UDC 004.056.57

V.I. HOROBETS, V.I. DUBROVIN
National University "Zaporizhzhia Polytechnic"
J.V. TVERDOHLIB
Freshcode Zaporizhzhya

DETECTION OF UNAUTHORISED ACTIONS AND ATTACKS IN NETWORKS OF THE METHOD OF WAVELET ANALYSIS

Behavioural methods based on the models of "normal" functioning of an information network. The principle of work is in identifying differences between the current state of the information system functioning and the one that is thought to be examplary for this network. Any discrepancy is seen as an intrusion or anomaly.

Perspective method for detecting unauthorised invasions must have high accuracy of detection known and unknown types of cyberattacks, perfectly own accuracy of decision-making, that is low number of false positives.

The detecting cyberattacks method based on wavelet analysis (WA) proved itself well in struggling against non stationary signals. The wavelet transform (WT) has a self-adjusting moving frequency-time window, but equally well reveals both low-frequency (LF) and high-frequency (HF) characteristics of the signal on different time scales. Wavelet filters allow not only to fight against noise, but also to extract the necessary components of the signal.

Today's society cannot do without information technology. IT plays a major role in and is an integral part of every sphere of our life. Current development of the information society is inextricably linked with collecting, processing and passing huge amounts of data, and converting data into a product that has significant value. This is the main reason behind the global shift from the industrial society to the information society. The invention of the Internet has led to a significant increase in international communication in various spheres of human life.

On the other hand, along with a large number of benefits, there has been a significant number of threats related to the current technology. There are currently multiple threats now on both national and international level. Therefore, different mechanisms for protecting cyberspace are now part of many countries' national strategy

Network anomalies are so varied that they cannot be categorized using one simple classification. The number of attacks, their power and complexity are increasing. Malicious users are looking for radically new ways of network intrusion and the existing methods of cyber protection often turn out to be inefficient. [1].

Keywords: wavelet basis, wavelet analysis, wavelet filter, de-noise suppression, network traffic, sinusoid, network anomaly.

В.І. ГОРОБЕЦЬ, В.І. ДУБРОВІН
Національний університет «Запорізька Політехніка»
Ю.В. ТВЕРДОХЛІБ
Навчальний центр Freshcode м. Запоріжжя

ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ДІЙ ТА АТАК В МЕРЕЖАХ МЕТОДОМ ВЕЙВЛЕТ-АНАЛІЗУ

Поведінкові методи засновані на моделях «нормального» функціонування інформаційної мережі. Принцип роботи полягає у виявленні відмінностей між поточним станом функціонування інформаційної системи та тим, який вважається зразковим для цієї мережі. Будь-яка невідповідність розглядається як вторгнення або аномалія

Перспективний метод виявлення несанкціонованих вторгнень повинен мати високу точність виявлення відомих та невідомих типів кібератак, володіти бездоганною достовірністю прийняття рішень, тобто низьким числом хибних спрацьовувань.

Метод виявлення мережевих атак на основі вейвлет-аналізу (ВА) добре зарекомендував себе в боротьбі з нестаціонарними сигналами. Вейвлет-перетворення (ВП) володіє самоналагоджувальним рухомим частотно-часовим вікном, однаково добре виявляє як низькочастотні (НЧ), так і високочастотні (ВЧ) характеристики сигналу на різних часових масштабах. Вейвлет-фільтри дозволяють не тільки боротися з шумами, але і витягувати необхідні компоненти сигналу.

Сьогодні сучасне суспільство вже не може обійтися без інформаційних технологій. Вони виконують головну роль та є невід'ємною частиною всіх сфер життя людини. Нинішній розвиток інформаційного суспільства нерозривно пов'язаний з необхідністю збору, обробки і передачі величезних об'ємів інформації, перетворенням інформації у товар, який має значну вартість. Це головна причина глобального переходу від індустріального суспільства до інформаційного. Поява всесвітньої мережі Інтернет спричинила масштабне зростання міжнародних спілкувань у різних сферах людського життя.

З іншого боку, поряд із великою кількістю переваг з'явилася значна кількість загроз, пов'язаних із функціонуванням сучасних технологій. Дане явище призвело до появи значної кількості небезпек, які вражають суспільство як на національному рівні, так і міжнародному. Отже, з'явилася потреба в механізмах захисту

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

кіберпростору, які описуються в національних стратегіях світових держав, що в свою чергу присвячені забезпеченню його захисту.

Відомі мережеві аномалії настільки різноманітні, що їх не можна категоризувати за допомогою однієї простої класифікації. Швидко зростає кількість атак, їх потужність та складність. Зловмисники шукають принципово нові методи незаконних втручань у мережу і дуже часто існуючі засоби захисту виявляються безсилими перед ними [1].

Ключові слова: вейвлет-базис, вейвлет-аналіз, вейвлет-фільтр, шумоподавлення, мережевий трафік, синусоїда, мережева аномалія.

