Cyberattack intensity forecasting on informatization objects of critical infrastructures

IOP Conf. Series: Materials Science and Engineering 481 (2019) 012003 doi:10.1088/1757-899X/481/1/012003

Cyberattack intensity forecasting on informatization objects of critical infrastructures

Y M Krakovsky[1], A N Luzgin[2], Y M Ivanyo[3]

[1]Irkutsk State Transport University, 15 Chernyshevskogo Street, Irkutsk 664074, Russia
[2]Administration of Irkutsk city, 14 Lenina, Irkutsk 664025, Russia
[3]Irkutsk State Agrarian University named after A.A. Ezhevsky, Irkutsk 664038, Russia

E-mail: alexln@mail.ru

Abstract. In regulatory documents of recent years in the field of information security, much attention is paid to information systems of critical infrastructures. This, in turn, justifies the need for scientific research on the development of new methods of protection against cyberattacks on such information systems. For this task, interval forecasting is recommended based on a probabilistic neural network with dynamic updating of the smoothing parameter. As benchmarks for comparing the interval forecasting results, the naive Bayesian model and the probabilistic cluster model were chosen.

1. Introduction

In last years, in Russia and World, much attention has been paid to the security of critical infrastructures. In accordance with the federal law «About security of a critical information infrastructure of Russian Federation» adopted in 2017 [1], the information systems (IS) are the important objects of protection. These objects fall under the Decree of the President of the Russian Federation 15.01.2013 N31s «On creation of the state system of detection, prevention and liquidation of consequences of computer attacks to information resources of Russian Federation». In a development of this Decree, in December 2014, the President of the Russian Federation approved a Concept of a state system for Russia's information resources for detecting and preventing computer attacks, and mitigating their consequences. In accordance with this Concept, the main functions of the system are: to identify signs of computer attacks, to determine their sources and other related information, to forecast a situation in the field of information security of the Russian Federation, to collect and analyze information about computer attacks on information resources of the Russian Federation, and to react to attacks and eliminate their consequences [2].

In 2016, the «Information security doctrine of the Russian Federation» was adopted, where it is noted that «the state of information security in the field of state and public security is characterized by a constant increase in complexity, an increase in a scale and growth of cyberattacks to objects of critical infrastructures» [3]. The federal law «About security of a critical information infrastructure of Russian Federation» [1] notes that there is a mandatory requirement for an implementation of a state system for detecting and preventing cyberattacks on IS of critical infrastructures, and mitigating their consequences. This once again confirms the importance and relevance of issues of cybersecurity of

these facilities for the Russian Federation. Thus, scientific research on the development of new methods of protection against cyberattacks on IS of critical infrastructures is important and necessary.

One of the most promising research directions for solving the task of protecting against cyberattacks on IS of critical infrastructures is to create cyberattack intensity forecasting methods based on machine learning [4, 5]. Note that the cyberattack intensity is the total number of these attacks per unit time. If a forecast is received that the cyberattack intensity on IS exceeds a predetermined value, additional protection measures can be taken; for example, the more detailed analysis of traffic. It should be noted that in the federal law «About security of a critical information infrastructure of Russian Federation», as well as in «Concept of the state system for detecting, preventing and eliminating of consequences of computer attacks on the information resources of Russian Federation», the need for using forecasts in the cybersecurity field is underlined. Thus, in research related to protection against cyberattacks, in addition to assessing different risks and using traditional protection systems, attention should be paid to cyberattack intensity forecasting [6].

In the past few years, there has been an increasing interest of researchers in probabilistic forecasting [7, 8]. This can be explained by the fact that probabilistic forecasts make it possible to obtain not only forecasts of future events, but also probabilistic estimates of these events. One type of probabilistic forecasting is interval forecasting (IF) [9-11]: this involves forecasting of an interval (from two predetermined intervals) in which a future value of an indicator will be located. Probability estimates are used for this purpose. A dividing bound of these intervals is determined by a calculation method based on statistical characteristics of the indicator.

In this paper, for forecasting cyberattack intensity on IS of critical infrastructures it is recommended carry out IF based on a probabilistic neural network with dynamic updating of the smoothing parameter value (PNN) [10,11]. As a standard for comparing the results of IF, a naive Bayesian model (NBM) and probabilistic cluster model (PCM) were selected [12].

