Method for detection of the modified DDoS cyber attacks on a web resource of an Information and Telecommunication Network based on the use of intelligent systems

Svitlana Onyshchenko[1,†], Olena Haitan[1,*,†], Alina Yanko[1,*,†], Yurii Zdorenko[1,*,†] and Oleksandr Rudenko[1,†]

[1] National University «Yuri Kondratyuk Poltava Polytechnic», Pershotravneva Avenue 24, Poltava, 36011, Ukraine

Abstract

Web services hosted in Information and Telecommunication Networks (ITNs) require reliable protection against cyber attacks. Most modern information services are characterized by increased requirements to ensure availability. One of the negative types of cyber influence in ITN is denial-of-service attacks (DDoS). Existing approaches for detecting attacks of this class are primarily based on classical signature analysis, and may also be based on the use of artificial intelligence at the current state of information technology development. However, existing approaches to implementing detection systems do not take into account the potential modification of cyber attacks, which makes their detection challenging. Therefore, it is proposed to use intelligent systems to improve the recognition of modified cyber impacts aimed at denial of service of a web service in ITN. These systems should be configured based on information about the level of traffic anomalies and data on the individual behavioral characteristics of a web resource.

Keywords

Information and Telecommunication Network, attack, availability, denial of service, artificial intelligence, neuro-fuzzy system

1. Introduction

The development of new electronic services requires compliance with the security requirements for the hosting web resources, including ensuring data integrity, confidentiality, and availability. Availability is a crucial indicator of a web resource

MoDaST-2024: 6th International Workshop on Modern Data Science Technologies, May, 31 - June, 1, 2024, Lviv-Shatsk, Ukraine

* Corresponding author.

† These authors contributed equally.

s07onyshchenko@gmail.com (S. Onyshchenko); azalie@ukr.net (O. Haitan); al9_yanko@ukr.net (A. Yanko); zdorenkoviti@gmail.com (Y. Zdorenko); alexantr@gmail.com (O. Rudenko)

0000-0002-6173-4361 (S. Onyshchenko); 0000-0002-7228-9937 (O. Haitan); 0000-0003-2876-9316 (A. Yanko); 0000-000L-5649-771X (Y. Zdorenko); 0000-0002-7110-0653 (O. Rudenko)

security. The inability to access a resource at the appropriate time may result in negative consequences. Therefore, ensuring the availability of web resources is an urgent task [1, 2]. Recent statistics indicate an increase in denial-of-service and availability attacks on web resources. Thus, the class of DDoS attacks is at the top of the list of methods of cyber interference in the operation of web services. Denial-of-service attacks can have distributed sources of negative influence and a slow, time-delayed profile [2, 3]. This indicates that the attackers are trying to hide the signs of an attack until a certain point in time and disguise malicious traffic as normal [2, 4].

Modification of DDoS attacks on a web resource should not affect the ability of detection systems to recognize such malicious activity. To protect web resources, it is crucial to use an attack detection system with the appropriate settings of the detection mechanisms [5]. Early detection of signs of cyber attacks aimed at denying service to web resources in ITN is an important component of this protection.

The classic implementation of attack detection systems necessarily includes the use of signature analysis methods which determine the presence or absence of an attack by comparing traffic telemetry indicators with known signatures [6]. However, modern attack detection systems must also be able to operate effectively against new and modified attacks. Signature detection methods do not allow ensuring this.

An important factor in evaluating attack detection systems is the absence of false positives. False positives can lead to erroneous preventive actions, such as blocking traffic from certain users, increasing the response time of a web resource, or reducing the rating of a web resource, etc. Therefore, modern attack detection systems should be based on intelligent approaches that take into account the level of traffic abnormality and are able to quickly learn and adapt to new conditions. The implementation of such systems is currently possible on the basis of artificial intelligence methods [7, 8, 9, 10]. Nevertheless, the presence of data on a high level of traffic abnormality when determining the cyber influence may not always indicate the presence of an attack. For instance, a high level of abnormality may be observed without malicious actions of users, but be caused by a combination of random factors. Each web resource operates within a specific segment of the ITN and has its own individual features, which are determined by the stack of network protocols utilized, characteristics of the traffic (average request intensity, rate of change in intensity, etc.), regional features, time of day, etc. These factors can influence the overall traffic profile of a given segment and can be used to analyze its abnormality. Therefore, it is crucial to correctly configure the parameters of the attack detection system, taking into account the specified conditions of the web resource within a particular ITN. The data obtained in this way about the level of traffic abnormality can be utilized to further decide on the presence of an attack. The utilization of this indicator in the subsequent stages of detecting modified denial-of-service attacks will allow for the necessary threat analysis to be conducted in time, thus enabling the implementation of preventive measures.

