Method of Early Detection of Information Security Anomalies and Incidents in Information Systems

Hryhorii Hnatiienko[1], Tetiana Babenko[1], Yuliia Kovalova[2] and Larysa Myrutenko[1]

[1] *Taras Shevchenko National University of Kyiv, Volodymyrs'ka str. 64/13, Kyiv, 01601, Ukraine*
[2] *Dnipro University of Technology, Dnipro, Dmytro Yavornytskyi Avenue, 19, Dnipro, 49005, Ukraine*

Abstract

In order to timely and effectively respond to external influences in any system, it is necessary to have the ability to detect external impacts at early stages of their manifestation. It is particularly important to stop access to the system if a malicious actor has already breached it. This requires conducting timely investigations into the causes and methods of the breach, anticipating such possibilities in the future, and ensuring more reliable protection. Traditionally, methods of attack detection are divided into two broad categories: misuse detection and anomaly detection. This paper considers approaches to early detection of anomalies in the system's operation at early stages by analyzing the entropy of the event log. This method is used for both detecting anomalies in network traffic and for analyzing anomalies in event logs on hosts, which can also indicate intrusion attempts.

The study conducted on the example of Windows event logs showed that entropy analysis can detect early security threshold breaches in the number of messages in the event log. Such indicators can indicate anomalies in the operation of the information system. The method proposed in the article can be applied in intrusion detection systems, which notify the security administrator about possible misuse or intrusion attempts.

Keywords [1]

External influences, anomalies, entropy, event log, information security, intrusion detection

1. Introduction

With the development of information technologies, threats related to new technologies are inevitably developing and spreading, and the problem of ensuring reliable and timely cybersecurity is becoming increasingly relevant. When implementing the plans of criminals, potential cybersecurity threats from potential opportunities can become real cyber attacks, i.e., attempts to penetrate the information infrastructures of organizations that can adversely affect cybersecurity. Ensuring reliable cybersecurity and timely effective response to cyber attacks is an urgent problem for both individual organizations and government structures. Data theft, data damage, and cyber attacks of various orientations are recognized risks in the modern world. With the development of technology, cyber attacks become increasingly inventive, sophisticated, and destructive [1-2]. The most well-known and dangerous cyber attacks in the world are on critical information infrastructure [3-5]. To detect potentially dangerous security events, indicators of compromise (IOCs) are often used, including:

- Non-typical traffic at the input/output of the system;
- Unknown files, applications, and processes in the system;
- Suspicious activity of privileged accounts;
- Attempts to probe the system;
- Attempts to use brute force methods to gain access to services;
- Appearance of network traffic on non-typical ports;

Information Technology and Implementation (IT&I-2022), November 30 - December 02, 2022, Kyiv, Ukraine
EMAIL: g.gna5@ukr.net (H. Hnatiienko); babenkot@ua.fm (T. Babenko), Kovalovajp@gmail.com (Y. Kovalova), myrutenko.lara@gmail.com (L. Myrutenko)
ORCID: 0000-0002-0465-5018 (H. Hnatiienko); 0000-0003-1184-9483 (T. Babenko); 0000-0002-9234-4454 (Y. Kovalova); 0000-0003-1686-261X (L. Myrutenko)

- Appearance of a large number of archived files in places where they should not be;
- Use of non-original configurations of DNS servers and registry;
- Changes in the configuration of the operating system, including on mobile devices.

The use of indicators of compromise (IOCs) in most cases allows information security specialists and system administrators to detect signs of attacks, intrusions, or other potentially dangerous actions, but it is necessary to detect existing indicators of compromise in the system, which is often a problem.

Considering the reality of the threats described above, it is evident that scientific research enabling the timely and confident detection of deviations in information processes is relevant. The success of such research will allow for the identification of vectors of cyber attacks and actions to neutralize such attacks [6-7]. A promising direction for scientific research in this field is the use of entropy indicators to evaluate various parameters of information system cybersecurity. This is evidenced by a significant amount of research in this area [8-12]. Modeling early anomaly detection is a relevant problem for many areas of human activity [13, 14]. Several approaches have been proposed and studied to solve this problem, which to varying degrees allow for the identification of anomalies and incidents of the information security in information systems [15, 16]. One of the main tasks in solving this problem is timely detection of system compromise indicators and warning of potential abuses in order to provide for prompt response measures.

2. Goal and Objectives of the Research

Many authors of modern research assume that we have a standard situation with known accompanying circumstances, and under these idealized conditions, we can propose a new approach, a new or improved method, a modified algorithm, etc. This fully applies to sliding windows and their width. This technology has been applied for a long time, intensively and productively. However, authors usually start from the fact of a given width of the sliding window or do not focus on this parameter at all. The problem of determining an acceptable, and even more so, an optimal or at least justified value of its width is discussed very rarely by researchers.

