A Proactive Protection by Computational Intelligence Methods

Subjects: Computer Science, Information Systems

Contributor: Igor Kotenko, Igor Saenko, Oleg Lauta, Alexander Kribel

A combination of computational intelligence methods: identifying anomalies in network traffic by evaluating its self-similarity, detecting and classifying cyberattacks in anomalies, and taking effective protection measures using Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) cells.

Keywords: time series ; fractal analysis ; fractal dimension ; Hurst exponent

1. Introduction

World trends in information and telecommunication technologies based on digital methods of information transmission, processing, storage, presentation, and protection consist in the mutual penetration and “merging” of information and telecommunication systems not only at the level of technologies for their development and operation, but also their structural and functional association. In this case, the term “data transmission network” (DTN) is widely used [1].

There is an integration and convergence of networks and services. This provides users with access to any service available in multiple networks, due to the flexible possibilities for their processing and management. As a result, on the one hand, the efficiency, reliability, economic benefits, and sustainability of the DTN operation increase. On the other hand, it gives the malefactors the opportunity to act by implementing cyberattacks (CAs) [2].

There are many reasons why it becomes possible to implement CAs. It can be an operating system or other software that has not been updated in time. In addition, outdated security features or vulnerabilities inherent in poorly protected network protocols can lead to attacks. As a result, an attacker can perform various malicious actions, such as blocking network communication, making unauthorized access to DTN devices, controlling traffic, changing network device parameters, and other actions.

The category of dangerous services includes services whose placement on the perimeter carries increased risks: file system access services, Remote Procedure Call (RPC), directory services, printers, virtualization system service interfaces, Virtual Private Network (VPN), DTN-specific systems, network device services, Telnet, Secure Shell Protocol (SSH), Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), and others [3]. In addition, it should be noted that security flaws in service protocols that lead to traffic redirection and interception of network configuration information, security flaws in the NetBIOS Name Service (NBNS) and Link-Local Multicast Name Resolution (LLMNR) protocols, as well as the use of open (unsecured) data transfer protocols in modern DTNs, have a high level of risk [4]. As practice shows, the vast majority of successful CAs are based on the exploitation of vulnerabilities in some resources that should not be available on the network perimeter [5].

This fully applies to information systems in the energy sector, built according to the Smart Grid (SG) concept. In accordance with this concept, the priority areas for the development of DTN in the energy sector for the coming years include [6]:

- widespread introduction at new and upgraded measurement points of intelligent measuring instruments—“smart” meters with the function of remote control of the load profile of the measured line and measuring transducers with standard communication interfaces and protocols that comply with information security standards;
- installation at each large facility connected to the power grid, advanced automated information-measuring systems operating in real-time;
- creation of a wide network of integrated communications based on various communication lines;

- implementation of automated production management systems in energy companies.

The application of modern information technologies (ITs) makes it possible to significantly increase SGs operation efficiency, making them more reliable and economical, which, in its turn, leads to a reduction in the cost of power reproduced or distributed by them. However, at the same time, there are opportunities to influence SGs by various CAs. A consequence of this impact is the appearance of anomalies in the SG network traffic [6].

Detecting CAs in SGs is quite a complex task. It is necessary to constantly monitor security and control network traffic in order to detect anomalous activity in it. If traffic anomalies are detected, it is necessary to analyze a large number of routes in the network, where sharp fluctuations in traffic, delays in its transmission, or large packet losses appear. At the same time, a high quality of telecommunications service and application service should be ensured. All of this is the motivation for finding and developing new methods and approaches for CAs detection in SGs. Such approaches in this research include an approach that combines several methods of computational intelligence: the use of fractal analysis, statistical methods, and machine learning.

It should be noted that a fairly large number of classification and prediction methods mostly related to anomaly detection [7][8] are currently known and widely used. In particular, regression-based methods have performed well. These include non-parametric regression and classification tree method (CART) [9], multivariate adaptive regression splines (MARS) [10] [11], support vector regression (SVR) [12] and others. Regression-based methods demonstrate high classification and prediction performance if their parameters are well-tuned. In some cases (for example, for MARS and SVR), it is proposed to use genetic algorithms to adjust the regression parameters.