An important factor in evaluating attack detection systems is the absence of false positives. False positives can lead to erroneous preventive actions, such as blocking traffic from certain users, increasing the response time of a web resource, or reducing the rating of a web resource, etc. Therefore, modern attack detection systems should be based on intelligent approaches that take into account the level of traffic abnormality and are able

to quickly learn and adapt to new conditions. The implementation of such systems is currently possible on the basis of artificial intelligence methods [7, 8, 9, 10]. Nevertheless, the presence of data on a high level of traffic abnormality when determining the cyber influence may not always indicate the presence of an attack. For instance, a high level of abnormality may be observed without malicious actions of users, but be caused by a combination of random factors. Each web resource operates within a specific segment of the ITN and has its own individual features, which are determined by the stack of network protocols utilized, characteristics of the traffic (average request intensity, rate of change in intensity, etc.), regional features, time of day, etc. These factors can influence the overall traffic profile of a given segment and can be used to analyze its abnormality. Therefore, it is crucial to correctly configure the parameters of the attack detection system, taking into account the specified conditions of the web resource within a particular ITN. The data obtained in this way about the level of traffic abnormality can be utilized to further decide on the presence of an attack. The utilization of this indicator in the subsequent stages of detecting modified denial-of-service attacks will allow for the necessary threat analysis to be conducted in time, thus enabling the implementation of preventive measures.

2. Problem formulation

In modern ITN, ensuring the availability of web services is one of the priority tasks. Systems for detecting attacks on the availability of web resources should also include signature methods that need to be updated when new attacks are detected. Nevertheless, the utilization of signature-based systems alone is insufficient for the detection of new and even slightly modified DDoS attacks prior to the update of signatures.

The implementation of new approaches based on intelligent traffic abnormality detection systems necessitates the consideration of various factors, with the possibility of periodic retraining of such systems. It should be borne in mind that a high level of abnormality does not always indicate an attack [11]. In this case, blocking the hosts from which traffic with signs of abnormality is coming may result in a loss of trust in the web resource, an increase in response time to user requests, and, as a consequence, a decrease in the ratings of the web service in the future. Therefore, existing approaches for detecting modified distributed denial-of-service attacks need to be improved.

One of the priority ways for this is the development and multi-stage application of intelligent systems based on fuzzy inference systems. Such systems can be used both for the analysis of anomalies based on traffic telemetry, and in the subsequent stages of attack detection (classification) using the behavioral characteristics of the web resource (for example, changes in the load level of the host's resources, changes in the number of return requests, and others). One of the most effective methods for achieving this objective is to develop and implement intelligent systems based on fuzzy inference systems in a multi-stage process [12]. Such systems can be used for both the analysis of abnormalities based on traffic telemetry and the subsequent detection (classification) of attacks using the behavioral characteristics of a web resource (changes in the level of host resource utilization, changes in the number of return requests, etc.) [10, 13, 14].

It is assumed that the application of intelligent systems will facilitate the early detection of modified attacks and significantly improve the availability of web resources in ITN in conditions of modified cyber attacks of the DDoS class [3].

3. Related works

The application of artificial intelligence methods to classify new or modified attacks is a promising area [15, 16]. For example, the use of the mathematical apparatus of fuzzy sets and neural networks to detect cyber influences is currently being studied in the work [11]. The authors of [17, 18, 19] developed the FIS, which classifies attacks based on a set of incoming traffic parameters.

However, the approach described in the reviewed literature does not take into account the peculiarities of new types of attacks. These features may be of a different nature related to the characteristics of a particular ITN, host features, and may not fall under anomalous data. A high level of traffic abnormality may not always indicate the presence of an attack. So, in most cases, with data on high traffic abnormality, it is not possible to accurately determine the presence of an attack until the moment it is completed and the relevant signs of damage to the web resource are obtained. In such cases, the preventive measures taken by a security expert may have negative consequences. Therefore, when determining the class of attack, it is necessary to use advanced approaches based on multi-stage analysis. The determination of the level of traffic abnormality in [11] can be based on data on traffic characteristics, taking into account the IP addresses of senders and receivers, ports of senders and receivers, the packets belonging to a specific protocol, the presence of certain flags in the packet header, and the total number of incoming and outgoing packets. These characteristics are used to find the level of traffic abnormalities in the ITN [11]. The coefficient of abnormality, which is determined in this case, can take values in the range $K=\{0;1\}$. At the second stage, the attack class can be determined based on signature and intelligent methods. For this purpose, the obtained data on the level of traffic abnormalities and behavioral information of the host are used. Data on the behavioral characteristics of a host, such as operating system load level, number of external network connections, and other characteristics, can be used for signature analysis. However, signature analysis systems can detect an attack only if the measured characteristics exactly match an existing pattern (signature). Even a slight modification of the attack makes the use of signature-based methods ineffective. To detect modified attacks, intelligent systems based on fuzzy logic can be used [1, 19, 20, 21, 22, 23]. This will make it possible to detect existing attacks based on pre-trained fuzzy inference systems even in the presence of minor changes (modifications) [19, 22, 24, 25, 26, 27]. Such systems, in general, have the appearance shown in Figure 1 [25].