Problem formulation

This article offers an approach for analysis of digital production security based on evaluation of a posteriori probability for change point in time-series, which are based on the change point coefficient values of digital wavelet-transform in the network traffic time-series. These time-series make it possible to consider the network traffic from several points of view at the same time, which plays an important role in the task of detecting network attacks. The attack methods vary significantly; therefore, in order to detect them it is necessary to monitor different values of various traffic parameters. The proposed method has demonstrated its efficiency in detecting network service denial attacks being realized at the application level..

Types of network attacks

Detecting network attacks is crucial because they can result in data breach or data tampering. Normally, one of the signs of a network attack is the appearance of a network anomaly. Network anomalies might be caused by different reasons including malicious users, incompetent users, hardware and software defects. There are visible anomalies that can be seen in information systems malfunctioning, and anomalies which have no visible signs but can lead to a system failure in the long run. Network anomalies can be divided into two groups: software and hardware anomalies and security issues (figure 1) [2].

Normal work of network devices and PC users can be described by a certain system of behaviour. The work users perform is normally defined by their working responsibilities, which implies using the same network resources, certain activity of the network devices, the direction of the inbound/outbound traffic on the ports of the network switches, routers, servers, and firewalls. As a rule, users use the same information resources in the local network: corporate portals, email and files servers.

Network attacks can be divided into active and passive ones. Active attacks have a visible influence on the system resulting in changing its state. Examples include malware that is inserted in a program, tampering with the data on a webpage, blocking a network service by bombarding it with requests. The defining feature of active attacks is that they leave traces.

Memory storage is changed, there are strange diagnostic messages, apps start working incorrectly, they might freeze or crash altogether, there are weird surges in activity in the network traffic properties and other static data about the system's performance. However, a carefully planned active attack can go unnoticed if the specialists who are in charge of network protection have no thorough understanding of the consequences of such attacks.

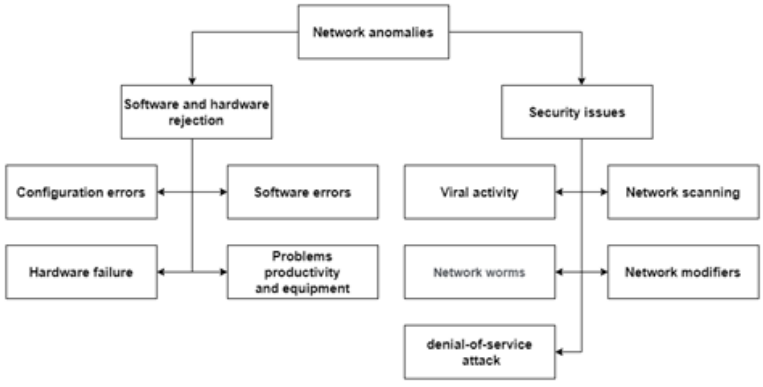

Fig. 1. Basic types of network anomalies [2]

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

Passive attacks do not disrupt normal functioning of the system-they have to do with collecting information about the system and eavesdropping on the intranet traffic. In many cases, passive attacks leave no traces, so they are hard to detect and they often go unnoticed [3].

DoS-attack and DDoS-attack

Active attacks include two highly common attacks: a denial-of-service attack (DoS-attack) and a distributed denial-of-service attack (DDoS attack).

In a DoS-attack, the system that was designed to process the requests of legal users suddenly stops doing this or does so with significant delays, which is equivalent to denial of service. A denial of service can occur as a result of malicious actions when overload is created deliberately: a barrage of requests is sent to a computer being attacked by the attacking computer. This barrage of requests «floods» the computer under attack causing an overload and, eventually, making it inaccessible. Blocking happens as a result of exhausting the resources of the CPU, operating system or bandwidth.

The malicious user can dramatically increase the negative effect of conducting a DoS-attack by stealing the computing power for their own use. In order to do this, the malicious user gains control of the computer, instals special malware into it and activates it. In this way, the malicious user takes hold of part of the computing power of the computer under attack without the computer's owner being aware of it.

Fig. 2. An example of a DDoS attack [4]

In this case, the owner of the computer under attack suffers no other losses apart from a fall in computer's performance. For a more powerful attack, the malicious user gains control of several computers, synchronises their work and directs a common barrage of requests from these computers to the computer they want to target. An attack of this kind is called a distributed denial-of-service attack (DDoS attack).

Spoofing

When carrying out network attacks, it is important for the malicious user not only to achieve their goal, which is doing harm to the object being targeted, but also to cover their tracks. One of the main ways of doing this is replacing the content of packages, or spoofing. In particular, in order to hide the location of the source of malicious packets, the malicious user changes the value of the sender's address field in the packages' headers. Since the sender's address is generated automatically by the system's software, the malicious user makes changes to the respective software modules in a way to be able to send packages with any IP-addresses from their computer [5].

