Interval forecasting of cyber-attacks on industrial control systems

To cite this article: Y M Ivanyo et al 2018 IOP Conf. Ser.: Mater. Sci. Eng. 327 022044

View the article online for updates and enhancements.

Related content
- Research on Multi-level Electromagnetic Leakage Protection Strategy of Industrial Control System
  Yang Li, Feng Li, Xu Wang et al.
- Interval forecasting of cyberattack intensity on informatization objects of industry using probability cluster model
  Y M Krakovsky, A N Luzgin and E A Mikhailova
- Automated control system for a mashing process
  E Teterin and V Rudnickiy

This content was downloaded from IP address 207.241.231.82 on 29/04/2019 at 09:18
Interval forecasting of cyber-attacks on industrial control systems

Y M Ivanyo¹, Y M Krakovsky², A N Luzgin³

¹ Irkutsk State Agrarian University named after A.A. Ezhevsky, Molodezhny Settlement, Irkutsk, 664038, Russia
² Irkutsk State University of Railway Transport, 15, Chernyshevsky St., Irkutsk, 664074, Russia
³ Administration of Irkutsk City, 14, Lenina St., Irkutsk, 660025, Russia

E-mail: alexln@mail.ru

Abstract. At present, cyber-security issues of industrial control systems occupy one of the key niches in a state system of planning and management. Functional disruption of these systems via cyber-attacks may lead to emergencies related to loss of life, environmental disasters, major financial and economic damage, or disrupted activities of cities and settlements. There is then an urgent need to develop protection methods against cyber-attacks. This paper studied the results of cyber-attack interval forecasting with a pre-set intensity level of cyber-attacks. Interval forecasting is the forecasting of one interval from two predetermined ones in which a future value of the indicator will be obtained. For this, probability estimates of these events were used. For interval forecasting, a probabilistic neural network with a dynamic updating value of the smoothing parameter was used. A dividing bound of these intervals was determined by a calculation method based on statistical characteristics of the indicator. The number of cyber-attacks per hour that were received through a honeypot from March to September 2013 for the group ‘zeppo-norcal’ was selected as the indicator.

1. Introduction

An application of information technology for the disruption of key industrial control systems is called cyber-attacks [1,2]. In many organisations, both the middle and lower levels of the hierarchy of industrial automation systems use modern technologies for information exchange and process management. As a result of disruption via cyber-attacks, an emergency may arise resulting in loss of life, environmental disasters, major financial and economic damage, or disrupted activities of cities and settlements. Technology networks are often coupled to corporate networks. Here, cyber-attacks acquire a particular relevance as they can occur daily and their number grows exponentially. In this regard, research is needed on the development of new protection methods against cyber-attacks [3,4]. The disadvantage of most modern protection methods against cyber-attacks is that when identifying such attacks, known signatures or prototypes of certain processes or events are used. For example, antiviruses, firewalls, intrusion detection and prevention systems work this way. It is noted [5] that such systems are effective only for novice attackers. In this regard, there is a need to develop additional protection techniques against cyber-attacks. In particular, a perspective technique is cyber-attack forecasting based on machine learning [6-12].
Cyber-attack forecasting allows for advance preparation and heightened protection against cyber-attacks. For example, if a security officer receives an important forecast, he can apply additional protective measures such as disconnecting the Internet or turning on another work mode of the protection system. Some actions can be performed automatically if the cyber-attack forecasting algorithms are integrated into protection systems. Thus, in addition to assessing different risks from using traditional protection systems, attention should be paid to cyber-attack forecasting [6].

It should be noted that in the past few years, there has been increased interest in probabilistic forecasting [13]. This can be explained by the fact that probabilistic forecasts allow the obtaining of not only forecasts of future events, but also of probabilistic estimates of these events. Interval forecasting is an example of this. Interval forecasting is the forecasting of one interval from two predetermined ones in which a future value of the indicator will be obtained. Probability estimates of the events are used in calculation. A dividing bound of these intervals is determined by a calculation method based on the statistical characteristics of the indicator.