In such systems, value of the output variable K is determined based on the fuzzy inference procedure based on values of the input variables $z_1, z_2, z_3, \ldots, z_n$.

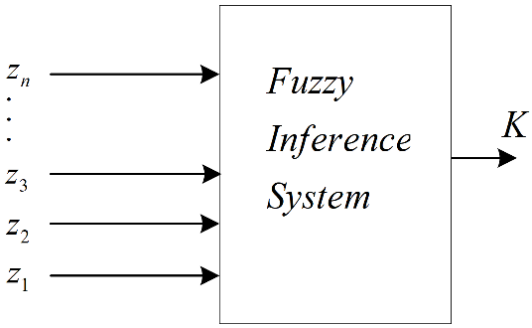

Figure 1: General FIS structure

The use of such systems for the classification of injection-type attacks is proposed in [28]. To do this, values of the behavioral characteristics of a host obtained during the operation of the ITN are fed to the FIS as input parameters. However, fuzzy inference systems require periodic retraining. This mentioned approach [28] lacks mechanisms for fast FIS training. It is possible to automate the learning process by combining the mathematical apparatus of fuzzy logic and neural networks [11].

In the reviewed sources [11, 29], ANFIS was used to find various parameters of information systems and showed its high efficiency in solving this problem. Therefore, this paper proposes to use a system of this type to determine the presence of DDoS attacks at several stages of intelligent analysis. It is anticipated that obtained in this way early information about a potential DDoS attack will allow the implementation of preventive measures to mitigate its impact and ensure the availability of the web resource in conditions of cyber influence.

4. Determination the level of network traffic abnormality on a web resource

Based on the analysis, it is proposed to improve the proposed approaches to detection of denial-of-service attacks by implementing several stages of applying fuzzy inference systems. At the first stage, it is proposed to use an adaptive fuzzy neural system to determine the level of traffic abnormalities, taking into account characteristics of the traffic associated with a given ITN [11, 24].

At the next stage, it is proposed to carry out measures to classify attacks based on signature and intelligent analysis methods, taking into account the behavioral characteristics of the host [6]. Since traffic with different characteristics can differently affect the characteristics of the host on which the web resource is deployed, it is important to take into account the behavioral characteristics of the host caused by the arrival of traffic with different parameters. At the next stage, it is proposed that measures be taken to classify attacks based on signature and intelligent analysis methods, taking into account the behavioral characteristics of the host. Since traffic with different characteristics can differently affect the characteristics of the host on which the web resource is deployed, it is crucial to take into account the behavioral characteristics of the host resulting from the arrival of traffic with different parameters.

The process of studying a system can be represented as a sequence of discrete time intervals of constant duration t_i. During these intervals, the main characteristics of traffic and behavioral characteristics of the host are measured.

In general, such a mechanism for detecting a modified attack should include elements for:

- Obtaining and summarizing information about the characteristics of the traffic coming to a web resource;
- Determining the level of traffic anomalies;
- Comparing of key traffic characteristics with signature characteristics;
- Determining the key behavioral characteristics of the host;
- Making a decision about the existence of an attack.

Figure 2 shows the block diagram of the system used to detect modified DDoS attacks, based on the approach described above. The diagram involves several stages.