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

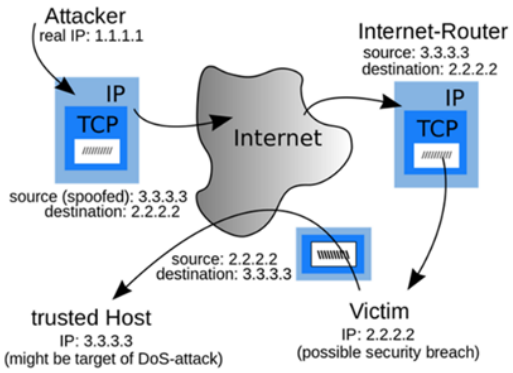

Fig. 3. An example of spoofing [4]

Algorithms and ways of detecting network anomalies

When researching normal behaviour, a profile that describes a network's normal performance needs to be created. This statistics can be received from network devices such as network switches, firewalls, and proxy servers with the help of active monitoring. Then this data needs to be analyzed and stored in a database. Any deviation from the rules of the profile that has been created needs to be subjected to the analysis of the network anomalies detection system. The analysis shows that there are numerous algorithms for detecting network anomalies. These algorithms are described below.

Algorithm based on discrete WT (wavelet transform) with the use of statistical criteria. In this algorithm, a sliding window method is used (W1 and W2), which lets one increase the chance of detecting insignificant anomalies. The main advantage of this algorithm is that an attack is well detected on any level of CWT decomposition (an F-factor detects an attack most notably).

The Brodsky-Darkhovsky algorithm of detecting anomalies. When selecting a standard mode, it is the noises that detect the special influence. When selecting the algorithm in the sliding window mode, the total number of obstacles decreases, and the surges that signal the beginning and end of the influence are more notable. For practical usage, it is better to use the algorithm in the sliding window mode.

The algorithm based on the sum of squared wavelet coefficients. The biggest effect is detected when using the Haar coefficients of approximation for wavelets on the higher levels of decomposition. Increasing the size of the analysis window can lead to the increase of the correct detection of an anomaly, but the likelihood of erroneous detection increases as well.

The algorithm based on the maximum of squared wavelet coefficients. This algorithm is less efficient than the one based on the sum of squared wavelet coefficients.The most informative display of an attack in this algorithm can be achieved by approximation coefficients with the use of the Haar wavelet.

Another way of detecting attacks is using a firewall. A firewall is a combination of software and hardware that isolates the internal network from the Internet. It allows certain packets to pass while blocking others. A firewall lets the network administrator control access to the corporate networks, which happens externally as well as control the resources of the admin network by regulating the incoming and outgoing traffic.

All firewalls fall into three categories::

- traditional packet filtering firewalls;
- circuit-level gateways;
- application-level gateways.

In packet filtering firewalls all the incoming and outgoing traffic of the internal corporate network passes through a router in which packets are filtered. A packet filtering firewall checks every datagram and determines what needs to be done with it based on the rules defined by the network administrator. The network administrator configures the firewall based on the organisation policy.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

Circuit-level gateways monitor the TCP connection and do the filtering based on this information. All the current TCP connections are monitored in a special connections table. If the incoming packet does not belong to the current connection, it will be declined by the firewall.

Application-level gateways that are aimed at providing more localized security combine the features of packet filtering firewalls and application-level gateways. An application-level gateway is a server that works on the application level and through which all the application data, both incoming and outgoing, passes. Several application-level gateways can work on one hosting, but each each gateway is a separate server with its own set of processes [4].

Intrusion detection systems

Intrusion detection systems let one detect various attacks, including tracerouting, port scanning, TCP scanning, DoS-attacks, worms and viruses as well as attacks on the operating system's or certain applications' vulnerabilities.

An organization's network can have several such systems. When they work simultaneously, they work in sync, sending messages about suspicious network traffic to the CPU which collects and systematizes this data and informs the administrator if necessary. Intrusion detection systems can be signatures-based and anomaly-based.

Signature-based systems have large databases of the attacks' signatures. Each signature is a set of rules that describes ways of fighting the attacks. This system analyzes each packet that goes through it and compares it to the signatures from the database. If the packet matches the signature, a warning is generated. The downsides to this approach are that the system is helpless against unregistered attacks, the matches with the signatures can turn out to be not an attack and when comparing a packet with a large collection of signatures, the system may perform poorly under the strain and miss malicious packets.

An anomaly-based system creates a profile of reliable traffic that works in a normal mode. Then it detects streams of packets that have static peculiarities. For instance, a disproportionate increase in packets or an abrupt surge of intensity in port scanning.The main benefit of these systems is their ability to detect new attacks that have not been previously described, yet it is incredibly hard to differentiate between normal traffic and unusual one.

