УДК 004.65:620.92

Б. В. ПЕТРИК, В. І. ДУБРОВІН
Національний університет "Запорізька Політехніка"

ВИЯВЛЕННЯ АТАК ТИПУ DOS В МЕРЕЖЕВОМУ ТРАФІКУ ЗА ДОПОМОГОЮ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

Мета роботи. *Кількість мережевих вторгнень і атак набирає все більш критичні позиції, які виходять з даних аналітичних агентств кібербезпеки. У 21 столітті майже всі організації не є на 100% захищені. В організаціях з передовими технологіями захисту можуть бути проблемні моменти в ключових елементах - розуміння зловмисником відомих технологій захисту. У таких ситуаціях використання інших способів виявлення може бути ключовим моментом в захисті від мережевої атаки. Є безліч методів перевірки рівня захищеності: аналіз безпеки систем і додатків, тестування на проникнення, оцінка обізнаності персоналу в питаннях інформаційної безпеки і т.д. Однак через постійні зміни технологій, появи нових інструментів і злочинних груп виникають нові типи ризиків, які важко виявити за допомогою традиційних способів аналізу захищеності. На цьому тлі найбільш поглиблений і прогресивний метод до тестування безпеки з перетворенням сигналу і вивченням вхідного трафіку буде здатний підвищити рівень надійності мережі.*

Методи дослідження. *Кібератаки в різних форматах, особливо відомі, постійно вимагають безперервну оцінку захищеності інформаційних систем. Ці отримані дані необхідні для вивчення і дослідження фахівцями для їх подальшого використання. Один із перспективних методів Data mining, який є прогресивним і поглибленим можливо вважати вейвлет-перетворення. Алгоритм вейвлет-перетворення слід застосовувати для аналізу дискретних даних. Це важливо коли потрібна висока швидкість обробки та аналізу інформації. Що є актуальним пунктом для вирішення завдання захисту мережі інтернет.*

Отримані результати. *Виконано аналіз алгоритмів вейвлет перетворення як для очитски вхідного трафіку від шуму, так і для виявлення мережевої аномалії. Докладно розглянуті основні етапи застосування і реалізації системи виявлення, що використовує порогові значення вейвлет-коефіцієнтів для виявлення мережевої атаки і аномалії.*

Наукова новизна. *Розроблена модель виявлення відповідно до ефективного алгоритму вейвлет-перетворення, яка комплексно стежить за поточним станом мережі, і повідомляє при ризики виникнення несприятливих подій.*

Практичне значення. *Розглядаючі мережеві атаки типу DOS і практичне реагування на можливі атаки, у разі використання вейвлет-перетворення для безпеки, можливо підвищити захист системи з виявлення до непомічених загроз. Щоб зупинити зловмисників на ранніх стадіях атаки і запобігти матеріальним збиткам для бізнесу слід звернути увагу саме на цей метод Data mining.*

Ключові слова: *Dos-атака, вейвлет - перетворення, порогове значення виявлення, шумозниження, мережевий трафік, вейвлет функція, алгоритм Малла.*

Б. В. ПЕТРИК, В. И. ДУБРОВИН
Национальный университет "Запорожская Политехника"

ОБНАРУЖЕНИЕ АТАК ТИПА DOS В СЕТЕВОМ ТРАФИКЕ С ПОМОЩЬЮ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Цель работы. *Количество сетевых вторжений и атак набирает все более критические позиции, которая выходят из данных аналитических агентств по кибербезопасности. В 21 веке почти все организации не является на 100% защищены. В организациях с передовыми технологиями защиты могут быть проблемные моменты в ключевых элементах - понимание злоумышленником известных технологий защиты. В таких ситуациях использование других способов обнаружения может быть ключевым моментом в защите от сетевой атаки. Есть множество методов проверки уровня защищенности: анализ безопасности систем и приложений, тестирования на проникновение, оценка осведомленности персонала в вопросах информационной безопасности и т.д. Однако через постоянные изменения технологий, появления новых инструментов и преступных групп возникают новые типы рисков, которые трудно обнаружить с помощью традиционных способов анализа защищенности. На этом фоне наиболее углубленный и прогрессивный метод к тестированию безопасности с преобразованиям сигнала и изучением входящего трафика будет способен изменить уровень надежности сети.*

Методы исследования. *Кибератаки в различных форматах, особенно известные, постоянно требуют непрерывную оценку защищенности информационных систем. Эти полученные данные необходимы для изучения и исследования специалистами для их дальнейшего использования. Одно из перспективных методов Data mining, который является прогрессивным и углубленным можно считать вейвлет-преобразования. Алгоритм вейвлет-преобразования следует применять для анализа дискретных данных. Это важно когда требуется высокая скорость обработки и анализа информации. Что является актуально для решения задачи защиты сети интернета.*