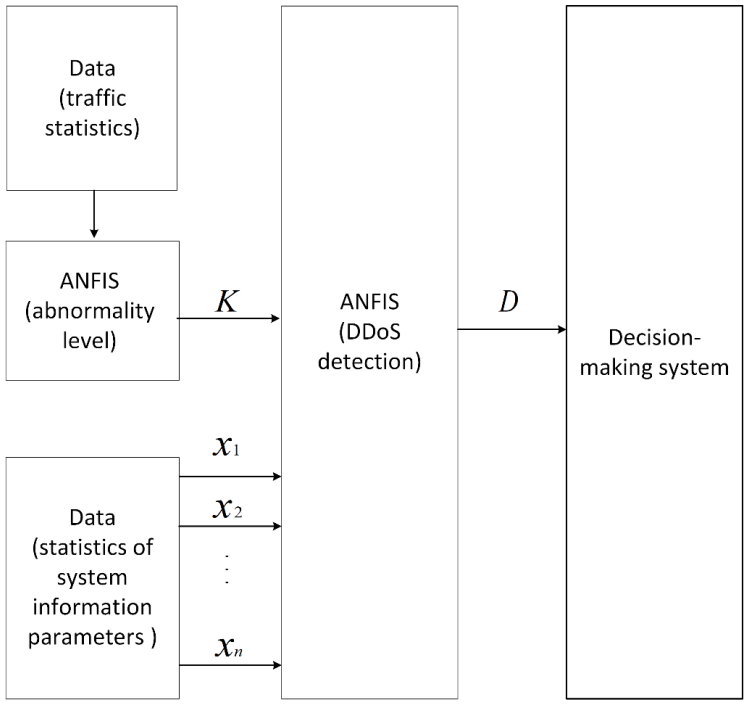

Figure 2: Structural diagram of the DDoS attack detection system

The use of ANFIS to determine the level of abnormality results in finding a functional dependence [11] in the form:

$$K = f(z_1, z_2, ..., z_n). \quad (1)$$

The internal structure of ANFIS is determined based on the chosen fuzzy inference algorithm, the number of input variables and membership functions of each input variable [11]. During the synthesis of ANFIS, it is proposed to use the first-order Sugeno algorithm

and three input variables with two membership functions each to determine the level of abnormality. In this case, the structure of this system will have the form shown in Figure 3.

It is proposed to use the following input values: z_1 is the number of incoming packets during the observation interval t_i, z_2 is the number of outgoing packets during the observation interval t_i, and z_3 is the rate of change of Moving Average of total packet number during the specified observation period.

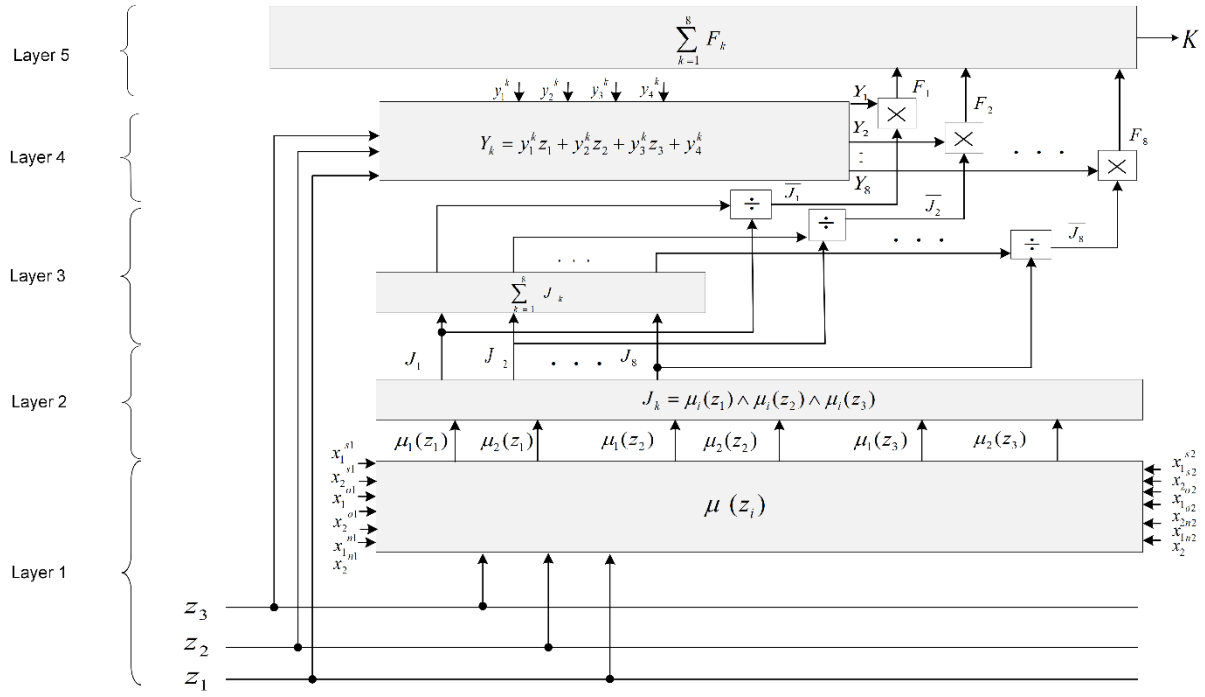

Figure 3: ANFIS structure used to determine the level of traffic abnormality

Finding the correct output value for ANFIS depends on the accuracy of its training, which is based on statistics obtained from traffic telemetry and observation data on the behavioral characteristics of the host on which the web resource is deployed. One of the most common training methods is a hybrid approach that combines gradient descent and inverse error propagation method [30]. To generate training data, it is necessary to observe the input variable values to obtain the desired output variable values. The training data and neural weight settings of the proposed ANFIS for determining the level of anomaly should be formed on the basis of traffic telemetry data in the ITN traffic segment. The training matrix developed for this purpose has the following form:

$$\begin{bmatrix} z^i{}_1 & z^i{}_2 & z^i{}_3 & K^i \\ z^{i-1}{}_1 & z^{i-1}{}_2 & z^{i-1}{}_3 & K^{i-1} \\ z^{i-2}{}_1 & z^{i-2}{}_2 & z^{i-2}{}_3 & K^{i-2} \\ & & & .... \\ z^{i-n}{}_1 & z^{i-n}{}_2 & z^{i-n}{}_3 & K^{i-n} \end{bmatrix} \quad (2)$$