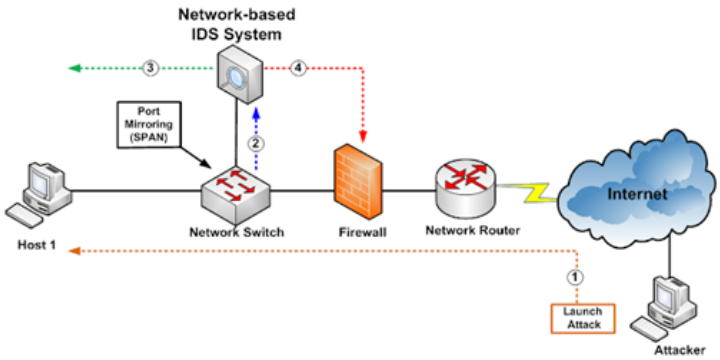

Fig. 4. An intrusion detection system [4]

Wavelet properties

A wavelet is a mathematical function that allows a signal to be divided into different frequency and time components. The term «wavelet» that stands for «a little wave» appeared relatively recently- it was introduced in mid 80s by Grossman and Morlet who were analyzing the properties of seismic and acoustic signals [6].

The graph of the function looks like a wave-like oscillation with an amplitude that decreases to zero far from the origin. However, in a general case the signals analysis is done in the frame of wavelet-coefficients (Scale-Time-Amplitude) [7].

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

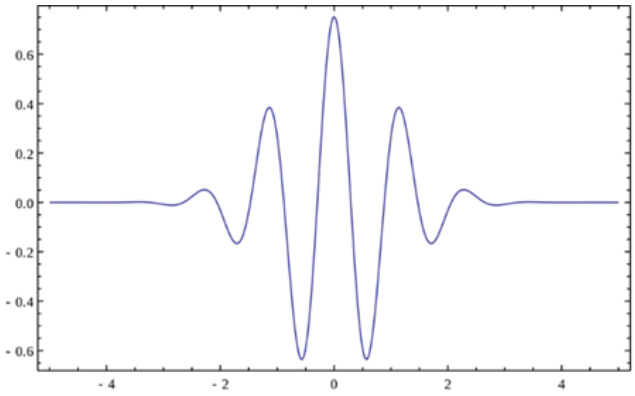

Fig. 5. Morlet wavelet [8]

WT is an integral transform that is a mix of a wavelet function with a signal. Wavelet transformation converts a signal from a temporal representation to a time-frequency one [9].

A method of converting a function (or signal) into a form that makes some of the output signal quantities more amenable to study, or allows the output data set to be compressed. WT is quite similar to the Fourier transform (or more like the windowed Fourier transform) but with a completely different evaluation function. The main difference is: the Fourier transform decomposes the signal into components in the form of sines and cosines, that are functions localised in Fourier space; however, WT uses functions localised in both real and Fourier space [10].

In numerical and functional analysis, DWTs refer to WTs in which wavelets are represented by discrete signals (samples).

The first DWT was invented by the Hungarian mathematician Alfred Haar. For an input signal represented by an array of 2^n numbers, the Haar WT simply groups the elements by 2 and forms sums and differences from them. Sums are grouped recursively to form the next level of decomposition. The result is $2^n - 1$ differences and 1 total.

This simple DWT shows the general useful characteristics of wavelets. First, the transformation can be performed in nlog2(n) operations. Secondly, it not only decomposes the signal into some semblance of frequency bands (by analysing it at different scales), but also represents the time domain, that is, the moments of occurrence of certain frequencies in the signal. Together, these properties characterise the fast WT – a possible alternative to the usual fast Fourier transform. When accepting the condition of randomness of the signal X, the spectral density of its amplitude Y is calculated based on the Yates algorithm:matrixY=matrix(±X), the reverse is also true matrixX=matrix(±Y).

FWT is an implementation of WT using arbitrary scales and practically arbitrary wavelets. The wavelets used are not orthogonal and the data obtained during this transformation are highly correlated. For discrete time sequences, this transformation can also be used, with the restriction that the smallest wavelet transfers must be equal to the data discretisation. It is sometimes called discrete-time GDP (DT-CWT) and is the most commonly used method for calculating CWT in real-world applications. We calculate the convolution of the signal with a scaled wavelet. For each scale, we obtain in this way a set of the same length N as the input signal.By using M arbitrarily chosen scales, we are getting an N×M field that directly represents the time-frequency plane.The algorithm used for this calculation can be based on direct convolution or on convolution using multiplication in Fourier space (this is sometimes can be called Fast wavelet transform).

The choice of wavelet to use in time-frequency decomposition is the most important thing to do. By doing this choice, we can influence the resolution of the result by time and frequency. This does not change the basic characteristics of the WT (low frequencies have good frequency resolution and poor time resolution; high frequencies have poor frequency resolution and good time resolution), but you can slightly increase the overall frequency or time resolution. This is directly proportional to the width of the wavelet used in real and Fourier space. For example, if a Morlet wavelet is used (the real part is a decaying cosine function), then one can expect a high frequency resolution, since

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

such a wavelet is very well localised in frequency. However, using the Derivative of Gaussian (DOG) wavelet, we will get good localisation in time, but poor in frequency.

FWT is commonly used for signal analysis. That is why it is widely used in scientific research of physical processes.

Advantages of WT

By conducting an analysis of the WT theory and comparing them with the main "opponent" – the Fourier transform, it was concluded that, despite the great role of the Fourier transform, the WT provides certain advantages in the analysis and processing of signals, which are:

- WTs have almost all the advantages of Fourier transforms;
- wavelet bases can be well localised both in terms of frequency and time;
- unlike to Fourier transforms, wavelet bases have quite a lot of various basic functions, the properties of which are oriented towards the solution of various tasks.