The aim of this study is to determine the size of a sliding window at which a cyber attack vector or any cybersecurity anomaly can be reliably detected. The main tasks of researching and detecting anomalies in the operation of information systems are as follows:

- not to miss the fact of an attack;
- recognize the beginning of an attack at an early stage;
- accurately recognize the attack and distinguish it from a typical event;
- minimize the number of errors made in identifying the attack;
- minimize the consequences of incorrect identification of the attack;
- teach the system to distinguish an attack from a standard event at an early stage, and so on.

3. The comprehensiveness of the research

In many cases, a comprehensive application of different approaches in scientific research is effective. In the situation of detecting attacks, it can be useful to use methods and algorithms that belong to the following directions:

- data recovery methods taking into account anomalies that arise;
- image recognition methods;
- machine learning methods;
- time series analysis methods - determining similarity measures of series, comparing trends, and other aspects of this research direction;
- statistical research based on various types of scales: fixed, interval, using membership functions, and so on.

To successfully and adequately apply the mentioned approaches simultaneously, it is necessary to take into account the features of multi-attribute choice and multi-criteria optimization. In addition, for the successful complex application of different approaches to the task of determining the beginning of an attack, it is necessary to consider the features of decision-making under fuzzy conditions.

4. Scheme for detecting anomalies and security incidents

The research conducted by the authors of this work on behavior traffic analysis using entropy values allows for the application of an expert approach to identify and classify different system operation conditions that cause changes in entropy. Visual analysis performed by the authors revealed that a highly skilled expert can distinguish and classify about 15 types of events. However, it is impossible to involve experts in solving this problem in everyday life. Therefore, it is logical to formalize this problem, involve high-level expert knowledge in its solution, and provide automated or automatic incident detection. To further investigate and refine the problem of identifying impacts on information security, heuristics will be introduced.

Heuristic E1. Based on the research of the entropy change graph, which reflects the behavior of the message source, it is possible to identify an attack with high accuracy.

Heuristic E2. To fully identify an attack on the system, several attack indicators must be present. The necessary conditions for an attack are a deep drop in entropy level and a significant increase in entropy level. However, if these two indicators are not related to each other, these indicators are insufficient to consider them individually as mandatory entropy indicators. It is obvious but necessary to formalize the behavior identification model with the following heuristic.

Heuristic E3. An attack is accompanied by a large range of entropy reduction at the beginning of the attack and a large increase in entropy at the end of the attack. In the future, it is also advisable to introduce heuristics for capturing the entire passage of the attack. Obviously, after determining the width of the sliding window, it is possible to automatically analyze the behavior of the function that reflects the level of entropy. It should also be noted that a risk-oriented approach allows for the classification of events that indicate the degree of risk of threat realization. Different scales can be used to classify events. In this work, we will introduce a five-level scale for classifying levels of impact on the system:

ξ_1 – the informative level of impact

ξ_2 – the low level of impact;

ξ_3 – the moderate impact level;

ξ_4 – the high or dangerous level of impact;

ξ_5 – the critical level of impact.

5. Determining the width of the sliding window

Expert decision-making technologies can be applied at different stages of research and practical situation modeling [17, 18]. The study of entropy behavior and determination of the sliding window width using expert methods can serve as both an element of a broader study and a goal in itself. The authors of this study propose several options for expert determination of the window width, taking into account the limited capabilities of involving high-level experts to solve this problem.

Firstly, expert survey can be organized to determine the values of the sliding window width, both in individual expert survey and group expert survey. Secondly, to determine the window width in which the information about the attack is guaranteed to be present, a series of studies can be conducted in which the beginning and end of the attack are reliably recorded by expert means. As a result of the analysis of such a survey, the window width is determined based on statistical analysis of the data obtained from the experts. It should be noted that the width of the sliding window is an important parameter that significantly affects the speed and quality of attack research. This value may relate to different aspects of the study, so it is necessary to distinguish between different quantities with this name. The width of the sliding window should be considered in several aspects, including:

- when studying trends in entropy changes;
- when detecting anomalous function values;
- for guaranteed event localization.

In such cases, precise approximation of the anomaly is not necessary, but using additional computer resources such as time and memory is also not sensible. When studying the behavior of a function that describes changes in entropy, we will distinguish at least several factors:

- the number of events in the sliding window;
- the diversity of different types of events in the window;
- the range of entropy changes in the window.

Definition 1. We define a Window for Attack Detection (WAD) as the number of recorded events during which the beginning of an attack, the maximum entropy change, and the end of the attack can be reliably identified. The width of WAD is denoted by S^1.