The matrix (2) was filled using data obtained from traffic telemetry in Information and Telecommunication Network segment, as well as a series of traffic generation experiments. The value of the input variable z_3 was calculated for each *i*-th time interval using formula:

$$z^i{}_3 = \frac{1}{\Delta t_{i-k}} \left(\sum_{j=i-n}^{i} \frac{z^j{}_1 + z^j{}_2}{n} - \sum_{l=k-n}^{k} \frac{z^l{}_1 + z^l{}_2}{n} \right) \quad (3)$$

At the next stage, ANFIS will also be used to detect modified DDoS attacks. This approach will facilitate the development of a method for detecting modified DDoS attacks on a web resource.

5. Method for the detection of modified DDoS attacks based on the use of ANFIS

This paper proposes a method for detecting modified cyber attacks based on the use of the mechanism for intelligent analysis of traffic telemetry data and the obtained data on the level of abnormality. The method involves the following steps:

1. Accumulate and structure statistical data on traffic characteristics in a defined segment of ITN.
2. Synthesize the ANFIS architecture and its implementation on the ITN web resource to determine the level of traffic abnormality.
3. Set up the ANFIS parameters by training based on traffic telemetry statistics in the ITN, which has been collected over previous time intervals for the specified abnormality levels.
4. Determine the level of traffic abnormality in the ITN segment using ANFIS.
5. Check the main characteristics of traffic with signature databases.
6. Accumulate and structure data on the behavioral characteristics of the host on which the web resource is located.
7. Synthesize ANFIS to detect modified DDoS attacks, taking into account traffic abnormalities and the behavioral characteristics of the web resource.
8. Conduct fuzzy inference based on ANFIS to detect a modified DDoS attack.
9. Make a decision on the presence of a DDoS attack on a web resource.

To implement all the stages of the proposed method, it is necessary to develop (synthesize) ANFIS for detecting modified attacks. For this purpose, we will also use the method defined in [11].

The result of fuzzy inference based on the use of this ANFIS is finding a functional dependence of the form (4) to determine the presence of a modified attack:

$$D = f(K, x_2, ..., x_n). \quad (4)$$

As input values, we use the value of the abnormality coefficient *K* obtained at the previous step for the *(i-1)* time interval. For the current time interval, the behavioral

characteristics of the host, on which the web resource is hosted, are calculated: $x_1 = K$, x_2, x_3,..., x_n. The output value of such a system is an indicator of the presence of a modified DDoS attack.

In order to obtain a sufficient level of data accuracy when finding dependence (4), it is suggested to use the 1st order Sugeno algorithm. The number of input values is three: *K*, which represents the traffic abnormality coefficient, x_1, which represents the host load level during the current time interval and which is determined by formula (5), and x_2, which represents the rate of change of the average moving level of the host load during the specified observation period Δt_{i-k} and will be determined by the formula (6):

$$x^i{}_1 = \frac{1}{m}\left(\sum_{j=1}^{T}\frac{n_j}{100}\right), \tag{5}$$

$$x^i{}_2 = \frac{1}{\Delta t_{i-k}}\left(\sum_{j=i-n}^{i}\frac{x^j{}_1}{n} - \sum_{l=k-n}^{k}\frac{x^l{}_1}{n}\right). \tag{6}$$

For each input value, it is sufficient to define two triangular membership functions corresponding to fuzzy sets, designated as "small value" and "large value," as shown in Figure 4.