The disadvantage of WT is their relative complexity.

It is possible to conclude about the expediency of using WT to analyse and process signals for further detection of possible unauthorised actions or attacks in the network [11].

Processing of informational signals using WT

The number of different wavelet functions is very large, but not all of them may be suitable for the analysis of the input signal of the network.

Given that the signal, which has undergone analog-digital conversion, is presented in the form of statistical data – for effective processing of discrete signal segments, the WT must be discrete.

For successful decomposition into approximating (approximating) cAj and detailing cDj coefficients, the wavelet family must possess a scaling function that determines a rough approximation of the signal and generates approximation coefficients, as well as a wavelet function $\psi(t)$ that determines signal details and generates detailing coefficients [12].

From the orthogonal wavelets presented in the PyWavelets package, you can select a group of orthogonal wavelets with a compact carrier (of finite length):

- Dobesha wavelet – «db»;
- Simlet wavelet – «sym»;
- Coiflet wavelet – «coif»;
- Haar wavelet – «haar».

These types of wavelets have the following main parameters:

- the scaling function $\psi(t)$ exists;
- functions $\psi(t)$ and $\phi(t)$ have a compact support;
- the function $\psi(t)$ has several zero moments.

These four wavelet functions were used to analyse and process the input traffic signal. The results of the first-level decomposition of the input signal by different wavelets can be seen in the pictures 6-10.

Fig. 6. The input signal from the data format *.csv

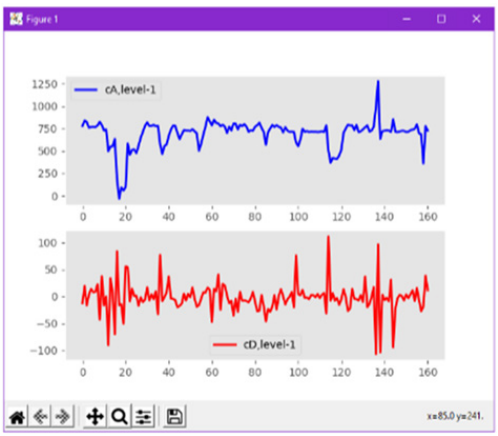

Fig. 7. The first level of signal decomposition into HF and LF using the Simlet-5 wavelet

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

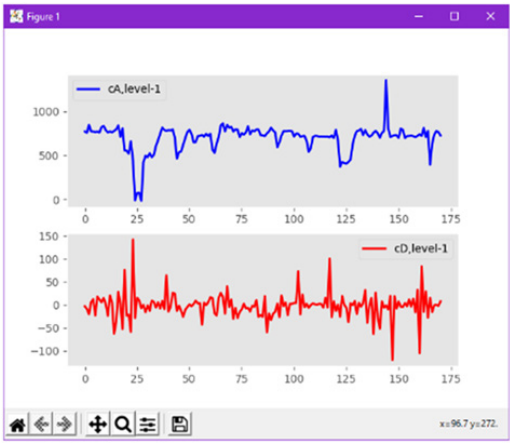

Fig. 8. The first level of signal decomposition in HF and LF using Coiflet-5 wavelet

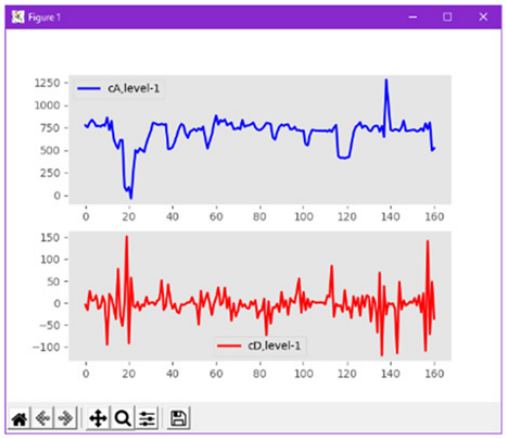

Fig. 9. The first level of signal decomposition in HF and LF using Dobesha-5 wavelet

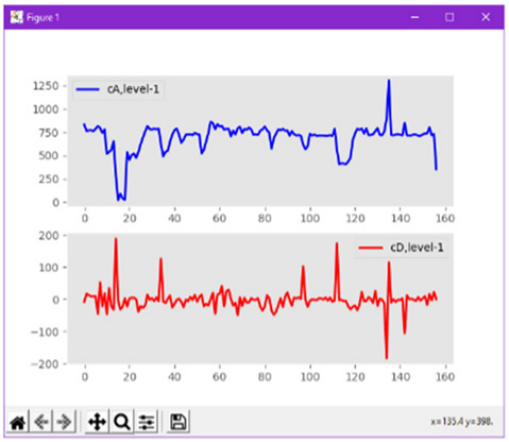

Fig. 10. The first level of signal decomposition into HF and LF using Haar-5 wavelet

Based on this, it is possible to conclude about the expediency of using the wavelet function of the 5-order Dobeshe family for the analysis and processing of signals for further detection of possible unauthorised actions or attacks in the network.