Definition 2. A window for detecting standard events (WDSE) is defined as the number of recorded events during which the beginning, minimum/maximum entropy, and completion of the event can be determined. The width of WDSE is denoted by S^2.

It is logical to assert that the size of the sliding window should be measured by the number of events recorded in the log in all cases. Such a coordinate system was adopted and successfully applied in a series of computational experiments. Based on visual observations, in all practical situations, it is obvious that the following relation always holds:

$$S^1 > S^2. \tag{1}$$

It should also be noted that the use of a properly defined window allows for achieving a whole range of results. In order to ensure further automatic investigation of the behavior of the function that describes the entropy value in the system, it is necessary to investigate:

- detecting peculiarities of the function graph behavior during attacks;
- identifying common attack characteristics reflected in the graph;
- finding the boundaries of the attack start and end, etc.

It should be noted that, with regard to relation (1), if the sliding window size is correctly defined, it is possible to correctly select and effectively apply the relevant mathematical tools.

6. Algorithmic determination of trend change intensity

It is evident that an attack can be studied by analyzing trends in behavior, particularly through the analysis of time series, which have been studied in works [19-21]. Trends are described using linear, logarithmic, power, and other equations, which have been investigated in works [22-24]. The authors proposed an approach that allows detecting a rapid change in trend behavior already in the early stages of its appearance. The validity of this approach has been verified and confirmed through a series of computational experiments.

Let a sequence of events be defined and recorded in a log, the number of which is equal to t. We will denote the set of these events by T, and represent the sequence of the events using indices

$$i \in T = \{1,...,t\}. \tag{2}$$

To clarify the decision-making situation, ensure transparency in further modeling, and refine the mathematical model to be constructed, it is necessary to formulate another heuristic. The introduction of such a heuristic is associated with the fact that in practical decision-making situations, thousands of events need to be researched and analyzed.

Heuristic E4: Each discrete element (2) corresponds to dozens or hundreds of events in specific cases, which in our mathematical model are indivisible and can be modeled by discrete elements (2).

Taking into account heuristic E4, we will denote the entropy value for each event by

$$a_i,\ i \in T. \tag{3}$$

To investigate the patterns of behavior of the values of the sequence (3), we will define WDSE, for example, in the interval of $\tau \in [1, t/2]$.

For each i-th discrete element, to which the next block of events, $i \in T$, of the form (2) corresponds, we will determine the values of the ratio between the current and the next discrete element

$$b_{ij} = a_i / a_{i+j} \text{ where } j = 1,...,\tau. \tag{4}$$

In situations where entropy values may be zero, some sufficiently small values $\varepsilon > 0$ may be added to the denominator in formula (4)

$$b_{ij} = a_i / \left(a_{i+j} + \varepsilon\right) \text{ where } j = 1,...,\tau. \tag{5}$$

It should be noted that the introduction of specific values of the variable $\varepsilon > 0$ is also a heuristic, but in this work, there is no need to investigate the dependence of experiments on the size of this variable. Therefore, we will not focus on the influence of the value of $\varepsilon > 0$ on the convergence of the procedure and the features of the computational experiment. The following two heuristics are fair:

Heuristic E5. It is obvious that the presence of values within the window width (4) of the type (3), which are significantly larger than the values in the series (3), can serve as indicators of a trend change when there is a sharp decrease in entropy. The formal aspect of this heuristic will be presented below, along with the further exposition of the research logic and the descriptive computational experiments.

Heuristic E6. In the opposite case to Heuristic E5, the presence of values of the type (5) that are significantly smaller than the inverse values in the series (3) are indicators of a trend change when there is a sharp increase in entropy. Finally, a heuristic for decision-making can be formulated for this situation.

Heuristic E7. The presence of several values of the type (5) that are described by heuristics E5 and E6 is a criterion for a sharp trend change. There may be at least two approaches for algorithmically determining the indicators that reflect the behavior of different event log fragments in an integral form:

- multiplicative approach;
- additive approach.

7. Multiplicative approach

Let's introduce notation for the window size, the dependency of which we will investigate in determining further criteria. Taking into account Heuristic E4, we will denote by $v \geq 2$ the window size based on which we need to calculate the criteria values that reflect the presence or absence of attacks on the information system. To investigate the behavior of an information system that reflects the dynamics of entropy values at each moment in time, let us introduce the following criterion function:

$$Q^M(t,v) = \begin{cases} \prod_{i=1}^{v-1} a_i \cdot a_v, & \text{якщо } a_{v-1} \leq a_v \\ \prod_{i=1}^{v-1} a_i / a_v, & \text{якщо } a_{v-1} > a_v \end{cases} \quad (6)$$

For each level of impact classification scale from to , boundary values of the criteria $Q^{M1},...,Q^{M5}$ can be determined. It would be useful to supplement the decision-making situation we are investigating with an additional heuristic that will contribute to the refinement and formalization of our research situation.