Полученные результаты. *Выполнен анализ алгоритмов вейвлет преобразования как для очитски входящего трафика от шума, так и для обнаружения сетевой аномалии. Подробно рассмотрены основные этапы применения и реализации сисетмы обнаружения использующую пороговые значения вейвлет-коефициентов для обнаружения сетевой атаки и аномалии.*

Научная новизна. *Разработанная модель обнаружения в соответствии с ефективным алгоритмом вейвлет-преобразования, комплексно учитывающий текущее состояние сети, и уведомляющий при риске возникновения неблагоприятных событий.*

Практическое значение. *Рассматривая сетевые атаки типа DOS и практическое реагирования на возможные атаки, при использовании вейвлет-преобразования для безопасности может повысить защиту системы по выявлению к незамеченным угрозам. Чтобы остановить злоумышленников на ранних стадиях атаки и предотвратить материальный ущерб для бизнеса следует обратить внимание именно на этот метод Data mining.*

Ключевые слова: *Dos-атака, мережева атака, вейвлет – преобразования, подавление шума, пороговое значение обнаружения, сетевой трафик, вейвлет функция, алгоритм Малла.*

B. V. PETRIK, V. I. DUBROVIN
National University "Zaporizhzhia Polytechnic"

DETECTION OF DOS ATTACKS IN NETWORK TRAFFIC BY WAVELET TRANSFORM

Purpose. *The number of network intrusions and attacks is gaining an increasingly critical position, which is emerging from the data of analytical agencies on cybersecurity. In the 21st century, almost all organizations are not 100% protected. In organizations with advanced security technologies, there may be bottlenecks in key elements - the attacker's understanding of known security technologies. In such situations, using other detection methods can be key to defending against a network attack. There are many methods for checking the level of security: analyzing the security of systems and applications, penetration testing, assessing the awareness of personnel in information security issues, etc. However, through the constant changes in technology, the emergence of new tools and criminal groups, new types of risks are emerging that are difficult to detect using traditional methods of security analysis. Against this background, the most advanced and progressive method for security testing with signal transformations and the study of incoming traffic will be able to change the level of network reliability.*

Methods. *Cyberattacks in various formats, especially well-known ones, constantly require continuous assessment of the security of information systems. These obtained data are necessary for study and research by specialists for their further use. One of the most promising data mining methods, which is progressive and in-depth, can be considered wavelet transforms. The wavelet transform algorithm should be used to analyze discrete data. This is important when a high speed of information processing and analysis is required. What is relevant for solving the problem of protecting the Internet.*

Results. *The analysis of wavelet transform algorithms is carried out both for cleaning incoming traffic from noise and for detecting a network anomaly. The main stages of application and implementation of a detection system using threshold values of wavelet coefficients for detecting a network attack and anomaly are considered in detail.*

Scientific novelty. *The developed detection model in accordance with an effective wavelet transform algorithm, comprehensively taking into account the current state of the network, and notifying at the risk of adverse events.*

Practical meaning. *By considering network attacks like DOS-attack and practical responses to possible attacks, using wavelet transform for security can increase the system's protection by detecting undetected threats. To stop cybercriminals in the early stages of an attack and prevent material damage to the business, you should pay attention to this particular data mining method.*

Keywords: *Dos attack, wavelet transform, detection threshold, noise reduction, network traffic, wavelet function, Mallat algorithm.*

Problem Statement

Analysis of network traffic data is very important for detecting DOS attacks and malicious anomalies. Many data mining techniques have been found to view data and use it for security purposes. Fast and accurate search for content–based queries is critical to making such numerous data streams useful. The need for analysis of network attacks and localization of anomaly data by the Data mining method is growing. When considering important points in the creation of a protection system, statistical data on the effectiveness of the method are needed. In experimental research, it is possible to analyze the possibilities and effectiveness of the analysis of the method in everyday use.

Analysis of Recent Researches and Publications

Wavelet transform(WT) is one of the most promising data analysis technologies, its tools are used in various fields of intellectual activity. In contrast to the fast Fourier transform (FFT), wavelet analysis allows you to select both frequency and time components of variability, ie allows you to analyze the time variability of the frequency spectrum of the process[1].

There is usually a distinction between discrete wavelet transform (DWT) and continuous wavelet transform (CWT). CWT is the implementation of wavelet transform using arbitrary scales and virtually arbitrary wavelets, while DWT uses orthogonal type wavelets and two–level scaling. In the first case, a more detailed study of traffic behavior is possible, while in the second faster conversion is achieved. In this paper we will consider both CWT [2,3] and DWT [4,5].