Analysis of the input signal with a selected wavelet function

To analyse the input signal, it is necessary to make a multi-level decomposition of this signal and obtain HF and LF graphs. Then choose the most informative level of decomposition. The approximation coefficients (cA) are the output of the low-pass filter (averaging filter) of the DWT. The detail coefficients (cD) represent the output of the high-pass filter (difference filter) of the DWT. The results of the multi-level decomposition of the signal by the Dobesha-5 wavelet function are shown in the pictures 11-15.

Based on the results of multi-level decomposition of the signal, it can be concluded that the higher the level of decomposition, the shorter the output signal of LF and HF. By approximating the input signal, you can see in which intervals the signal behaves abnormally.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

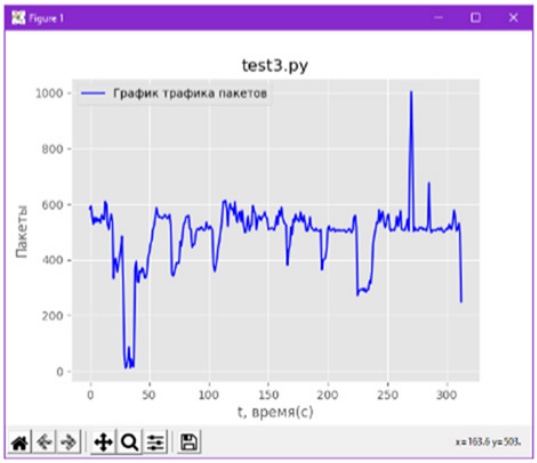

Fig. 11. The input signal from the data format *.csv

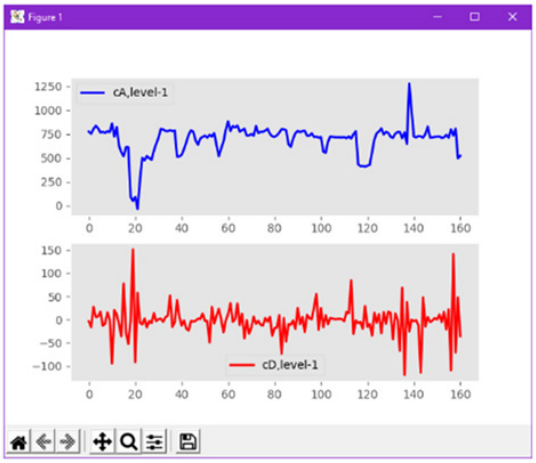

Fig. 12. The first level of signal decomposition in HF and LF using Dobesha-5 wavelet

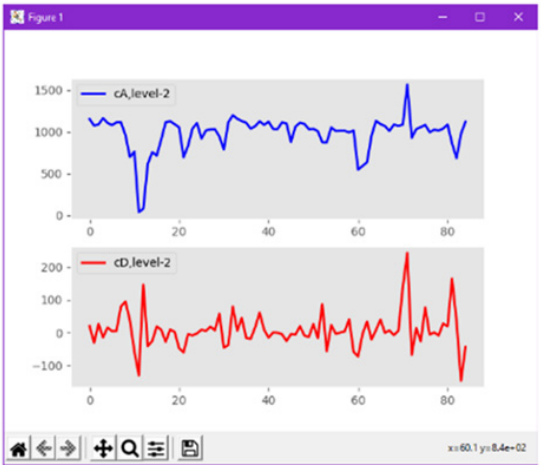

Fig. 13. The second level of decomposition of the signal into HF and LF using the Dobesha-5 wavelet

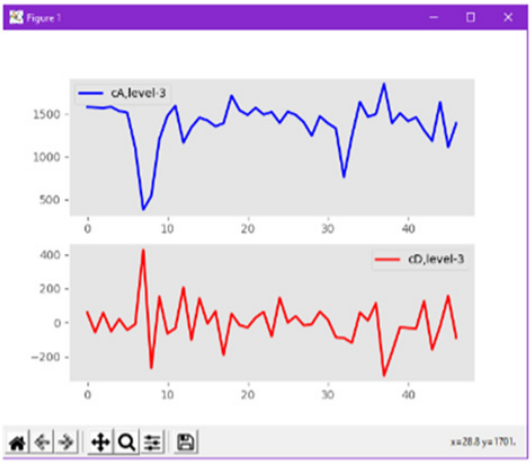

Fig. 14. The third level of signal decomposition into HF and LF using Dobesha-5 wavelet

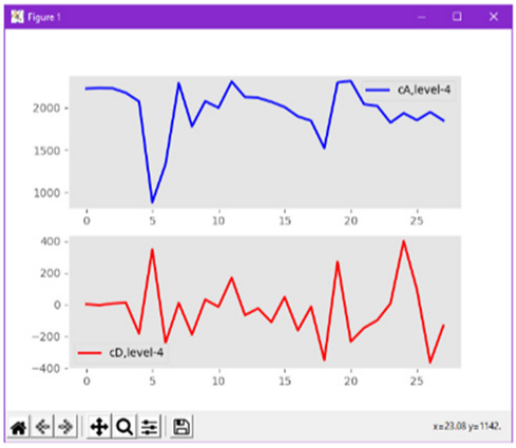

Fig. 15. The fourth level of signal decomposition in HF and LF using the Dobeshe-5 wavelet

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

A practical example of anomaly detection using WA

WA is classified as a behavioural attack detection method. This is a method that is based on the use of information about the normal behaviour of the system and its comparison with the parameters of the observed behaviour [13].