Heuristic E8: The extreme values of the criterion function (6) for the standard (normal, stable, etc.) operation of the information system and the extreme values of the function (6) for the attack differ significantly in magnitude. Variations of the values of $v \geq 2,$ and $t = 1,2,...$ will allow the researcher to determine the combinations of function values and arguments, or intervals of such values, that best correspond to the conditions of situation classification and the probability of an attack on the information system.

8. Additive approach

An additive approach can also be applied to investigate the behavior of a function that reflects the dynamics of entropy values at each moment in time. In this case, the behavior of such a function can be introduced and investigated:

$$Q^A(t,v) = \begin{cases} \sum_{i=1}^{v-1} a_i + a_v, & \text{якщо } a_{v-1} \leq a_v \\ \sum_{i=1}^{v-1} a_i - a_v, & \text{якщо } a_{v-1} > a_v \end{cases} \quad (7)$$

In this case, the behavior of criteria of the form (6) and (7) differs from each other. Therefore, there is an opportunity for the integrated use of these tools to improve early detection methods of cyber attacks or other impacts on the information system. Based on the conducted research, which

was a combination of expert methods and calculations based on formulas (6)-(7), critical values of the function K were determined, at which the situation reflected in values (3) can be classified with a high degree of certainty as belonging to one of the variants of the impact risk of $\xi_1,...,\xi_5$.

It should be noted that the application of the proposed approaches indirectly solves the problem of the sliding window size. Clearly, the indicators of the situation classification are the values of functions (6)-(7). Depending on the value of the parameter, which can be interpreted as the window size, the functions (6)-(7) take on certain values. Based on the magnitude of these values, one can draw conclusions about the degree of danger of impacts on the information system, i.e. about the classification of the decision-making situation into one of the classes $\xi_1 - \xi_5$ introduced by us.

9. Computational experiment

For the investigation of the methods described in this work, individual fragments of the event log were considered. The computational experiment was conducted on three fragments, all of which were unambiguously identified by the experts as reflecting the normal operation of the system. One fragment was also selected for which an attack was emulated.

It should be noted that to ensure the purity of the experiment, communication channels, external networks, etc., were disabled. Such measures were taken to ensure the absence of communication with sources from which a potential attack can be expected.

A whole range of decision-making situations were considered, where the entropy values, from the experts' point of view, confidently correspond to the normal functioning of the information system. Several fragments of this situation are presented in this work in figures 1-3. In addition, figure 4 will show a fragment that undoubtedly contains an attack on the information system, deliberately provoked by the experiment organizers. For example, among the hundreds of decision-making situations investigated, we will select some of the most characteristic situations. To illustrate the course of the computational experiment and the detection of a change in the behavior gradient of the function, we will consider information on entropy, which we will present in the form of tables 1-3.

Table 1

Fragment of row number 1, which reflects a period in the event log when no incidents or attacks occurred

Discrete	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Entropy	2,0	1,5	1,8	1,9	2,1	1,5	1,9	2,1	2,2	2,3	1,9	1,7	1,5	1,9	1,7	1,5	1,7	1,9	1,8	1,7
Discrete	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Entropy	2,0	1,8	1,9	1,8	1,7	1,6	1,7	1,8	1,9	2,2	2,0	2,1	2,5	2,3	2,2	2,1	2,3	2,2	2,0	1,9

Table 2

Fragment of row number 2, which reflects a period in the event log when no incidents or attacks occurred.

Discrete	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Entropy	1,7	1,5	2,3	1,7	1,3	1,3	1,5	1,7	1,2	1,5	2,0	1,4	1,7	1,5	2,0	1,6	2,0	2,2	1,5	0,9
Discrete	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Entropy	1,4	0,8	1,0	1,3	0,9	0,8	0,8	0,7	0,8	0,7	0,8	0,8	1,0	1,0	1,4	1,9	1,0	1,9	1,5	0,8

Let's present Table 1 as a graph - Figure 1, which visualizes the behavior of the information system in situations of cyber attacks or other incidents. Among the hundreds and thousands of decision-making situations that have been reflected in the event log, those that best reflect the normal functioning of the information system have been identified through expert analysis. The numerical indicators for three such typical situations of standard information system functioning are presented for illustration in Table 1, Table 2, and Table 3. Table 2 is visualized as Figure 2. Obviously, this graph differs from Figure 1, but it also represents indicators that correspond to normal functioning of the information system. Table 3 is represented in Figure 3. In the computational experiment, hundreds of fragments were analyzed, samples of which are presented in Figure 1, Figure 2, Figure 3.