Wavelet transform for traffic analysis in educational networks. Most research and scientific Internet networks are used to analyze these networks. Reliability, security and accuracy of such networks allow to make the exact analysis of a potential anomaly. This anomaly can be considered as a network attack, noise and quarterly network loads. In [4] the work on monitoring the university network is presented. It has been demonstrated that using continuous wavelet transform (CWT) it is possible to analyze how the frequency content of data changes over time. This depends on the time of the variable frequency information, which is not available in other methods, such as FFT. This feature is considered in the analysis of network traffic.

Figure 1 shows the network traffic data of the LSBU World Wide Web (WWW) in 3D format in Figure 1-a and the corresponding 2D representation in Figure 2-b. The results show that WWW traffic is very seasonal. These data respond to the busy day of the work week and less active weekends. This agrees well with the quarterly updates in the system, which are represented by the highest system activity. Also affects the periods of holidays and vacations. WWW traffic data vary significantly during the day, the highest from 10:00 to 19:00 and the lowest from 06:00 to 09:00.

2D network traffic data and 3D presentations, which have traffic for 24 hours and 365 days, help to best design and break down the structure of the system. With the support of the WT method, it is possible to decompose network traffic data. With CWT, it is possible to analyze data and show which is the most common data component issued over time.

Using the features of the CWT method, it is possible to see the general characteristics of WWW traffic and easily identify the situation, which will allow you to accurately identify the required part of the traffic, where there is a place of suspicious activity.

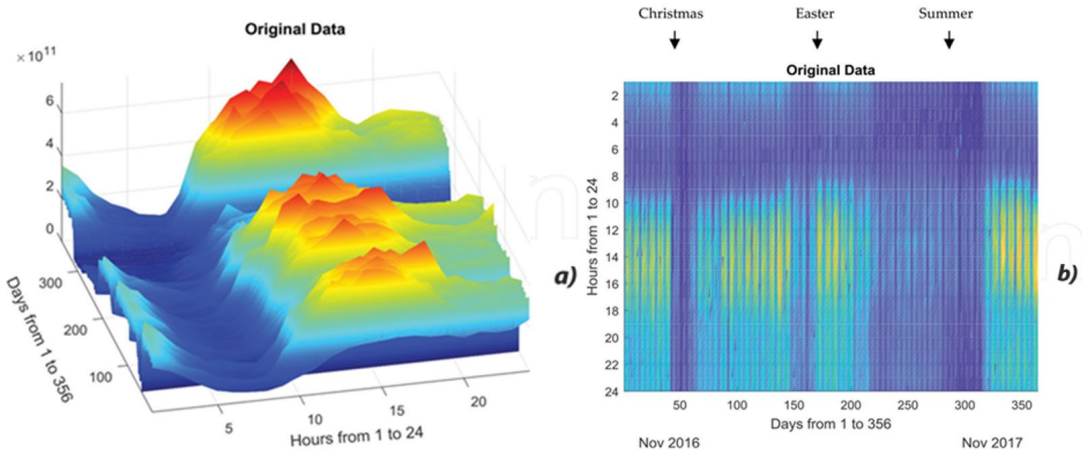

Fig. 1: 3D–presentation (a) and 2D–presentation (b) of WWW–traffic data in the scheme of daily use [2]

Application of signal processing strategies that include Morlet wavelet. There are various methods based on the host and network methods to monitor network intrusions in real time, but they are limited in the context of detecting anomalies. In [3], in order to increase security in modern network systems (MS), one method is to apply signal processing strategies that include powerful CWT methods consisting of Morlet wavelet to detect any anomalies in MS data. Percentage deviations were used to assess the quality of wavelet performance when detecting abnormal events, such as port scans and DoS attacks.

Re–decomposition of WT is a summation of the signal, which shows a scaled and offset version of the wavelet for the full time of the signal. Thus, the wavelet coefficients are generated by this process, which is a function of scale as well as position. After applying algorithm, the WT coefficients are produced at different scales using different parts of the signal. The coefficients represent the results of the regression of the output signal performed on the Morlet wavelet. The CWT is a time scale signal.

In the field of network intrusion, in order to detect anomalies in long–term data on network traffic, CWT Morle seems to be a very promising candidate for the wavelet function. This study limited the duration to one week, approximately 160,000 data points, and the Morlet wavelet demonstrated its best performance.

Analysis of network traffic to detect attacks on digital product infrastructure. Digital manufacturing integrates with all areas of human activity, including critical industries. Therefore, the task of detecting network attacks is a key priority in protecting digital production systems. In [4], an approach to analyzing the security of digital production is proposed, based on the assessment of the posterior probability of a point change in time series, based on the change in the DWT coefficient values in the time series of network traffic. These time series allow us to consider network traffic from several points of view simultaneously, which plays an important role in detecting network attacks. The attack methods vary considerably. Therefore, to detect them, it is necessary to track different values of different traffic parameters.