In practice, the average values of the following values aggregated for five-minute intervals were used as output data: the number of bytes per second, the number of packages per second, the number of flows per second, and the average size of a TCP package. In each case, the collected data was a discrete sequence of the frequency-time signal, which, according to the proposed BA algorithm, was decomposed into a hierarchy of several layers. For each of the extracted signals, the time variable was independent [14].

The presence of sharp amplitudes in each of the signals presented corresponded to certain groups of anomalies:

- anomalies caused by errors in network equipment settings, as well as equipment failure (G1);
- network attacks represented by the denial-of-service class (G2);
- congestion in the network (flash crowd), which arise as a result of sudden surges, for example, at times of increase in legitimate requests for downloading new software (G3);
- other anomalies, which include the exchange of large amounts of data, errors when recording traffic on the sensor or sending data to the NetFlow collector, which allows for analysis of network traffic at the session level (G4).

Three components of the primary signal were identified [14]. The LF component of the signal captured long-term network anomalies, which lasted for several days. The mid-frequency part had zero mathematical expectation and was intended to analyze fluctuations within one day. The HF part corresponded to small short-term changes, which can be considered as noise.

After splitting the original signal [14], the procedure for calculating the local variance within a sliding window of 3 hours was applied to its first two components. Next, the threshold analysis method is used. Anomaly is identified if the peak point of the last signal exceeded the specified threshold.

As a result of the study, it was concluded that the presented types of anomalous events can be identified at specific, inherent frequencies. Thus, coarse-grained anomalies of the G1, G2, and G4 classes are recognized at high and medium frequencies, while low- and medium-frequency signals correspond to the G3 class anomalies [10].

The disadvantages of WA can be called – the ambiguity of the choice of basis functions, the high computational complexity when calculating the coefficients of the signal decomposition. The task of correctly assigning the size of the window is non-trivial. As noted, if the size of the sliding window is much larger than the duration of the anomaly, then the frequency spike corresponding to it can be smoothed out, and thus the attack will be missed. Otherwise, if the size of the window is too small, then a flow of meaningless anomalies is inevitable.

Conclusion

WTs have practically all the advantages of Fourier transforms. Wavelet bases can be well localised both in frequency and in time. When highlighting well-localised multi-scale processes in the signals, only those large-scale levels of decomposition that are of interest can be considered.

Wavelet bases, in contrast to the Fourier transform, have many different basic functions, the properties of which are aimed at solving various problems. Basic wavelets can be both finite and infinite carriers implemented by functions of different smoothness.

The disadvantage of WT is the ambiguity of the choice of basis functions, great computational complexity when calculating the signal decomposition coefficients. The task of correctly assigning the size of the window is non-trivial. As noted, if the size of the sliding window is much greater than the duration of the anomaly, then the frequency spike corresponding to it can be smoothed out, and thus the attack will be missed. Otherwise, if the size of the window is too small, then an inevitable flow of meaningless anomalies.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

Список використаної літератури

1. 'Горобець В.І., Дубровін В. І., Твердохліб Ю.В. Поведінкові методи виявлення несанкціонованих дій та атак в мережах методом вейвлет-аналізу. *Комбінаторні конфігурації та їхні застосування*: Матеріали XXIII Міжнародного науково-практичного семінару імені А.Я. Петренюка, присвяченого 70-річчю Льотної академії Національного авіаційного університету (Запоріжжя–Кропивницький, 13-15 травня 2021 року) / за ред. Г.П. Донця – Кропивницький: ПП «Ексклюзив-Систем», 2021. 208 с.
2. Tverdohleb J.V., Dubrovin V.I. Processing of ECG signals based on wavelet transformation. *International journal of advanced science and technology*, 2011. Vol. 30. p. 73 – 81.
3. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. СПб.: Питер, 2016. 992 с.: ил. (Серия «Учебник для вузов»).
4. Види мережевих атак. Способи їх виявлення. – URL: http://holodoks.blogspot.com/2017/12/blog-post.html. (дата звернення 01.12.2022).
5. Куроуз Джеймс, Кит Росс. Компьютерные сети : Нисходящий подход : 6-е изд. М.: Издательство «Э», 2016. 912 с.
6. Астафьева Н. М. Вейвлет-анализ: основы теории и примеры. *Успехи физических наук*. М.: Наука, 1996. Том 166, №11. С. 1145-1170.
7. Смоленцев Н. К. Введение в теорию вейвлетов. Ижевск: РХД, 2010. 292 с.
8. Вейвлет. Википедия. Свободная энциклопедия. – URL: https://ru.wikipedia.org/wiki/Вейвлет (дата обращения 02.12.2022).
9. Дьяконов В. П. Вейвлеты. От теории к практике. М.: СОЛОН-Пресс, 2004. 440 с.
10. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак. *Труды СПИИРАН*. 2016. № 45. С. 207-244.
11. Вейвлет – преобразование. URL: http://gwyddion.net/documentation/user-guide-ru/wavelet-transform.html (дата обращения: 02.12.2022).
12. Критерии оценки качества алгоритмов обнаружения сетевых аномалий. URL: http://research-journal.org/technical/kriterii-ocenki- kachestva-algoritmov-obnaruzheniya-setevyx-anomalij.html (дата обращения: 03.12.2022).
13. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems. *Computer Networks*. 1999. Vol. 31. Issue 8. pp. 805–822.
14. Barford P., Kline J., Plonka D., Ron A. A signal analysis of network traffic anomalies. *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement*. 2002. pp. 71–82.