Based on the results of the conducted experiment, it was shown that the method presented in this paper allows for identifying the beginning of an attack after only 4-5 discrete units (2).

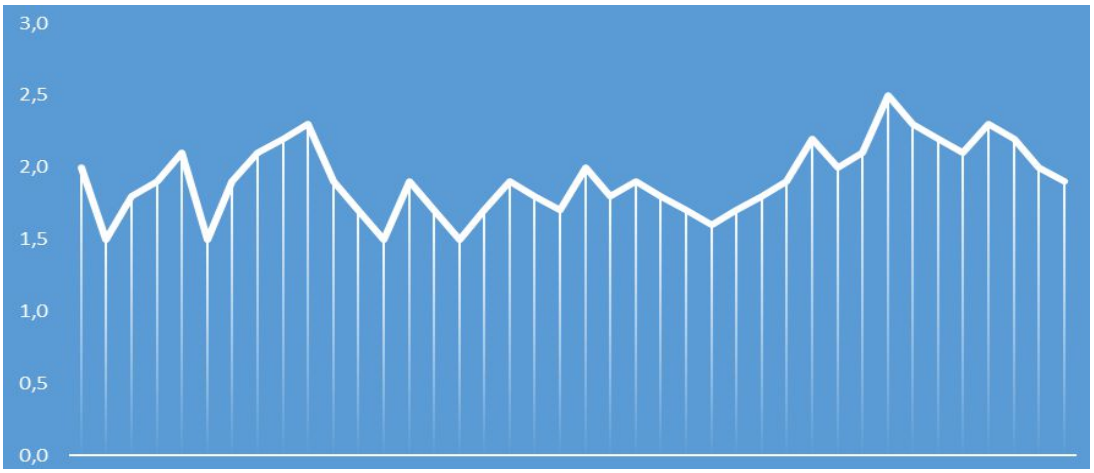

Figure 1: Entropy under normal functioning (fragment 1): a graph of entropy values corresponding to the data presented in Table 1

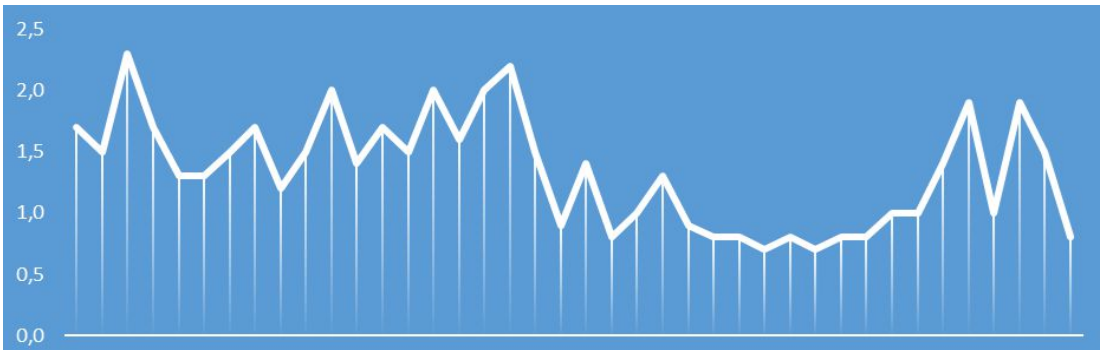

Figure 2: Entropy under normal functioning (fragment 2): A graph of entropy values that corresponds to the data presented in Table 2

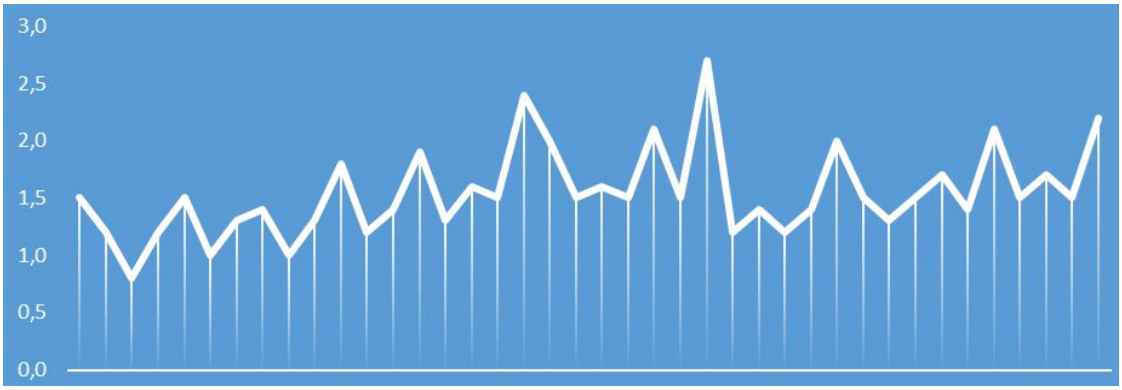

Figure 3: Entropy under normal functioning (fragment 3): A graph of entropy values that corresponds to the data presented in Table 3