The proposed method has demonstrated its effectiveness in detecting DOS attacks implemented at the application level. Time series built and based on the "number of HTTP packets" parameter were used to detect this attack. Figure 2 shows the time series built by the number of packets for traffic with suspicious activity.

In the figure 2, you can see 4 intense data jumps, and they all coincide with the attack time. In this case, it should be noted that the developed method does not trigger false responses. A noticeable jump after 1200 in the middle chart looks like an anomaly, but the bottom chart showing the posterior value of the point change probability shows that the point change probability is very small: less than 0.2.

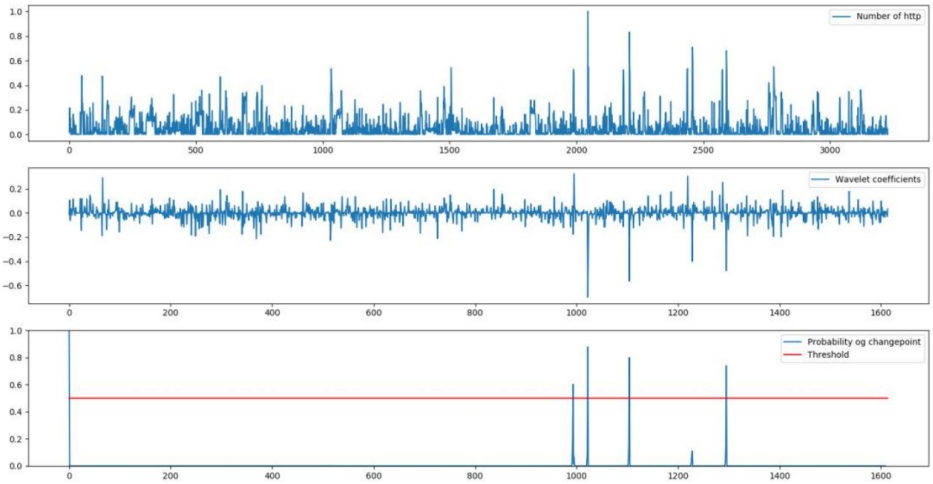

Fig. 2. Analysis of time series of abnormal traffic [4]

Thus, it has been experimentally proven that the developed method, which demonstrates the application of the Bayesian algorithm to the parameters of time series of network traffic, transformed using the wavelet transform, was effective.

Automatic detection of anomalies in network traffic. Automatic detection of anomalies in network traffic is an important and difficult task. In [5] it was shown that to create a wavelet analysis system for network traffic monitoring it is expedient to use Haar wavelet $\psi_{m,\ k}(t)$, scaling function $\phi_{m,\ k}(t)$, and fast wavelet analysis algorithm (Mallat algorithm) to obtain the best result in comparison of IDS (Intrusion Detection System) Snort and StopAttack with created on the basis of use of wavelet – transformation of the program of the anomaly analyzer (AA).

Test verification of the developed method of substantiation of the threshold level of anomalous activity of network subjects was performed using the MATCAD package. The evaluation of the efficiency of the prototype of the automatic intrusion detection system was carried out on the experimental section of the telecommunication network of the electronic document management and interaction management system. The results of the experiment are presented in Figure 3.

Intrusion type	IDS	Average time detection, sec.	Probability of detection,%	Accuracy rating
Port scanner	Snort	4,11	86	0,04
	StopAttack	3,86	84	0,0376
	AA	3,8	94	0,028
Denial of Service	Snort	2,08	72	0,0724
	StopAttack	1,22	79	0,0674
	AA	0,98	84	0,05
Server attack	Snort	2,78	66	0,023
	StopAttack	2,46	70	0,046
	AA	2,28	84	0,049
Spam	Snort	–	–	–
	StopAttack	3,6	80	0,043
	AA	3,15	86	0,0469

Fig. 3. Results of the comparative characteristics of IDS [5]

In comparison with the known IDS, the proposed AA solution takes higher characteristics: speed by 10–12%, probability of missed attack by 12–22%, with a permissible level of probability of false alarm 5% and with a probability of detection of 78–88%.

Purpose of the Study

With a continuous change of parameters for the calculation of the wavelet spectrum requires large computational costs. Most wavelet functions are redundant. It is necessary to

sample the parameters while maintaining the possibility of restoring the signal from its conversion. To begin the analysis of traffic on the chosen technology it is necessary to apply WT and to choose effective tools of wavelet analysis. WT is a signal in the form of a generalized series or Fourier integral on a system of basic functions, which are constructed from the parent (original) wavelet due to time shift operations and changes in time scale. The use of wavelet spectrum will determine the time of onset of signal frequency changes [6].