2. Description and formalization of a cyberattack intensity indicator

Given that information about the cyberattack intensity on IS is confidential, we have used another public indicator of cyberattack intensity. This indicator is the cyberattack number per day that occurred from 1998 to 2015 in South Korea [14]. This indicator has a large volume of values, suitable for constructing various machine learning models for IF. On the other hand, the chosen indicator is non-stationary with respect to the location and the scale parameters, which underlines its dynamic statistical characteristics [10]. Thus, if this indicator shows good results of cyberattack intensity IF, then we can more confidently draw similar conclusions with regard to IS.

This indicator was formalized as the time series:

$$\boldsymbol{z} = \{z_t : t \in \boldsymbol{t}\}, \quad (1)$$

z_t is the value of the indicator at the discrete moment of time t; $t \in \mathbf{t}$; $\mathbf{t} = \{1, \dots, n\}$; and n is the number of values. For the chosen indicator, $n = 1552$.

Let $[z_{min}; z_{max}]$ be the conditional range of possible values of the indicator (1), then z_α is the threshold of the cyberattack intensity ($z_{\min} \le z_\alpha \le z_{\max}$). The threshold of the cyberattack intensity z_α is a value for which the probability that $z_t \le z_\alpha$ equals α. Thus, z_α is the quantile of a probability distribution function of (1) for a given probability α.

Note that in a future scenario, with respect to the selected indicator, it is sufficient to take only the integer part of z_α, since the cyberattack intensity is always an integer value.

Further, it is proposed to perform the following completely reversible transformation of the original indicator (1):

$$\boldsymbol{q} = log(\boldsymbol{z} + 1) - log(z_\alpha + 1) = \{q_t : t \in \boldsymbol{t}\}. \quad (2)$$

Here q_t is the value of the indicator at the discrete moment of time t; $t \in \mathbf{t}$; $\mathbf{t} = \{1, \dots, n\}$; n is the number of values; and z_α is the threshold of the cyberattack intensity.

This conversion is useful for several reasons:

1) The values of the initial indicator (1) are in a very wide range, and some (extreme) values significantly exceed the others. Logarithmic transformation helps to improve visual work with such data and their associated graphs;

2) The indicator (2) contains both positive and negative values, in contrast to the indicator (1). Some forecasting models (including PNN) are sensitive to the sign of predictors and demonstrate better IF accuracy after such transformations;

3) The equivalent of z_α for the indicator (2) is always 0. That is, the distribution of positive and negative values relative to z_α for indicator (1) and relative to 0 for the obtained indicator (2) is identical, and this slightly simplifies the formalization of IF for the indicator (2) without distorting the essence and interpretation of the obtained results.

Figure 1 shows the graph of the obtained indicator (2).

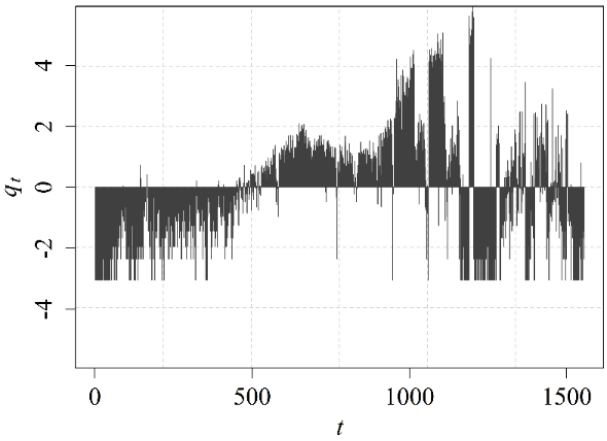

Figure 1. The graph of **q** (2) for $\alpha = 0.5$.

Thus, it should be noted that the transformation of the indicator (1) into the indicator (2) is an integral part of the implementation of IF.

For obtaining some statistical characteristics of this indicator, its class was determined by the method described in [10]. This indicator is an indicator of the first class, non-stationary in terms of the location and scale parameters, which indicates its distinct statistical nature among indicators of other classes [9,10].