For this study, the number of cyber-attacks per hour that were received through a honeypot from March to September 2013 for the group ‘zeppo-norcal’ was selected as the indicator [14]. For analyzing ‘fronts’ of the start and end of cyber-attacks, the author of [14] recommended to apply to a simple moving average to the indicator. This approach reduces the influence of outliers and high-frequency noise in the source data. Taking into account these recommendations, the simple moving average of the source data with the window width of 4 hours was applied, and a corresponding indicator (ZNI) was obtained. To obtain some statistical characteristics of this indicator, its class was determined by the described method in [15]. Afterwards, a study of cyber-attack interval forecasting results based on a probabilistic neural network [16] with a dynamic updating value of the smoothing parameter [17] was carried out. The obtained results demonstrate the high accuracy of the interval forecasting.

2. Formalization and classification of a cyber-attack indicator
A cyber-attack indicator is formalized as the time series:

\[ q = \{ q_t : t \in \mathbb{T} \} \]

Here, \( q_t \) is the value of the indicator at the discrete moment of time \( t \); \( t \in \mathbb{T} \); \( \mathbb{T} = \{0, \ldots, n-1\} \); \( n \) is the number value. For the selected indicator \( n = 4374 \).

Figure 1 shows a graph of 500 last values of ZNI.

![Graph of the last 500 ZNI values](image)

**Figure 1.** A graph of the last 500 ZNI values.

Calculations show ZNI is a first-class indicator [15]. This indicator is the most difficult class for the implementation of interval forecasting (in the statistical sense).
3. Interval forecasting formalization

Define the range \((q_{\text{min}}, q_{\text{max}})\) of possible values \(q\) (1) and an inner point (a dividing bound of intervals) \(\hat{q}\) \((q_{\text{min}} < \hat{q} < q_{\text{max}})\) and construct two intervals:

\[
I^- = (q_{\text{min}}, \hat{q}), I^+ = (\hat{q}, q_{\text{max}}).
\]

The value of \(\hat{q}\) in (2) is proposed as follows:

\[
\hat{q} = \text{med}(q) + \beta \times \text{med}(|q - \text{med}(q)|) = \text{med}(q) + \beta \times \text{MAD}(q).
\]

Here \(\beta \in [-1; 1]\) is a coefficient (the value is set beforehand); \(\text{med}(\cdot)\) is median; \(\text{MAD}(\cdot)\) is the median absolute deviation.

At time \(t = n - 1\) it is necessary to identify which of the intervals (2) the future (unknown) value \(q_{t+p}\) will be in. The following estimates of probabilities are required: \(\rho_{t+p}^-\) and \(\rho_{t+p}^+\), where \(p = 1, \ldots, r\) is the look-ahead period, \(\rho_{t+p}^+\) is the probability that the indicator future value \(q_{t+p} \in I^+\); \(\rho_{t+p}^-\) is the probability that the indicator future value \(q_{t+p} \in I^-\); \(\rho_{t+p}^+ + \rho_{t+p}^- = 1\). The interval forecasting is carried out according to the following rules: the future value \(q_{t+p} \in I^+\) if \(\rho_{t+p}^+ > \rho_{t+p}^-\); and the future value \(q_{t+p} \in I^-\) if \(\rho_{t+p}^- \leq \rho_{t+p}^+\).

It is necessary to consider expression (3) in detail. Note that the indicator (1) is considered as a random variable with some unknown probability distribution function whose robust characteristics are the location parameter and the scale parameter. These parameters characterize the center of the grouping of random variable values and the degree of deviation of random variable values relative to this center [15].

In the expression (3), the first term is the location parameter estimate, and the second term is the scale parameter estimate that is multiplied by \(\beta \in [-1; 1]\). Using \(\hat{q}\), the value of \(\hat{q}\) can change in the range of \(\text{med}(q) - \text{MAD}(q)\) to \(\text{med}(q) + \text{MAD}(q)\). For \(\beta = -1.0\) the interval \(I^+\) contains about 75% all values of \(q\) (1) and for \(\beta = 1.0\), the interval contains about 25%. The value variation of \(\hat{q}\) in this range is enough by further research.

It should also be noted that the cyber-attack intensity is the total number of these attacks per unit of time (in our case an hour). With this in mind, the value of \(\hat{q}\) (3) was called the pre-set level of the cyber-attack intensity. The higher the value of \(\hat{q}\) (3), the more intense a cyber-attack must be in order to get into the interval \(I^+\) (2). It is needed to set \(\beta\) for which the interval forecasts of \(q_{t+p} \in I^+\) will indicate a necessity for additional protective measures. Forecasts of \(q_{t+p} \in I^-\) will be considered as a usual situation and will remain without attention. The lower the value of \(\beta\), the more often the forecasts of \(q_{t+p} \in I^+\) will be made (and vice versa). Of course, in each specific case and in each particular organization, the values of \(\beta\) can be chosen by experts and, consequently, these values can be different.