One of the methods for processing noisy signals is trasholding. It represents the decomposition of the considered signal into a wavelet spectrum with its subsequent processing [7]. When considering a discrete signal, the study needs to check the correctness and effectiveness of methods for suppressing the noise part of a typical signal. Using WT with subsequent reconstruction, it is possible to obtain a signal without degrading its quality. Together with noise cleaning and the use of an effective algorithm WT, it is possible to identify an existing network attack by an anomaly threshold.

Description of Main Material of Research

Purification of noise from the analyzed signal. Noise is considered to be high–frequency components of the signal. Noise reduction is an important process of eliminating noise from a useful signal in order to improve its subjective quality or to reduce the level of errors in transmission channels and digital data storage systems.

All recording devices, both analog and digital, have properties that make them susceptible to noise. The noise can be random and incoherent, ie not related to the signal itself, or coherent, introduced by recording devices and processing algorithms. Often in the communication lines, the signals are exposed to interference "white noise", which create detailed coefficients with a high content of noise components that have large random emissions of signal values.

Traditionally, to solve these problems, the method of noise attenuation of high–frequency components of the spectrum known from the practice of filtration is used. In addition, using wavelets, there is another method – limiting the level of detail coefficients. By setting a certain threshold for their level and "cutting off" the coefficients below this threshold, you can significantly reduce the noise level and compress the signal.

In discrete wavelet transform, the signal is decomposed into approximating coefficients representing the smoothed signal and detailing coefficients describing the noise oscillations. Therefore, the noise component is better reflected in the detail coefficients. Such components can be removed using a reset procedure or recalculation of the detail coefficients, the values of which are smaller than the threshold value. The most important thing is that the threshold level can be set for each factor separately. This allows you to build adaptive to signal changes methods of cleaning from noise.

There can be different types of restriction thresholds: soft or flexible and hard or hard. At the same time various rules of a choice of a threshold are established: adaptive, heuristic, minimax.

The procedure of threshold processing, or "thrasholding", today, is a promising tool for "cleaning" signals from noise (high–frequency components).

The quality of signal attenuation and, therefore, the degree of increase in the signal–to–noise ratio depends not only on the type of thrasholding function, but also on the method of its application. Depending on this, thrasholding is divided into global and local, and local in turn into general and multilevel.

From the study [8] the size of the remote noise signal is much smaller than the output signal, so the data will take up less space and is better suited for transmission over the Internet.

Choice of wavelet basis. WT offers a large set of data processing tools that help to divide the output signal into components and see its structure at different scales. The choice of wavelet base is an important issue before starting the detection procedure. But there is no universal method that will offer a choice of wavelet basis. The choice of the wavelet, leaving the study of the received signal, most often depends on the output signal [9]. Because wavelets have good frequency–time adaptation, they can be a handy tool for studying the frequency characteristics of a signal.

According to the frequency approach, the resulting range of wavelets can be divided into two components - low-frequency and high-frequency. The frequency of their separation is equal to half the sampling frequency of the signal. The main idea is to use a wavelet basis, each function of which characterizes both a certain spatial (temporal) frequency and the place of its localization in physical space (in time).

Function, which is usually called a wavelet, highlights the details of the signal and its local features. Functions that are well localized in both the time and frequency domains are usually selected as analytical wavelets.

Today there are whole wavelet families: Haar, Dobeshi, Simlet, Koiflet, Meyer, Gauss, Shannon, biorthogonal and others, each of which has certain advantages. The Haar wavelet has a compact media and provides signal and function reconstruction. Each function is strictly localized in physical space (in time), but is characterized by a slowly decreasing frequency spectrum. That is, spatial (temporal) and frequency characteristics cannot be measured simultaneously with arbitrarily high accuracy. The advantages of the Haar basis are that fast algorithms for fiberboard execution have been developed for it [10]. The decomposition of the signal in the system of basic Haar functions has the following structure. The first basic function is a straight line. In the case of a normalized basis, the convolution of the first basic function with the output signal will determine the average value of the function. The following basic functions of the Haar decomposition are scaled by the degree of two shifted steps. The system of basic Haar functions in a discrete space must be given by two parameters(1) – shift and frequency:

$$\varphi_{ab}(t) = \frac{1}{\sqrt{a}}\varphi(\frac{t-b}{a}), \tag{1}$$

where $\varphi_{ab}(t)$ – Haar basis function,

a – frequency of the basic function,

b – shift.

Studies [11] have shown that it is advisable to use a Haar wavelet to monitor network traffic, because with a high reliability of a significant criterion a, the type of wavelet has a significant impact.