3. Formalization of cyberattack intensity interval forecasting

Let $[q_{min}; q_{max}]$ be the conditional range of possible values of the indicator (2). Construct two intervals:

$$I^- = [q_{min}; 0],\ I^+ = (0; q_{max}]. \quad (3)$$

At time $t = n - 1$ it is necessary to identify the interval (3) in which the future (unknown) value q_{t+p} will be located. The following estimates of probabilities are required: ρ^+_{t+p} and ρ^-_{t+p} where $p = 1, \dots, r$ is the look-ahead period, ρ^+_{t+p} is the probability that the indicator future value $q_{t+p} \in I^+$; and ρ^-_{t+p} is the probability that the indicator future value $q_{t+p} \in I^-$; $\rho^+_{t+p} + \rho^-_{t+p} = 1$.

Let $\tilde{\rho}^+_{t+p}$ and $\tilde{\rho}^-_{t+p}$ be probability estimates of ρ^+_{t+p} and ρ^-_{t+p}. The interval forecasting is carried out according to the following rules: the future value $q_{t+p} \in I^+$ if $\tilde{\rho}^+_{t+p} > \tilde{\rho}^-_{t+p}$; and the future value $q_{t+p} \in I^-$ if $\tilde{\rho}^+_{t+p} \le \tilde{\rho}^-_{t+p}$.

4. Formalization of training set for learning of probabilistic models

It is necessary to consider some features of the formation of a training set for the implementation of IF.

Suppose $t = n$ and there is a sequence of values $q_{t-f+1}, \dots, q_t$ in a number of f. Create a vector $\mathbf{h} = (q_{t-f+1}, \dots, q_t)$. Let y_{t+p} be a dependent variable (or a response) the true value of which is unknown and that can take only two possible values: $y_{t+p} = 1$ if $q_{t+p} \in I^+$ and $y_{t+p} = -1$ if $q_{t+p} \in I^-$.

Performing IF using $\mathbf{h}$ requires making a forecast of y_{t+p} based on probability estimates that $q_{t+p} \in I^+$ and $q_{t+p} \in I^-$. Recall that if $\tilde{\rho}^+_{t+p} > \tilde{\rho}^-_{t+p}$, then $y_{t+p} = 1$, else $y_{t+p} = -1$.

Next, create a training set based on the values of $\mathbf{q}$ (1) for $t = 1, \dots, m$, where $m = n - f - p + 1$ (this value is chosen so that the responses' values can be calculated based on pre-history values of the indicator):

$$\mathbf{x} = \begin{pmatrix} q_1 & \cdots & q_{1+f-1} \\ & \cdots & \\ q_m & \cdots & q_{m+f-1} \end{pmatrix}, \ \mathbf{y} = (y_1, \dots, y_m). \tag{4}$$

Here $\mathbf{x}$ is the matrix of dimensions $m \times f$ (a training set); $\mathbf{y}$ is a vector of responses of size m (these responses are calculated based on the pre-history values of the indicator); and m is the number of training samples.

Each row i of the matrix $\mathbf{x}$ corresponds to the response of $\mathbf{y}$ (4): $\mathbf{x}_i \to \mathrm{y_i}$.

Using the training set (4), it is possible to build and train some forecasting model, and also implement the IF.

Often the matrix of predictors $\mathbf{x}$ is used not in pure form, but in the transformed one. For example, for PNN each row of $\mathbf{x}$ is transformed so that the sum of squares of each row of values is equal to 1. For NBM and PCM, this is not necessary.

5. General algorithm of interval forecasting of cyberattack intensity

The IF algorithm in its general form consists of the following stages:

- Prepare initial data: $\boldsymbol{z}$ (1);
- Set the parameter: α;
- Construct a piecewise linear probability distribution function of $\boldsymbol{z}$ (1) and estimate z_α for selected value of α;
- Transform $\mathbf{z}$ (1) to $\mathbf{q}$ (2);
- Set the parameters: p, f;
- Create the training set (4);
- Select a forecasting model and set its parameters (parameter values can be optimized based on the training set; for example, by cross-validation methods [15]);
- Carry out IF.

Thus, this algorithm has three parameters: α is the probability with which the cyberattack intensity will be below the threshold cyberattack intensity z_α; p is the ahead time; and f is the dimension of a training set.

6. Interval forecasting results and prospects of their practical application

For an analysis of IF results of cyberattack intensity, several scores were used. They are considered in more detail, and reasons are provided for choosing each of them.