However, this does not allow one to speak about the possibility of early detection of CAs. Therefore, it is believed that the most effective method of classification and prediction is the Long Short-Term Memory (LSTM) neural network algorithm. The LSTM property of recurrence allows an Artificial Neural Network (ANN) to “refer” to the results of its work in the past, to analyze predictions. Thus, the content of decisions made to protect SGs from CAs will depend not only on the results of initial training of the LSTM network, but also on the results of further operation of this network in the flow [13][14].

The key parameter of fractal analysis is the Hurst exponent. This measure is used in the analysis of time series. The Hurst exponent shows the amount of delay in the time series between two identical pairs of values. The bigger it is, the smaller this parameter is. To find this parameter, it is first necessary to check the process under study for stationarity. The presence or absence of stationarity of the process influences the choice of the algorithm by which the scaling index can be calculated.

Fractal properties are more pronounced in non-stationary network traffic, which is predominant in SGs on large data scales. On small amounts of data, or in application layer protocols of the TCP/IP (Transmission Control Protocol/Internet Protocol) model, network traffic can be stationary and show less fractal properties. In this case, machine learning methods are used for further analysis.

Thus, in order to detect and classify the CAs, first, it is necessary to determine whether the traffic is stationary or non-stationary. Next, you should calculate the Hurst exponent (i.e., determine the presence of the self-similarity property in the traffic). In the final stage, anomalies are detected and measures are developed to protect the SG using LSTM [6][15].

2. A Proactive Protection by Computational Intelligence Methods

Fractal analysis, which studies the properties of self-similarity, is currently in a phase of active development. Fractal analysis is widely used for state monitoring problems, in which time series are investigated. For example, [16] proposes to use the R/S analysis method to analyze the self-similarity of time series. The self-similarity properties of the Voice Over Internet Protocol (VoIP) traffic are modeled and studied in [17]. The fractal dimension, which is an additional measure with respect to the Hurst exponent, is investigated in [18]. The reasons explaining the presence of self-similarity properties in telecommunication traffic are given in [19]. However, the main area of research in all these papers, as a rule, is both VoIP-telephony and economic systems.

At the same time, it should be noted that there are few practical experiments aimed at studying the fractal properties of the network traffic in information and telecommunication systems. Among such works, researchers can single out works [20][21][22]. However, [20] considers the mobile communication traffic generated by cellular stations. The researchers conclude that the properties of self-similarity are inherent not only in computer and telecommunications networks, but also in the radio waves on which cellular stations operate. Self-similarity of motion is considered in [21][22]. To detect it, it is

proposed to use visual cues, which allow one to find similar areas on the motion graph. These areas allow one to identify self-similar processes.

One of the first works, in which the main attention was paid to the self-similarity property of the network traffic, is the work [11]. It significantly changed the existing ideas about the processes taking place in information and telecommunication networks. These issues will be discussed in more detail in the next section. In addition, researchers should mention some works in which the mathematical models designed to describe self-similarity in network traffic have been proposed and investigated [23][24]. However, these works cannot be considered exhaustive, since they did not consider the issues of CA detection. Consequently, researchers can assume that their work, on the one hand, further develops the theoretical positions achieved in the study of the fractal properties of the network traffic. On the other hand, it develops the well-known solutions further in the direction of creating a method that makes it possible to detect network traffic anomalies caused by the impact of CAs.

At the same time, it should be noted that when considering threats to SG security, one should be guided by the following two indicators that characterize these threats. The first indicator is the probability of the threat realization. The second indicator is the potential damage that can be incurred by the power company in case of security threat realization [6][14]. Considering and combining these indicators, it is possible to substantiate the choice of the most acceptable threat models for SGs and to create protection systems for them, in which the decisions made would allow one to minimize security risks.

The first group [25][26][27][28][29][30][31] summarizes the techniques based on quantitative criteria. Thus, [25] proposes to use the acceptable level of the possible damage from information and technical impact on SG resources and the assessment of the profit factor from investments in protective measures as a measure to rank threat models. Quantitative methods comply with the requirements of ISO 27,001 and 27,002, NIST, and COBIT IV [26][27]. Although these methods take into account the predetermined risk appetite, they do not consider the variability in the construction of the SG protection system [28]. In addition, one of the significant disadvantages of the aforementioned methods is the high cost and complexity of their implementation [29]. At the same time, the complexity of quantitative methods is due to the need to take into account each potential security threat in the formation of options for counteracting CAs and developing solutions to eliminate the consequences of CAs [30]. For these purposes, [31] proposes to perform the ranking of security SG risks. Although this technique is undoubtedly of interest, it contains a number of negative factors associated with the problem of cloud resources.