Choice of wavelet transform algorithm. The essence of Mallat algorithm operations is as follows. Representation of the signal in the form of a set of successive approximations of the approximating and detailing components to which a set of filters is used – low–frequency and high–frequency. First, the signal is passed through a low–pass filter, resulting in approximation coefficients that characterize the global trend of the series under study. The output sequence is also passed through a high–pass filter, with the output of the detail coefficients that characterize the local features of the data series. To increase the frequency resolution, it is possible to re–decompose for the approximation coefficients of the previous level. In the context of intensive exchange of network traffic components, there will be even more interest in analyzing local data features to detect threats using parameters generated from traffic data to improve the detection of low–duration and high–intensity network attacks.

WT with a consistent increase in the values of the components of traffic leads to the form of rapid iterative calculations of wavelet coefficients. Equations of fast iterative calculations of wavelet coefficients provide realization of fast WT one–dimensional

numerical series on the basis of pyramidal algorithm of calculation of wavelet coefficients (Mallat algorithm).

Using discrete wavelet – packet transformation. When considering discrete wavelet packet transformation (DWPT) according to Mallat algorithm [12], the signal is split at each step. High–frequency and low–frequency components are obtained and the high–frequency component is cut off. Because the low frequency region contains more information about the output signal than the high frequency region. Recognition by wavelet coefficients, which are several times less than the signal discrete, will reduce computational costs [13].

The use of DWPT provides a wider part of the frequency range than DWT. From the set of possible bases of wavelet decomposition at all levels of detail, values with the condition are selected experimentally taking into account time constraints. That is, on which the abnormal state of traffic is most clearly manifested.

It is proposed to use the criterion of minimum entropy as a criterion for choosing the optimal basis. It characterizes the level of averaging and determines the number of significant coefficients of the traffic model. The criterion is the ratio of variances and mean DWPT coefficients. The adaptation of the decomposition level selection is as follows. If at any level of DWPT there is an excess of the upper threshold, the decision on existence of an anomaly is made. If at this level the lower threshold is exceeded, then there may be an anomaly in this place. Then further wavelet decomposition is performed to the next level, at which the analysis is performed again. This happens until the value of the relationship exceeds the upper threshold. This will indicate possible attacks. Or it will stop exceeding the threshold at all. This will indicate the absence of anomalies. In Figure 4 shows graphs of outgoing traffic (top right). Also shown is the optimal decomposition tree (top left) and the restored random component of traffic on one node (6.1) (bottom left). The anomaly in this case is the result of a SYN–Flood attack. Because on the restored random component of the signal, the peaks coincide on the time axis with the anomalies in the output traffic. Anomalies are well localized by inverse DWPT when using sample nodes of the optimal decomposition tree. A window similar to the main menu of the ToolBox Wavelet – wavemenu with the selected option – wavelet–packet 1–D was used to conduct the experiment.