First of all, we are interested in an accuracy with which the forecasting of events is carried out, $q_{t+p} \in I^+$. In fact, when obtaining such a forecast, it is necessary to take additional measures to protect against increasing cyberattacks. The more accurate such forecasts, the fewer mistaken additional measures will be taken to protect against cyberattacks (i.e. false positives). The fewer false positives, the more effective the system of protection against cyberattacks will be. For estimating the accuracy of such forecasts, it is proposed to use the score:

$$pr^+ = l^+/u^+, \tag{5}$$

where pr^+ is the estimation of forecasting accuracy of events $q_{t+p} \in I^+$, l^+ is the number of justified forecasts that $q_{t+p} \in I^+$, and u^+ is the total number of forecasts that $q_{t+p} \in I^+$, $0 \le pr^+ \le 1$.

Also, we are interested in the accuracy with which the forecasting of events $q_{t+p} \in I^-$ is carried out. Here, when we get a forecast that $q_{t+p} \in I^-$, the system of protection against cyberattacks continues to work in its regular mode. The more accurate such forecasts, the less likely situations will arise when, in fact, additional measures of protection from cyberattacks were required, but this was not done (i.e. false negative). This also affects the effectiveness of protection systems against cyberattacks. To estimate the corresponding accuracy of such forecasts, the following score was used:

$$pr^- = l^-/u^-, \tag{6}$$

where pr^- is the estimation of forecasting accuracy of events $q_{t+p} \in I^-$, l^- is the number of justified forecasts that $q_{t+p} \in I^-$, and u^- is the total number of forecasts that $q_{t+p} \in I^-$, $0 \le pr^- \le 1$.

Thus, the larger the both values pr^+ and pr^-, the better. It should be noted that the forecasting model should forecast both variants of events: $q_{t+p} \in I^+$ and $q_{t+p} \in I^-$. For example, the model that gives the result $pr^+ = 0.75$ and $pr^- = 0.80$ is preferable to the one that gives the result $pr^+ = 0.55$ and $pr^- = 0.95$. This allows to determine the final score characterizing the accuracy of the IF based on any selected model:

$$pr = min(pr^+, pr^-). \tag{7}$$

Here pr^+ is the estimation of forecasting accuracy of events $q_{t+p} \in I^+$ (5), and pr^- is the estimation of forecasting accuracy of events $q_{t+p} \in I^-$ (6). The larger the value of pr (7), the more accurate IF.

The testing of the selected models was carried out as follows. The training set (4) was divided into two parts. The first part included the even rows of **x** and elements of **y**. This part was used for training and optimizing models. The second part with odd rows of **x** and elements of **y** is used for obtaining forecasts. Subsequently, the second part was used for training and optimizing selected models, and the first part for obtaining forecasts. Next, the values (5-7) were estimated by the cross-validation method for two blocks [15].

The estimates of the scores (5-7) were carried out for different values of α from 0.20 to 0.80 with the step 0.1. In all cases, the parameter p was fixed and equal to 1. At a fixed valueα a sequential search of the parameter f from 1 to 10 values was carried out (this parameter is common for PNN, CPM, and NBM). For NBM, for each new value of f, the values of the smoothing parameter of a nonparametric density function of predictors are changed from 0.1 to 1 with the step 0.1. Among all the estimates obtained (7), such a model was chosen in its class, for which the value of (7) was maximal. All algorithms were implemented using the R language [16-18]. Table 1 shows the results obtained.

Table 1. Interval forecasting results.

Parameter, α	Threshold, z_α	PNN, pr	NBM, pr	PCM, pr
0.2	3	0.75	0.60	0.66
0.3	6	0.76	0.70	0.75
0.4	11	0.84	0.81	0.83
0.5	20	0.88	0.88	0.88
0.6	35	0.88	0.83	0.86
0.7	55	0.81	0.75	0.80
0.8	79	0.79	0.77	0.74

As follows from the above results, PNN is more accurate and acceptable in all cases. The highest accuracy is observed in the middle of the parameter values of α. In practice, the choice of the value of

α can be done experts. It should be noted that the range of α from 0.20 to 0.80 is quite sufficient for solving practical problems. It is not advisable to specify larger or smaller values of α, as this will lead to a serious «imbalance» in the training set, and the results of IF can consequently be unstable and inadequate.