The second group of methods [32][33][34][35] received the generally accepted name of qualitative methods. These methods apply qualitative indicators and criteria for the characterization of SG security threats. The essence of qualitative methods is the search for such a solution, in which the necessary balance is observed between the costs spent on building the protection system and the effect achieved with its help. Such methods form a direction called Cost/Benefit Analysis. In these methods, basically, different positions of the game theory, for example, matrix games are used. Speaking about the disadvantages of qualitative methods, it is necessary to point out their comparatively high computational complexity. It is due to the need to conduct a security risk analysis in order to make an economic justification for the introduction of protection mechanisms and means for various threat models into SG protection systems. Methods using qualitative criteria are similar in essence to the Facilitated Risk Analysis Process (FRAP) method [36][37].

The third approach [38][39][40][41] is an integrated one; it rationally combines the first and second groups of methods. Most often, the methods of this group find their application in small and medium-sized energy companies. The disadvantages of these methods include, as a rule, a very small amount of analytical data characterizing the potential damage under the given models of CA realization, as well as insufficiently complete risk assessment.

Besides, the works [42][43] present a structured approach to assessing the threat model for information and telecommunication resources (methods “CRAMM”, “MEHARI”). Here an integrated representation of the information security threat parameters is performed, but the specificity of building the SG protection system is practically not considered.

There is a well-known methodology for managing the information security system—Microsoft Security Assessment Tool (MSAT) [44][45]. This tool uses a mechanism for ranking threat models. In addition, the tool provides countermeasures for SG security threats and evaluates their effectiveness. However, the tool is not scalable enough. That is why in SG it is usually implemented in local computing networks or in companies with fewer than 1000 employees. The Risk Management Guide [34] is the basis for this tool’s design and operation. Among the main functions performed by the tool, in addition to risk assessment and decision support, one can include performance monitoring and evaluation [13].

Thus, all the considered approaches to CA early detection and prediction are based either on an in-depth analysis of possible risks (probable damage), or on a selective ranking of threats and defenses. In researchers' opinion, these approaches are insufficient to protect SGs from CAs. For this reason, this research discusses the key points of building an improved system for CA early detection, which can be called proactive. The proactivity of the system lies in the fact that it implements anomaly detection in the network traffic, their identification, and classification based on fractal analysis methods, and a neural network with a long short-term memory, which allows one to reduce risks in the implementation of CAs. The consideration of the proposed system is architecture-oriented. On the one hand, it goes beyond an abstract representation, and on the other hand, it does not pay much attention to technical details.