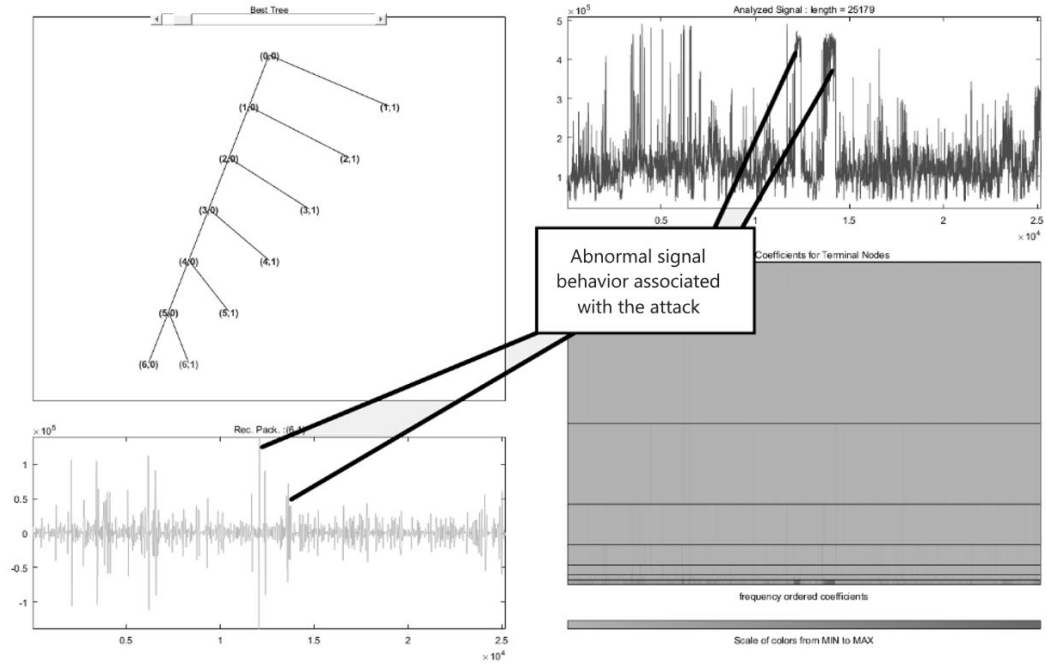

Fig. 4. Results of wavelet packet decomposition by Haar functions

Conclusions

According to the results of the study, it can be concluded that there is a vulnerability for MS, according to which an attacker can implement a DoS–attack, or another network attack, which can be specially configured for certain protection limits. Then the presence of detection by WT will significantly increase the possibility of detecting such an attack. During the work, we developed our own method of detecting anomalies and network attacks based on the integration of the wavelet packet model of network traffic in the interactive development environment Matlab, namely, identified a number of parameters that are taken into account when implementing WT.

Considering the features of this work, we can make the following recommendations:

- network traffic anomalies can be divided into two major classes – short–term and long–term.
- application of the Haar wavelet function to improve the correct detection characteristic in WT–based detection systems;
- when changing the length of the wavelet filter, it is possible to observe an increase in the detection efficiency.
- the analysis of efficiency of algorithms of WT that in general makes 70–94% of correct detection of an anomaly is carried out;
- when using WT, a jump in the energy distribution dispersion becomes noticeable, which can be recorded at an early stage of the attack, well ahead of the accumulation of overload, which makes it effective for detecting the attack;
- promising is the method of detecting network traffic anomalies using entropy [14];
- Mallat algorithm makes it possible to analyze the frequency–time representation of the signal on low–frequency and high–frequency components, which provides the ability to localize signal anomalies of different types;
- use of DWPT, which significantly reduces computational costs in the decomposition of WT components.

References

1. Tverdohleb J., Dubrovin V., Zakharova M. Wavelet technologies of non–stationary signals analysis. *1–th IEEE International Conference on Data Stream Mining & Processing.* Ukraine, Lviv: LPNU, 2016. P. 75–79.
2. Mohammed Alharbi and Marwan Ali Albahar. Time and frequency components analysis of network traffic data using continuous wavelet transform to detect anomalies. *ICIC International 2019* / ISSN 1349–4198. 2019, № 4(15). P. 1323–1336.
3. Shwan D., Perry X. Wavelet Transform for Educational Network Data Traffic Analysis, Wavelet Theory and Its Applications. Sudhakar Radhakrishnan. 2018. 268 p.
4. Соловьев Н.А., Тишина Н.А., Цыганков А.С., Юркевская Л.А., Чернопрудова Е.Н. Методы спектрального анализа в задаче обнаружения аномалий информационных процессов телекоммуникационных сетей: монография. Оренбург: ОГУ, 2013. 171 с.
5. Lavrova D., Semyanov P., Shtyrkina A., Zegzhda P. Wavelet–analysis of network traffic time-series for detection of attacks on digital production infrastructure. *SHS Web of Conf.* 2018. Vol. 44. P. 1–8.
6. Аносов А.О., Проценко М.М., Дубинко О.Л., Павлунько М.Я. Застосування вейвлет-перетворення для аналізу цифрових сигналів. *Сучасний захист інформації.* 2018. №1(33). С. 38–42.
7. Московский С.Б., Сергеев А.Н., Лалина Н.А. Очистка сигнала от шумов с использованием вейвлет-преобразования. *Universum: технические науки: электрон. научн. журн.* 2015. №2 (15). С. 1-2.

8. Donghong S., Zhibiao S., Wu L., Ping R., Jian–ping W. Analysis of Network Security Data Using Wavelet Transforms. *Journal of Algorithms & Computational Technology*. 2003. Vol. 8. №1. P. 59–79.
9. Dubrovin V.I., Tverdohleb J.V., Kharchenko V.V. R-peaks detection using wavelet technology. *Радиоэлектроника, информатика, управление.* 2013. №2 (29). С. 126–129.
10. Проценко М.М., Павлунько М.Я., Мороз Д.П., Бржевська З.М. Методика фільтрації цифрових сигналів з використанням швидкого вейвлет–перетворення. *Сучасний захист інформації.* 2019. №1 (37). С. 64–69.
11. Шелухин О.И., Филинова А.С. Сравнительный анализ алгоритмов обнаружения аномалий трафика методами дискретного вейвлет–анализа. *T–Comm – Телекоммуникации и Транспорт.* 2014, Т. 8, № 9. С. 89–97.
12. Проценко М.М., Куртсеітов Т.Л., Павлунько М.Я., Бржевська З.М. Застосування пакетного вейвлет–перетворення для обробки радіотехнічних сигналів. *Сучасний захист інформації.* 2018, №3 (35). С. 11–15.
13. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Научно – техническое издательство Горячая линия – Телеком. 2016. 221 с.
14. Дубровин В.И., Твердохлеб Ю.В. Исследование изменений энтропии и энергии при разложении сигналов. *Радиоэлектроника, информатика, управление.* 2013, № 2 (29). С. 54–58.

