building a sensitivity matrix for subjects of social information network. Information and Security Journal, 3: 401-408.
9. Ostapenko, G.A., D.G. Plotnikov, O.A. Ostapenko and S.S. Kulikov, 2012. Concept of probabilistic risk analysis in distributed systems. Information and Security Journal, 4: 511-518.
10. Ostapenko, G.A., I.Y. Lvovich, N.M. Radko, S.V. Fursov and D.G. Plotnikov, 2012. On the issue of risk assessment in attacked distributed information systems: developing conceptual apparatus. Information and Security Journal, 4: 583-584.

6/4/2014