References

1. Kaur, S.; Goel, R. A Review on Data Transmission Techniques for Energy Efficiency in Wireless Sensor Networks. In Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 23–25 March 2016; pp. 699–703.
2. Vyshnavi, S.B.; Sree, S.R.; Jayapandian, N. Network Security Tools and Applications in Research Perspective. In Proceedings of the 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 12–14 December 2019; pp. 655–659.
3. Mellia, M.; Zincir-Heywood, N.; Diao, Y. Overview of Network and Service Management. In Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning; IEEE: Piscataway, NJ, USA, 2021; pp. 1–18.
4. Belej, O.; Nestor, N.; Polotai, O.; Sadeckii, J. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. In Proceedings of the 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2–6 July 2019; pp. 317–322.
5. Uçtu, G.; Alkan, M.; Doğru, İ.A.; Dörterler, M. Perimeter Network Security Solutions: A Survey. In Proceedings of the 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 11–13 October 2019; pp. 1–6.
6. Kotenko, I.; Saenko, I.; Lauta, O.; Kribel, A. An Approach to Detecting Cyber Attacks against Smart Power Grids Based on the Analysis of Network Traffic Self-Similarity. Energies 2020, 13, 5031.
7. Ageev, S.; Kotenko, I.; Saenko, I.; Kopchak, Y. Abnormal Traffic Detection in Networks of the Internet of Things Based on Fuzzy Logical Inference. In Proceedings of the IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg, Russia, 19–21 May 2015; pp. 5–8.
8. Desnitsky, V.A.; Kotenko, I.V.; Nogin, S.B. Detection of Anomalies in Data for Monitoring of Security Components in the Internet of Things. In Proceedings of the IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg, Russia, 19–21 May 2015; pp. 189–192.
9. Brezigar-Masten, A.; Masten, I. CART-based selection of bankruptcy predictors for the logit model. Expert Syst. Appl. 2012, 39, 10153–10159.
10. Ju, X.; Chen, V.C.P.; Rosenberger, J.M.; Liu, F. Fast knot optimization for multivariate adaptive regression splines using hill climbing methods. Expert Syst. Appl. 2021, 171, 114565.
11. Ju, X.; Rosenberger, J.M.; Chen, V.C.P.; Liu, F. Global optimization on non-convex two-way interaction truncated linear multivariate adaptive regression splines using mixed integer quadratic programming. Inf. Sci. 2022, 597, 38–52.
12. Ju, X.; Liu, F.; Wang, L.; Lee, W.-J. Wind farm layout optimization based on support vector regression guided genetic algorithm with consideration of participation among landowners. Energy Convers. Manag. 2019, 196, 1267–1281.
13. Kotenko, I.; Saenko, I.; Lauta, O.; Karpov, M. Methodology for Management of the Protection System of Smart Power Supply Networks in the Context of Cyberattacks. Energies 2021, 14, 5963.
14. Kotenko, I.; Saenko, I.; Lauta, O.; Kribel, A. Ensuring the survivability of embedded computer networks based on early detection of cyber attacks by integrating fractal analysis and statistical methods. Microprocess. Microsyst. 2022, 90, 104459.
15. Leland, W.E.; Taqqu, M.S.; Willinger, W.; Wilson, D.V. On the self-similar nature of Ethernet traffic. SIGCOMM Comput. Commun. 1993, 23, 183–193.
16. Raimundo, M.S.; Okamoto, J., Jr. Application of Hurst Exponent (H) and the R/S Analysis in the Classification of FOREX Securities. Int. J. Model. Optim. 2018, 8, 116–124.