4. Results and discussion

In analyzing the cyber-attack interval forecasting results, two scores were used:

\[
ps = \frac{l}{u}, \quad bs = \frac{1}{u} \sum_{t \in G} \left(\tilde{\rho}_{t+p}^+ - \nu_{t+p}^\top\right)^2.
\]

Here \(l\) is the number of true forecasts; \(u\) is the total number of forecasts; \(\tilde{\rho}_{t+p}^+\) is the probability estimate of \(\rho_{t+p}^+\) based on a selected model; \(G\) is the set of values \(t\) at which the forecasts were
made; $v_{t+p}$ is the outcome of the event (equal to 1 if $q_{t+p} \in I^+$ and equal to 0 if $q_{t+p} \in I^-$); $ps$ is the frequency of true forecasts [17]; $bs$ is the Brier score (the measure of the forecasting accuracy) [18,19]; $0 \leq ps \leq 1$; $0 \leq bs \leq 1$. The higher the value of $ps$ and the lower the value of $bs$, the better the interval forecasting accuracy. The values were estimated by the leave-one-out cross-validation method.

For the implementation of all algorithms, R [20] was used. At the same time, for accelerating of some functions and procedures, C ++ was used. For the integration of R and C ++, Rcpp-package was used [21].

Table 1 shows the interval forecasting results of the cyber-attacks one hour ahead ($p=1$) for different values of $\beta$ and values of $f$ for which the interval forecasting accuracy was maximum. The value of $f$ was varied from 1 to 10. In addition, the frequency ($sa$) of the indicator values (1) that are in $I^+$ for a set value of $\beta$ is given.

Table 1. Interval forecasting results

| $\beta$ | $f$ | $ps$ | $bs$ | $sa$ |
|---------|-----|------|------|------|
| -1.0    | 7   | 0.77 | 0.15 | 0.75 |
| -0.8    | 6   | 0.75 | 0.17 | 0.69 |
| -0.6    | 6   | 0.73 | 0.18 | 0.64 |
| -0.4    | 7   | 0.72 | 0.19 | 0.58 |
| -0.2    | 6   | 0.70 | 0.20 | 0.52 |
| 0.0     | 6   | 0.69 | 0.20 | 0.47 |
| 0.2     | 7   | 0.71 | 0.19 | 0.41 |
| 0.4     | 7   | 0.72 | 0.18 | 0.37 |
| 0.6     | 7   | 0.74 | 0.18 | 0.33 |
| 0.8     | 6   | 0.76 | 0.17 | 0.29 |
| 1.0     | 6   | 0.79 | 0.15 | 0.25 |

According to Table 1, it is clear that the interval forecasting accuracy of the cyber-attacks for selected indicator is quite high. The minimum value of $ps$ is 0.69 and the maximum value of $bs$ is 0.20. With a linear increase of the value of $\beta$, the frequency of the cyber-attacks (which are in $I^+$) nonlinearly decreases from 0.75 to 0.25. Thus, cyber-attack interval forecasting based on a probabilistic neural network with a dynamic updating value of the smoothing parameter copes with the task successfully for all values of $\beta$.

Taking into account the obtained results, the following scheme for protection against cyber-attacks using interval forecasting is recommended:

1) Determine the value of $\beta$ and, accordingly, the value of $\hat{q}$ (5). For example, this can be done empirically or by expert judgment. Here, an additional criterion for choosing a value of $\beta$ can be the frequency ($sa$) of the values of $q$ (1) that are in $I^+$. This value is easily calculated based on the values of $q$ (1);

2) Estimate by leave-one-out cross-validation the value of $f$ at which the value of $bs$ (4) is minimum;

3) Make an interval forecast for the hour ahead ($p=1$). If $q_{t+p} \in I^+$, then implement the additional measures (they can be automatic) against the cyber-attacks. If $q_{t+p} \in I^-$, then proceed normally;

4) After one hour, add a new value to the end of $q$ (1) and return to step 3.
It should be added that the pre-set level of the cyber-attack intensity (3) can be periodically reviewed because, for example, the cyber-attacks to an industrial control system grow in number.