Table 3

Fragment of row number 3, which reflects a period in the event log when no incidents or attacks occurred

Discrete	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Entropy	1,5	1,2	0,8	1,2	1,5	1,0	1,3	1,4	1,0	1,3	1,8	1,2	1,4	1,9	1,3	1,6	1,5	2,4	2,0	1,5
Discrete	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Entropy	1,6	1,5	2,1	1,5	2,7	1,2	1,4	1,2	1,4	2,0	1,5	1,3	1,5	1,7	1,4	2,1	1,5	1,7	1,5	2,2

Table 4
Fragment of row number 4, which shows the period in the event log when the attack was emulated

Discrete	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Entropy	1,7	2,3	2,2	2,4	2,5	2,2	2,1	1,9	2,2	2,0	2,0	1,8	1,7	1,5	1,3	1,0	0,8	0,5	0,4	0,1
Discrete	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Entropy	0,5	0,6	1,0	1,2	1,5	1,8	1,8	2,1	2,0	2,5	2,0	1,8	1,9	1,5	1,3	1,1	1,4	1,9	1,7	2,2
Discrete	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
Entropy	2,1	2,5	2,8	2,7	3,3	3,0	3,1	2,7	2,5	2,0	2,1	2,3	2,1	2,4	2,2	2,5	2,3	2,3	2,2	2,6

By applying additional criteria, the confidence in the presence of an attack or incident during event log analysis can be significantly increased. Additional criteria may include a decrease in entropy value, continued monitoring of the behavior of the function that reflects entropy, and so on.

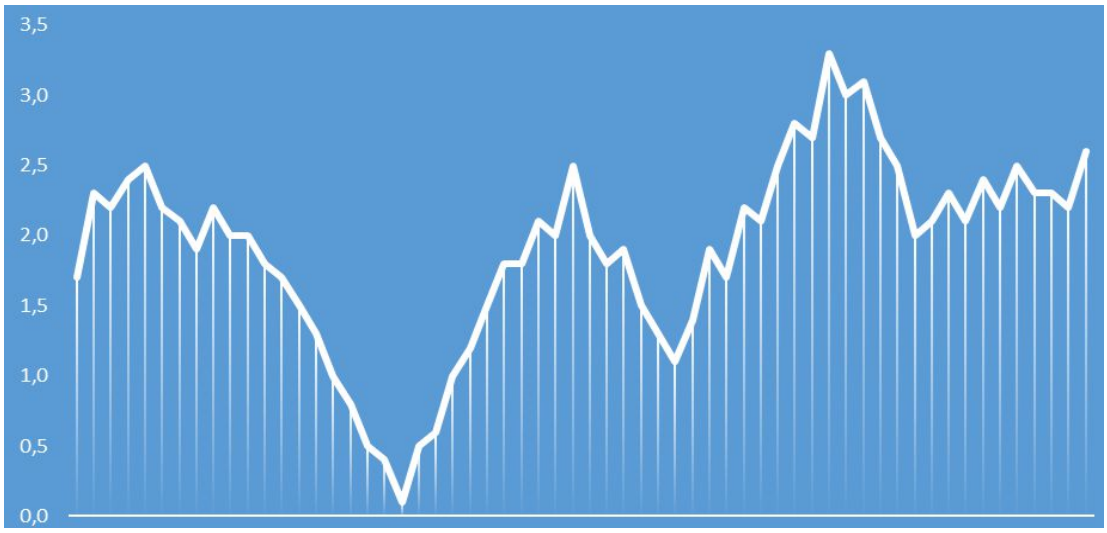

Figure 4: The diagram fragment that contains the attack: A graph of entropy values that corresponds to the data presented in Table 4

10. Prospects for further research

Algorithms for computing potential threats through trend analysis, similar to the algorithms described by formulas (2)-(5), can be developed to expand the toolkit for researching attacks and incidents. Using precedents for analyzing the similarity measures of series and identifying patterns in the behavior of the function that describes the change in system entropy is also promising. In the future, automated tracking of trend behavior and identification of situations such as plateaus, sharp or smooth growth, and declines are planned. Support for decision-making regarding trend similarity will be provided by analyzing the range of entropy values within a justified window.