References

1. Horobets, V.I., Dubrovin, V. I., & Tverdokhlib, Yu.V. (2021). Povedinkovi metody vyiavlennia nesanktsionovanykh dii ta atak v merezhakh metodom veivlet-analizu. *Kombinatorni konfihuratsii ta yikhni zastosuvannia*: Materialy XXIII Mizhnarodnoho naukovo-praktychnoho seminaru imeni A.Ia. Petreniuka, prysviachenoho 70-richchiu Lotnoi akademii Natsionalnoho aviatsiinoho universytetu (Zaporizhzhia–Kropyvnytskyi, 13-15 travnia 2021 roku) / za red. H.P. Dontsia – Kropyvnytskyi: PP «Ekskliuzyv-System».
2. Tverdohleb, J.V., & Dubrovin, V.I. (2011). Processing of ECG signals based on wavelet transformation. *International journal of advanced science and technology*, **30**, 73 – 81.
3. Olifer, V. G., & Olifer, N. A. (2016). Kompyuternyie seti. Printsipyi, tehnologii, protokolyi: Uchebnik dlya vuzov. 5-e izd. SPb.: Piter.
4. Vydy merezhevykh atak. Sposoby yikh vyiavlennia. – URL: http://holodoks.blogspot.com/2017/12/blog-post.html. (data zvernennia 01.12.2022).
5. Kurouz, Dzheyms, & Kit, Ross. (2016). Kompyuternyie seti : Nishodyaschiy podhod : 6-e izd. M.: Izdatelstvo «E».

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

6. Astafeva, N. M. (1996). Veyvlet-analiz: osnovyi teorii i primeryi. Uspehi fizicheskih nauk. M.: Nauka, **166** (11), 1145-1170.
7. Smolentsev, N. K. (2010). Vvedenie v teoriyu veyvletov. Izhevsk: RHD.
8. Veyvlet. Vikipediya. Svobodnaya entsiklopediya. – URL: https://ru.wikipedia.org/wiki/Veyvlet (data obrascheniya 02.12.2022).
9. Dyakonov, V. P. (2004). Veyvletyi. Ot teorii k praktike. M.: SOLON-Press.
10. Branitskiy, A. A., & Kotenko, I. V. (2016). Analiz i klassifikatsiya metodov obnaruzheniya setevyih atak. *Trudyi SPIIRAN*. **45**, 207-244.
11. Veyvlet – preobrazovanie. URL: http://gwyddion.net/documentation/user-guide-ru/wavelet-transform.html (data obrascheniya: 02.12.2022).
12. Kriterii otsenki kachestva algoritmov obnaruzheniya setevyih anomaliy. URL: http://research-journal.org/technical/kriterii-ocenki- kachestva-algoritmov-obnaruzheniya-setevyx- anomalij.html (data obrascheniya: 03.12.2022).
13. Debar, H., Dacier, & M., Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. *Computer Networks*. **31** (8), 805–822.
14. Barford, P., Kline, J., Plonka, & D., Ron, A. (2002). A signal analysis of network traffic anomalies. *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement*, 71–82.

Горобець Владислав Ігорович – студент Національного університету «Запорізька політехніка», факультет комп'ютерних наук і технологій, програмна інженерія. e-mail: vladoshorobets@gmail.com, ORCID: 0000-0003-2905-9420.

Дубровін Валерій Іванович – к.т.н., професор кафедри програмної інженерії Національного університету «Запорізька політехніка». e-mail: vdubrovin@gmail.com, ORCID: 0000-0002-0848-8202.

Твердохліб Юлія Володимирівна – к.т.н. з інформатики, лектор веб fullstack розробки в навчальному центрі Freshcode (м. Запоріжжя), e-mail: julia.tverdohleb@gmail.com

https://doi.org/10.32782/mathematical-modelling/2022-5-1-1