References

1. Tverdohleb, J., Dubrovin, V. & Zakharova, M. (2016). Wavelet technologies of non-stationary signals analysis. *1–th IEEE International Conference on Data Stream Mining & Processing*. (Ukraine, Lviv, 23-27 August, 2016). Lviv: LPNU, 75–79.
2. Mohammed, Alharbi & Marwan, Ali Albahar. (2019). Time and frequency components analysis of network traffic data using continuous wavelet transform to detect anomalies. *ICIC International 2019.* ISSN 1349–4198. **4** (15), 1323–1336.
3. Shwan, D. Perry X. (2018). Wavelet Transform for Educational Network Data Traffic Analysis, Wavelet Theory and Its Applications. Sudhakar Radhakrishnan.
4. Solovev N.A., Tishina N.A., Tsyigankov A.S., Yurkevskaya L.A., Chernoprudova E.N. (2013). Metodyi spektralnogo analiza v zadache obnaruzheniya anomaliy informatsionnyih protsessov telekommunikatsionnyih setey: monografiya. Orenburg: OGU.
5. Lavrova, D., Semyanov, P., Shtyrkina, A. & Zegzhda, P. (2018). Wavelet–analysis of network traffic time-series for detection of attacks on digital production infrastructure. *SHS Web of Conf.* **44**, 1–8.
6. Anosov, A.O., Protsenko, M.M., Dubinko, O.L. & Pavlunko, M.Ya. (2018). Zastosuvannya veyvlet-peretvorennya dlya analIzu tsifrovih signalIv. *Suchasniy zahist InformatsIYi.* **1** (33), 38–42.
7. Moskovskiy, S.B., Sergeev, A.N. & Lalina, N.A. (2015). Ochistka signala ot shumov s ispolzovaniem veyvlet-preobrazovaniya. *Universum: tehnicheskie nauki: elektron. nauchn. zhurn.* **2** (15), 1-2.
8. Donghong, S., Zhibiao, S., Wu, L., Ping, R. & Jian–ping, W. (2003). Analysis of Network Security Data Using Wavelet Transforms. *Journal of Algorithms & Computational Technology*. **8**, 1, 59–79.
9. Dubrovin, V.I., Tverdohleb, J.V. & Kharchenko, V.V. (2013). R–peaks detection using wavelet technology. *Radio Electronics, Computer Science, Control.*, **2** (29), 126–129.

10. Protsenko, M.M., Pavlunko, M.Ia., Moroz, D.P. & Brzhevska Z.M. (2019). Metodyka filtratsii tsyfrovykh syhnaliv z vykorystanniam shvydkoho veivlet–peretvorennia. *Suchasnyi zakhyst informatsii*. **1** (37), 64–69.
11. Sheluhin, O.I. & Filinova, A.S. (2019). Sravnitelnyiy analiz algoritmov obnaruzheniya anomaliy trafika metodami diskretnogo veyvlet–analiza. *T–Comm – Telekommunikatsii i Transport*. **8**, 9, 89–97.
12. Protsenko, M.M., Kurtseitov, T.L., Pavlunko, M.Ia. & Brzhevska, Z.M. (2018). Zastosuvannia paketnoho veivlet–peretvorennia dlia obrobky radiotekhnichnykh syhnaliv. *Suchasnyi zakhyst informatsii*. **3** (35), 11–15.
13. Sheluhin, O.I., Sakalema, D.Zh. & Filinova, A.S. (2016). Obnaruzhenie vtorzheniy v kompyuternyie seti (setevyie anomalii). Nauchno – tehnicheskoe izdatelstvo Goryachaya liniya – Telekom.
14. Dubrovin, V.I. & Tverdohleb, Yu. V. (2013). Issledovanie izmeneniy entropii i energii pri razlozhenii signalov. *Radio Electronics, Computer Science, Control.* **2** (29), 54–58.

Дубровін Валерій Іванович – к.т.н., професор, професор кафедри програмних засобів національного університету “Запорізька Політехніка”, e–mail: vdubrovin@gmail.com, ORCID: 0000–0002–0848–8202.

Петрик Богдан Вячеславович – студент кафедри програмних засобів національного університету “Запорізька Політехніка”, e–mail: dartbogdan32@gmail.com, ORCID: 0000–0002–9528–4610.