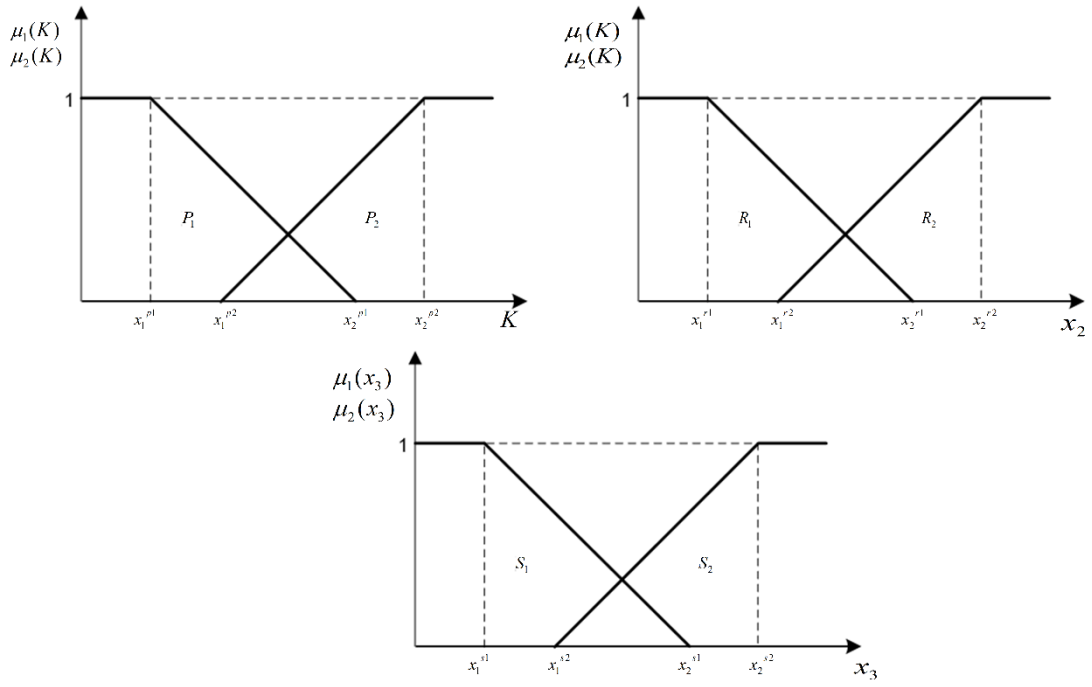

Figure 4: Membership functions for ANFIS input values

Then the proposed ANFIS will have the following structure (Figure 5):

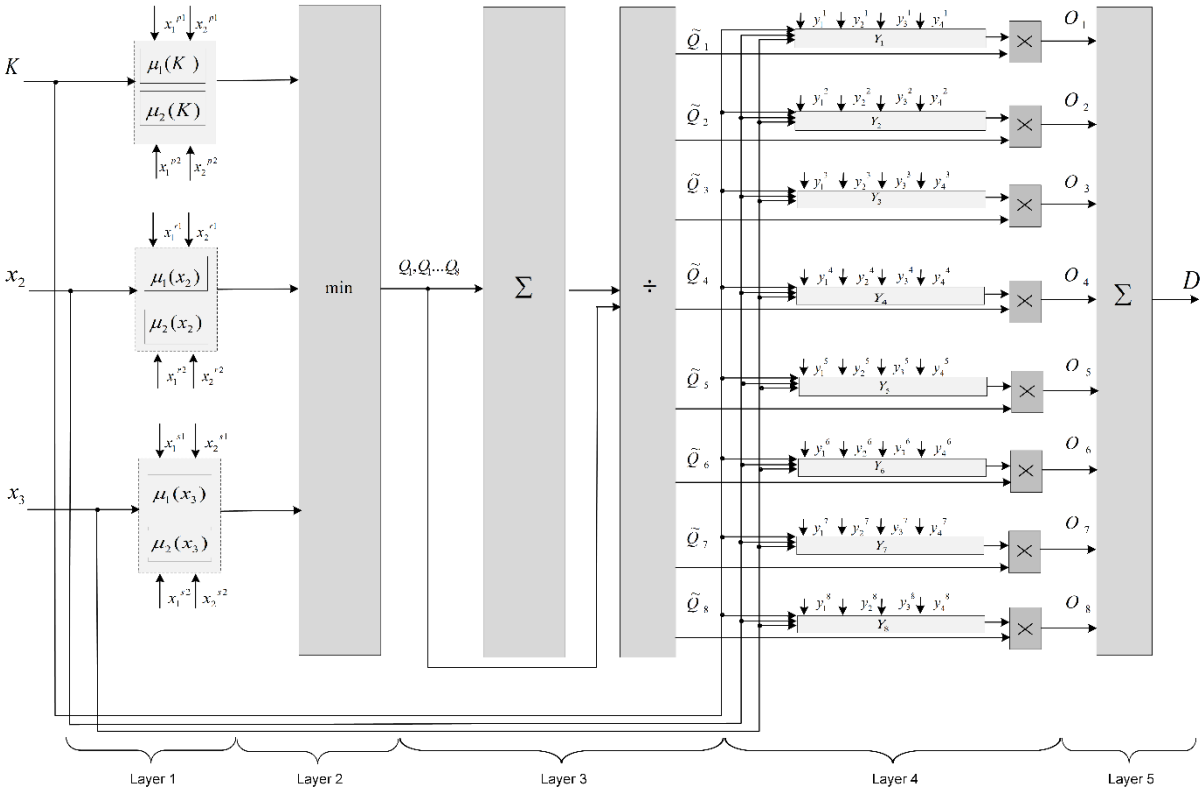

Figure 5: ANFIS structure for determining the presence of a DDoS attack on a web resource