The behavior of the entropy change function can also be approximated using primitive shapes such as triangular functions [25-27]. In addition to the multiplicative and additive approaches proposed in this paper, neural networks [28, 29] can also be used for decision-making in this situation. In this case, the neural network identifies the nature of the functional dependency during normal operation of the information system and changes in dependencies during situations that experts identify as attacks. The neural network determines the type of functional dependence during normal system operation and changes in dependencies during situations that experts identify as attacks, thus identifying patterns in the behavior of entropy and the relationship between functions that reflect the dynamics of entropy change.

In order to increase confidence in the identification of the decision-making situation and the classification of the level of danger, several approaches can be simultaneously applied in a complex [30, 31]. To increase confidence in identifying situations and decision-making, multiple approaches can be simultaneously applied, necessitating the use of multi-criteria optimization methodology [32, 33].

11. Conclusions

The paper proposes a model for early detection of anomalies and incidents in information systems. A scheme for early detection of anomalies is proposed. Approaches to determining the window width in studying the operation of the information system are discussed. The algorithmic determination of trend change intensity is described. The computational experiment described in this paper demonstrates an example of detecting a change in the gradient of the criterion function's behavior. The application of research related to numerical series is a promising direction and has broad prospects when various methods are applied together. It should be noted that this paper describes an idealized situation for detecting an attack. After a series of additional studies and computational experiments, the approaches described can be applied to real decision-making situations.

Prospects for further research on detecting cyber-attacks, incidents, and anomalies in the functioning of information systems are also identified. It is clear that the subject of research can be significantly expanded in the future, as the detection of anomalies in the functioning of complex systems of various kinds is a popular direction for scientific research.

12. References

[1] Geer, D.; Jardine, E.; Leverett, E. On market concentration and cybersecurity risk. J. Cyber Policy 2020, 5, 9–29.

[2] Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity 2019, 2, pp. 1–22.

[3] Papastergiou, S.; Mouratidis, H.; Kalogeraki, E.M. Cyber security incident handling, warning and response system for the european critical information infrastructures (cybersane). In Proceedings of the International Conference on Engineering Applications of Neural Networks, Crete, Greece, 24–26 May 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 476–487.

[4] Babenko, T., Hnatiienko, H., Ignisca, V., Iavich, M. Modeling of critical nodes in complex poorly structured organizational systems // Proceedings of the 26th International Conference on Information Society and University Studies (IVUS 2021), Kaunas, Lithuania, April 23, 2021 / CEUR Workshop Proceedings, 2021, 2915, pp. 92–101.

[5] Krumay, B., Bernroider, E.W.N., Walser, R. (2018). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. In: Gruschka, N. (eds) Secure IT Systems. NordSec 2018. Lecture Notes in Computer Science(), vol 11252. Springer, Cham. https://doi.org/10.1007/978-3-030-03638-6_23

[6] Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms, 10(2), [39]. https://doi.org/10.3390/a10020039

[7] Rupa Devi, T.; Badugu, S. A review on network intrusion detection system using machine learning. In Advances in Decision Sciences, Image Processing, Security and Computer Vision; Springer: Berlin/Heidelberg, Germany, 2020; pp. 598–607.

[8] Salih AA, Abdulazeez AM (2021) Evaluation of classification algorithms for intrusion detection system: a review. J Soft Comput Data Mining 2(1) 31–40.

[9] Han, Q., & Yang, D. (2018). Hierarchical Information Entropy System Model for TWfMS. Entropy, 20(10), 1–20.

[10] Li Y. and Chao X., "Distance-entropy: an effective indicator for selecting informative data," Frontiers in Plant Science, vol. 12, pp. 818-895, 2021.

[11] Shiju Rawther, S Sathyalakshmi, "Entropy Analysis of Cyber-Attack Propagation in Network", 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp.1-4, 2022.

[12] Hamid T, Al-Jumeily D, Mustafina J (2018) Evaluation of the dynamic cybersecurity risk using the entropy weight method. In: Dastbaz M et al (eds) Technology for Smart Futures, pp 271–287.

[13] Pu G., Wang L., Shen J., Dong F., A hybrid unsupervised clustering-based anomaly detection method. Tsinghua Sci. Tech., 26 (2) (2021), pp. 146-153, 10.26599/TST.2019.9010051

[14] Moon, D.; Im, H.; Kim, I.; Park, J.H. DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. J. Supercomput. 2017, 73, 2881–2895.