Conclusion
The analysis of contemporary scientific studies has shown that for several years the scientific community is carrying out research on cyber-attack forecasting by different methods with the target of creating adequate instruments of protection against cyber-attacks. The paper studied the interval forecasting results of cyber-attacks based on intelligent modeling. A probabilistic neural network with a dynamic updating value of the smoothing parameter was used. This approach allows carrying out the cyber-attack interval forecasting with a pre-set intensity level of cyber-attacks. The approach demonstrates the high accuracy of cyber-attack interval forecasts for selected data. At the same time, the necessary practical recommendations on an application of the interval forecasting results to the protection against the cyber-attacks in industrial control systems were formulated. It should be noted that similar studies about cyber-attack interval forecasting are not known to the authors, so this work can be considered one of the first works. The obtained results can find a practical application and further theoretical development in the protection against cyber-attacks.

References
[1] Amoroso E 2013 Cyber Attacks: Protecting National Infrastructure (United Kingdom: Butterworth-Heinemann)
[2] Loukas G 2015 Cyber-Physical Attacks. A Growing Invisible Threat (United Kingdom: Butterworth-Heinemann)
[3] Mezzour G, Carley L R and Kathleen M 2014 Global Mapping of Cyber Attacks (USA: Carnegie Mellon University)
[4] Han M L, Han H C, Kang A R, Kwak D I, Mohaisen A and Kim H K 2016 WHAP: Web-hacking profiling using Case-Based Reasoning IEEE Communication and Network Security (Philadelphia: IEEE) pp. 344–5.
[5] Jones M, Kotsalis G and Shamma J S 2013 Control of Cyber-Physical Systems. Lecture Notes in Control and Information Sciences (Luxembourg: Springer)
[6] Gandotra E, Bansal D and Sofat S 2015 Computational Techniques for Predicting Cyber Threats Proc. Intelligent Computing, Communication and Devices (AISC, vol 308) ed J Kacprzyk (New Delhi: Springer ) pp. 247–53
[7] Kim Y, Lee T, In H Chung Y J, Kim I and Baik D K 2005 A probabilistic approach to estimate the damage propagation of cyber attacks Proc. Information Security and Cryptology (ICISC, vol 3935) ed D Won, S Kim (Seoul: Springer) pp. 175–85
[8] Wu J 2012 Cyber Attacks Prediction Model Based on Bayesian Network IEEE Parallel and Distributed Systems (Singapore:IEEE) pp. 730–731
[9] Du H 2017 Probabilistic Modeling and Inference for Obfuscated Network Attack Sequences (New York:Rochester Institute of Technology)
[10] Zhan Z, Xu M and Xu S 2015 Predicting cyber attack rates with extreme values IEEE Transactions on Information Forensics and Security (TIFS, vol 10) ed M Barni (Siena: IEEE) pp. 1666–77
[11] Munkhdorj B, Yuji S 2017 Cyber attack prediction using social data analysis Journal of High Speed Networks 23(2) 109–135
[12] Werner G, Yang S and McConky K 2017 Time series forecasting of cyber attack intensity Proc. of the 12th Annual Conference on Cyber and Information Security Research ed R Bridges (Tennessee: Oak Ridge National Laboratory) pp. 18–25
[13] Elliott G, Granger A 2013 Handbook of Economic Forecasting (Amsterdam: Elsevier)
[14] Data driven Security, http://datadrivensecurity.info/blog/posts/2014/Jan/blander-part1
[15] Kargapolov S K, Krakovsky Y M and Luzgin A N 2016 Nonparametric classification of technical condition parameters based on shift and scale tests IEEE Industrial Engineering,
Applications and Manufacturing ed A Radionov (Saint-Petersburg: IEEE) pp. 1–5

[16] Specht D H 1990 Probabilistic Neural Networks *Neural Networks* 3 109–118

[17] Kargapol'tsev S K, Krakovsky Y M, Lukyanov A V and Luzhin A N 2017 A dynamic updating algorithm of smoothing parameter values of probabilistic neural networks *Far East Journal of Electronics and Communications* 17(4) 909–914

[18] Scolnik R 2016 *Predictive Accuracy Measures for Binary Outcomes: Impact of Incidence Rate and Optimization Techniques* (Florida: Florida State University)

[19] Rufibach K 2010 Use of Brier score to assess binary predictions *Journal Clinical of Epidemiology* 63(8) 938–939

[20] The R project of statistical computing, http://www.r-project.org

[21] Seamless R and C++ Integration, https://cran.r-project.org/web/packages/Rcpp/index.html