The shown ANFIS structure involves five layers. Each of the presented layers is required for the fuzzy inference procedure to find an indicator of the presence of a modified DDoS attack. The formed knowledge base of such ANFIS will contain 8 rules of the following form (7)-(14):

$$If\ (K=P_1)\ and\ (x_2=R_1)\ and\ (x_3=S_1)\ then\ (D=Y_1), \quad (7)$$

$$If\ (K=P_1)\ and\ (x_2=R_1)\ and\ (x_3=S_2)\ then\ (D=Y_2), \quad (8)$$

$$If\ (K=P_1)\ and\ (x_2=R_2)\ and\ (x_3=S_1)\ then\ (D=Y_3), \quad (9)$$

$$If\ (K=P_1)\ and\ (x_2=R_2)\ and\ (x_3=S_2)\ then\ (D=Y_4), \quad (10)$$

$$If\ (K=P_2)\ and\ (x_2=R_1)\ and\ (x_3=S_2)\ then\ (D=Y_5), \quad (11)$$

$$If\ (K=P_2)\ and\ (x_2=R_1)\ and\ (x_3=S_1)\ then\ (D=Y_6), \quad (12)$$

$$If\ (K=P_2)\ and\ (x_2=R_2)\ and\ (x_3=S_1)\ then\ (D=Y_7), \quad (13)$$

$$If\ (K=P_2)\ and\ (x_2=R_2)\ and\ (x_3=S_2)\ then\ (D=Y_8), \quad (14)$$

where P_1 is the "small value" term of the input value K; P_2 is the "large value" term of the input value K; R_1 is the "small value" term of the input value x_2; R_2 is the "large

value" term of the input value x_2; S_1 is the "small value" term of the input value x_3; S_2 is the "large value" term of the input value x_3; $Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7, Y_8$ are the values of the individual output of the fuzzy rule number k, where $k = 1,2...8$.

The outcome of ANFIS training is the obtained expression for the membership functions of the input variables:

$$\mu_1(K) = \begin{cases} 1, & K < {x_1}^{p1}; \\ \dfrac{{x_2}^{p1} - K}{{x_2}^{p1} - {x_1}^{p1}}, & {x_1}^{p1} \le K < {x_2}^{p1}; \\ 0, & K \ge {x_2}^{p1}; \end{cases} \quad (15)$$

$$\mu_2(K) = \begin{cases} 0, & K < {x_1}^{p2}; \\ \dfrac{K - {x_1}^{p2}}{{x_2}^{p2} - {x_1}^{p2}}, & {x_1}^{p2} \le K < {x_2}^{p2}; \\ 1, & K \ge {x_2}^{p2}; \end{cases} \quad (16)$$

$$\mu_1(x_2) = \begin{cases} 1, & x_2 < {x_1}^{p1}; \\ \dfrac{{x_2}^{p1} - x_2}{{x_2}^{p1} - {x_1}^{p1}}, & {x_1}^{p1} \le x_2 < {x_2}^{p1}; \\ 0, & x_2 \ge {x_2}^{p1}; \end{cases} \quad (17)$$

$$\mu_2(x_2) = \begin{cases} 0, & x_2 < {x_1}^{p2}; \\ \dfrac{x_2 - {x_1}^{p2}}{{x_2}^{p2} - {x_1}^{p2}}, & {x_1}^{p2} \le x_2 < {x_2}^{p2}; \\ 1, & x_2 \ge {x_2}^{p2}; \end{cases} \quad (18)$$

$$\mu_1(x_3) = \begin{cases} 1, & x_3 < {x_1}^{p1}; \\ \dfrac{{x_2}^{p1} - x_3}{{x_2}^{p1} - {x_1}^{p1}}, & {x_1}^{p1} \le x_3 < {x_2}^{p1}; \\ 0, & x_3 \ge {x_2}^{p1}; \end{cases} \quad (19)$$

$$\mu_2(x_3) = \begin{cases} 0, & x_3 < {x_1}^{p2}; \\ \dfrac{x_3 - {x_1}^{p2}}{{x_2}^{p2} - {x_1}^{p2}}, & {x_1}^{p2} \le x_3 < {x_2}^{p2}; \\ 1, & x_3 \ge {x_2}^{p2}; \end{cases} \quad (20)$$