[15] Yao D., Yin M., Luo J., Zhang S., Network anomaly detection using random forests and entropy of traffic features, in: Fourth International Conference on Multimedia Information Networking and Security, Nanjing, 2012, pp. 926–929. doi: 10.1109/MINES.2012.146.
[16] Shukla A.S., Maurya R., Entropy-based anomaly detection in a network. Wireless Pers. Commun., 99 (4) (2018), pp. 1487-1501.
[17] Hnatiienko H. Choice Manipulation in Multicriteria Optimization Problems / Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019), pp. 234–245 (2019).
[18] McAndrew, T. et al. (2021) Aggregating predictions from experts: a review of statistical methods, experiments, and applications. WIREs: Comput. Stat. 13, e1514.
[19] Fawaz H. I., Forestier G., Weber J., Idoumghar L. and Muller P.-A., "Deep learning for time series classification: a review," Data Mining and Knowledge Discovery, vol. 33, no. 4, pp. 917–963, 2019.
[20] Li, D., Chen, D., Jin, B., Shi, L., Goh, J., Ng, S.-K.: MAD-GAN: multivariate anomaly detection for time series data with generative adversarial networks. In: Tetko, I.V., K˚urková, V., Karpov, P., Theis, F. (eds.) ICANN 2019. LNCS, vol. 11730, pp. 703–716. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30490-4_56
[21] Zhou B., Liu S., Hooi B., Cheng X., and Ye J., "BeatGAN: Anomalous Rhythm Detection using Adversarially Generated Time Series," in Proc. of the 28th Int. Joint Conf. on Artificial Intelligence, (IJCAI), 2019, pp. 4433–4439
[22] Guo, Y., Liao, W., Wang, Q., Yu, L., Ji, T., Li, P.: Multidimensional time series anomaly detection: a GRU-based Gaussian mixture variational autoencoder approach. In: Asian Conference on Machine Learning, pp. 97–112 (2018)
[23] Radivilova, T.; Kirichenko, L.; Lemeshko, O.; Ageyev, D.; Mulesa, O.; Ilkov, A. Analysis of anomaly detection and identification methods in 5G traffic. In Proceedings of the Eleventhth IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 22–25 September 2021; pp. 1108–1113.
[24] Hrechko Viktoriia; Hrygorii Hnatienko; Tetiana Babenko. An intelligent model to assess information systems security level // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 29-30 July 2021/ Date Added to IEEE *Xplore*: 19 August 2021, Pp 128 – 133, DOI: 10.1109/WorldS451998.2021.9514019
[25] Zare, A.; Shoeibi, A.; Shafaei, N.; Moridian, P.; Alizadehsani, R.; Halaji, M.; Khosravi, A. Accurate Prediction Using Triangular Type-2 Fuzzy Linear Regression. *arXiv* 2021, arXiv: 2109.05461.
[26] Iraq Tariq Abbas. Triangular membership functions for solving single and multiobjective fuzzy linear programming problem // Iraqi Journal of Science,Vol 53,No 1,2012, Pp. 125-129.
[27] Lathamaheswari, M.; Nagarajan, D.; Kavikumar, J.; Broumi, S. Triangular interval type-2 fuzzy soft set and its application. *Complex Intell. Syst.* **2020**, *6*, 531–544.
[28] Raghuraman, C.; Suresh, S.; Shivshankar, S.; Chapaneri, R. Static and dynamic malware analysis using machine learning. In Proceedings of the First International Conference on Sustainable Technologies for Computational Intelligence, Jaipur, India, 29–30 March 2019; Springer: Berlin/Heidelberg, Germany, 2020; pp. 793–806.
[29] Sekhar Ch et al (2021) Deep learning algorithms for ıntrusion detection systems: extensive comparison analysis. Turkish J Comput Mathe Edu (TURCOMAT) 12(11):2990–3000.
[30] Voloshin, A.F., Gnatienko, G.N., Drobot, E.V. A Method of Indirect Determination of Intervals of Weight Coefficients of Parameters for Metricized Relations Between Objects // Journal of Automation and Information Sciences, 2003, 35(1-4).
[31] Ghafari N., Yaghoobi M.A., An algorithm for a multicriteria optimization problem and its application to a facility location problem, J. Mahani Math. Res. 2022; 12(3): 197-213.
[32] Kravchenko, Y., Starkova, O., Herasymenko, K., Kharchenko, A. Peculiarities of the IPv6 implementation in Ukraine // 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 - Proceedings, 2017, 2018-January, pp. 363–368
[33] Hnatiienko, H., Kiktev, N., Babenko, N., Desiatko, A., Myrutenko, L. Prioritizing Cybersecurity Measures with Decision Support Methods Using Incomplete Data // Selected Papers of the XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS 2021), Kyiv, Ukraine, December 9, 2021 / CEUR Workshop Proceedings, 2021, 3241, pp. 169–180.