It is possible that the additional measures to protect against cyberattacks should not be applied at the first hit of the future value in the interval I^+, but after several of hits. More research is needed in this direction.

7. Conclusion

As follows from the results of this work, interval forecasting of cyberattacks intensity on IS of critical infrastructures is a necessary and important practical task. Experiments showed that interval forecasting of cyberattack intensity based on a probabilistic neural network for the selected indicator is more accurate than other models.

Given that information about cyberattack intensity on IS of critical structures is confidential, the number of cyberattacks per day that occurred from 1998 to 2015 in South Korea was considered as an alternative indicator in this work [14]. This indicator was chosen because it is publicly available and it has a large volume of data, suitable for constructing various models of machine learning for the purpose of IF. On the other hand, the selected indicator is non-stationary in terms of the location and scale parameters, which underlines its dynamic statistical nature. Since this indicator showed good results of interval forecasting of cyberattack intensity, similar conclusions can be drawn with respect to the IS of critical infrastructures.

8. References

[1] Federal act of security of a critical information infrastructure of Russian Federation on 26–07–2017 189–FZ
[2] Extract from Concept of the state system for detection, prevention and liquidation of the consequences of computer attacks on information resources of Russian Federation, approved by the President of the Russian Federation on 12–12–2014 K1274.
[3] Presidential Decree of the approval of the Doctrine of information security of the Russian Federation.
[4] Petrenko S A and Petrenko A S 2016 The concept of early detection and prevention of computer attacks *Materials of Russian Scientific and Practical Conference «Information Systems and Technologies in Modeling and Control»* p 82–6
[5] Petrenko S A and Stupin D D 2017 National early warning system of computer attacks (Publishing house: «Athena»)
[6] Gandotra E, Bansal D and Sofat S 2015 Computational Techniques for Predicting Cyber Threats *Proceedings of Intelligent Computing, Communication and Devices* p 247–253
[7] Zhan Z, Xu M, and Xu S 2015 Predicting cyberattack rates with extreme values *IEEE Transactions on Information Forensics and Security* **10** (**8**) p 1666–1677
[8] Werner G, Yang S and McConky K 2017 Time series forecasting of cyberattack intensity *Proceedings of the 12th Annual Conference on Cyber and Information Security* p 224–240
[9] Krakovsky Y M and Luzgin A N 2017 *Applied aspects of application of interval forecasting in system analysis* Modern technology. System Analysis. Modeling **2**(**54**) p 115–121
[10] Kargapoltsev S K, Krakovsky Y M and Luzgin A N 2017 Nonparametric classification of technical condition parameters based on shift and scale tests *International Conference on Industrial Engineering, Applications and Manufacturing* p 1–5
[11] Kargapoltsev S K, Krakovsky Y M, Lukanov A V and Luzgin A.N 2017 A dynamic updating algorithm of smoothing parameter values of probabilistic neural networks *Far East Journal of Electronics and Communications* **17**(**4**) p 909–914
[12] Ethem A 2014 Introduction to Machine Learning: Massachusetts Institute of Technology *The MIT Press Cambridge* p 616

[13] Krakovsky Y M and Luzgin A N 2018 Robust interval forecasting algorithm based on a probabilistic cluster model *Journal of statistical computation and Simulation* **88**(**12**) p 2309–2324
[14] Han L, Han Ch, Kang R, Kwak I, Mohaisen A and Kim H 2016 WHAP: Web-hacking profiling using Case-Based Reasoning *IEEE Conference on Communications and Network Security* p 344–5
[15] Browne M 2000 Cross-validation methods *Journal of Mathematical Psychology* vol 44 p 108–132
[16] The R Project for Statistical Computing https://www.r-project.org
[17] Krakovsky Y M, Kurchinsky B V and Luzgin A N 2018 Cyber-attack intensity interval forecasting on objects of critical information infrastructure *Proceedings of Tomsk State University of Control Systems and Radioelectronics* **21** no 1 p 71–9
[18] Krakovsky Y M and Luzgin A N 2015 Software for interval prediction of non-stationary dynamic indicators *Proceedings of Irkutsk State Technical University* **1** no 4 p 12–16