17. Dang, T.D.; Sonkoly, B.; Molnar, S. Fractal analysis and modeling of VoIP traffic. In Proceedings of the 11th International Telecommunications Network Strategy and Planning Symposium (NETWORKS 2004), Vienna, Austria, 13–16 June 2004; IEEE: Vienna, Austria, 2004; pp. 123–130.
18. Sánchez-Granero, M.J.; Fernández-Martínez, M.; Trinidad-Segovia, J.E. Introducing fractal dimension algorithms to calculate the Hurst exponent of financial time series. Eur. Phys. J. B 2012, 85, 1–13.
19. Grillo, D.; Lewis, A.; Pandya, R. Personal Communication Services and Teletraffic Standardization in ITU-T. In The Fundamental Role of Teletraffic in the Evolution of Telecommunications Networks, Proceedings of the 14th International Teletraffic Congress—ITC 14, Antibes Juan-les-Pins, France, 6-10 June 1994; Labetoulle, J., Roberts, J.W., Eds.; Elsevier: Amsterdam, The Netherlands, 1994; pp. 1–12.
20. Strelkovskaya, I.; Solovskaya, I.; Makoganiuk, A. Spline-Extrapolation Method in Traffic Forecasting in 5G Networks. J. Telecommun. Inf. Technol. 2019, 3, 8–16.
21. Ju, F.; Yang, J.; Liu, H. Analysis of Self-Similar Traffic Based on the On/Off Model. In Proceedings of the 2009 International Workshop on Chaos-Fractals Theories and Applications, Shenyang, China, 6–8 November 2009; pp. 301–304.
22. Fractal Objects and Self-Similar Processes. Available online: https://archive.physionet.org/tutorials/fmnc/node3.html (accessed on 15 January 2022).
23. Ruoyu, Y.; Wang, Y. Hurst Parameter for Security Evaluation of LAN Traffic. Inf. Technol. J. 2012, 11, 269–275.
24. Ably, P.; Flandrin, P.; Taqqu, M.S.; Veitch, D. Self-Similarity and long-range dependence through the wavelet lens. In Theory and Applications of Long Range Dependence; Birkhauser Press: Boston, MA, USA, 2002; pp. 345–379.
25. Canadian Electricity Association. Canadian Smart Grid Framework; Canadian Electricity Association: Calgary, AB, Canada, 2010.
26. Federal Office for Information Security. Protection Profile for the Gateway of a Smart Metering System; V.1.2; Federal Office for Information Security: Bonn, Germany, 2014.
27. European Network and Information Security Agency (ENISA). Smart Grid Security: Recommendations for Europe and Member States; ENISA: Athens, Greece, 2015.
28. ISO/IEC 27005; Information Technology—Security Techniques—Information Security Risk Management. ISO: Geneva, Switzerland, 2008.
29. ISO/IEC TR 27019:2013; Information Security Management Guidelines based on ISO/IEC 27002 for Process Control Systems Specific to the Energy Utility Industry. ISO: Geneva Switzerland, 2013.
30. Kendrick, D.; Groom, L.; Stewart, J.; Watson, M.; Mulvaney, C.; Casterton, R. “Risk Watch”: Cluster randomised controlled trial evaluating an injury prevention program. Inj. Prev. 2007, 13, 93–99.
31. Fang, X.; Misra, S.; Xue, G.; Yang, D. Managing smart grid information in the cloud: Opportunities, model, and applications. IEEE Netw. 2012, 26, 32–38.
32. Prasad, I. Smart Grid Technology: Application and Control. Int. J. Adv. Res. Electr. Electron. Instrum. Eng. 2014, 3, 9533–9542.
33. Müller, K.J. Verordnete Sicherheit—Das Schutzprofil für das Smart Metering Gateway. Datenschutz Datensicherheit 2014, 35, 547–551.
34. Protection Profile for the Security Module of a Smart Metering System (Security Module PP). Available online: http://www.commoncriteriaportal.org/files/ppfiles/pp0077b_pdf.pdf (accessed on 15 January 2022).
35. Anwar, A.; Mahmood, A. Cyber Security of Smart Grid Infrastructure. In The State of the Art in Intrusion Prevention and Detection; CRC Press: Boca Raton, FL, USA, 2014; pp. 139–154.
36. Bale, J.P.M.; Sediyono, E.; Marwata, M. Risk management in information technology using facilitated risk analysis process (FRAP) (case study: Academic information systems of Satya Wacana Christian University). J. Theor. Appl. Inf. Technol. 2014, 68, 339–351.
37. Nurul, A.H.; Zaheera, Z.A.; Puvanasvaran, A.P.; Zakaria, N.A.; Ahmad, R. Risk assessment method for insider threats in cyber security: A review. Int. J. Adv. Comput. Sci. Appl. 2018, 9, 16–19.
38. Tankard, C. Advanced persistent threats and how to monitor and deter them. Netw. Secur. 2011, 2011, 16–19.
39. Lekidis, A. Cyber-Security Measures for Protecting EPES Systems in the 5G Area. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES ’22), Vienna, Austria, 23–26 August 2022.
40. Bella, H.K.; Vasundra, S. A study of Security Threats and Attacks in Cloud Computing. In Proceedings of the 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 January

2022; pp. 658–666.

41. Sterbenz, J.P.G.; Hutchison, D.; Çetinkaya, E.K.; Jabbar, A.; Rohrer, J.P.; Schöller, M.; Smith, P. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Comput. Netw. 2010, 54, 1245–1265.
42. El Fray, I. A Comparative Study of Risk Assessment Methods, MEHARI & CRAMM with a New Formal Model of Risk Assessment (FoMRA) in Information Systems. In Computer Information Systems and Industrial Management. CISIM 2012. Lecture Notes in Computer Science; Cortesi, A., Chaki, N., Saeed, K., Wierzchoń, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7564, pp. 428–442.
43. Syalim, A.; Hori, Y.; Sakurai, K. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. In Proceedings of the 2009 International Conference on Availability, Reliability and Security, Fukuoka, Japan, 16-19 March 2009; IEEE: New York, USA, 2009; pp. 726–731.
44. MEHARI. Overview. Available online: http://meharipedia.x10host.com/wp/wp-content/uploads/2019/05/MEHARI-Overview-2019.pdf (accessed on 15 January 2022).
45. Microsoft Security Center of Excellence. Available online: http://www.microsoft.com/rus/technet/security (accessed on 15 January 2022).