The training matrix, which was formed for this purpose, has the following form (21):

$$\begin{bmatrix} K^i & x^i{}_2 & x^i{}_3 & D^i \\ K^{i-1} & x^{i-1}{}_2 & x^{i-1}{}_3 & D^{i-1} \\ K^{i-2}{}_1 & x^{i-2}{}_2 & x^{i-2}{}_3 & D^{i-2} \\ & & & .... \\ K^{i-n}{}_1 & x^{i-n}{}_2 & x^{i-n}{}_3 & D^{i-n} \end{bmatrix} \quad (21)$$

Data sets on the value of input variable and the expected value of the output variable were recorded for the $i = 1..n$ time intervals of observation. The result of ANFIS training is the adjustment of weights of the first layer neurons based on the obtained values of the coefficients $x_1{}^{p1}$, $x_2{}^{p1}$, $x_2{}^{p2}$, $x_2{}^{p1}$, $x_1{}^{r1}$, $x_2{}^{r1}$, $x_1{}^{r2}$, $x_2{}^{r2}$, $x_1{}^{s1}$, $x_2{}^{s1}$, $x_1{}^{s2}$, $x_2{}^{s2}$ and the adjustment of weights of the fourth layer neurons based on the obtained values of the coefficients $y_1{}^k$, $y_2{}^k$, $y_3{}^k$, $y_4{}^k$ for $k = 1..8$. Based on the obtained values of the coefficients, the values of the individual outputs of the fuzzy rule number k ($k = \overline{1,8}$) are determined according to the 1st-order Sugeno fuzzy inference algorithm using the expression:

$$Y_k = y_1^k K + y_2^k x_2 + y_3^k x_3 + y_4^k \quad (22)$$

The general procedure for using ANFIS to detect modified attacks is described below.

The first layer of ANFIS according to expressions (15)-(20) performs fuzzification of the values of the input variables K, x_2, and x_3 to find the values of the membership functions of these variables.

The second layer of ANFIS performs aggregation based on expressions (23)-(30):

$$Q_1 = \mu_1(K) \wedge \mu_1(x_2) \wedge \mu_1(x_3) \quad (23)$$
$$Q_2 = \mu_1(K) \wedge \mu_1(x_2) \wedge \mu_2(x_3) \quad (24)$$
$$Q_3 = \mu_1(K) \wedge \mu_2(x_2) \wedge \mu_1(x_3) \quad (25)$$
$$Q_4 = \mu_2(K) \wedge \mu_1(x_2) \wedge \mu_1(x_3) \quad (26)$$
$$Q_5 = \mu_1(K) \wedge \mu_2(x_2) \wedge \mu_2(x_3) \quad (27)$$
$$Q_6 = \mu_2(K) \wedge \mu_2(x_2) \wedge \mu_1(x_3) \quad (28)$$
$$Q_7 = \mu_2(K) \wedge \mu_1(x_2) \wedge \mu_2(x_3) \quad (29)$$
$$Q_8 = \mu_2(K) \wedge \mu_2(x_2) \wedge \mu_2(x_3) \quad (30)$$

The result of aggregation is then fed to the input of the third layer of neurons, where it is normalized for $k = \overline{1,8}$.

$$\widetilde{Q}_k = \frac{Q_k}{\sum_{k=1}^{8} Q_k}. \quad (31)$$

The result of normalization is fed to the input of the fourth layer of neurons. In this layer, the activation procedure is performed to determine the individual outputs of each fuzzy rule by formula (22). Then, the neurons of this layer calculate the product of the results of activation and normalization for $k = \overline{1,8}$ according the formula:

$$O_k = \widetilde{Q}_k Y_k. \tag{32}$$

The results of the operation of the fourth layer of ANFIS, determined by formula (30), are fed to the input of the fifth layer of neurons, where defuzzification is performed to find the value of the ouput value D. For this pirpose, the sum of the results of the operation of the fourth layer of neurons is calculated according to the formula:

$$D = \sum_{k=1}^{8} O_k \tag{33}$$

The outcome of the fifth layer of ANFIS is finding of a precise value of the desired output variable, which serves as an indicator of a modified DDoS attack.

The data collection for the formation of training matrices (2) and (21) can be carried out by telemetry of traffic in the ITN segment and observation of the behavioral characteristics of the host. Such observations are carried out in a normal state of operation of a particular ITN and in an abnormal state. An abnormal state of operation can be ensured by creating artificial abnormal events similar to a DDoS attack or by observing a real (confirmed) modified DDoS attack. To create artificial abnormal events, artificial traffic generators are used from sources distributed throughout the network with an abnormal number of requests (packets) directed to a web resource. It is also possible to use accumulated traffic telemetry data with confirmation of a DDoS attack as training data. Traffic telemetry data from DDoS attacks is also stored in publicly available databases, such as KDD99, and can also be used to obtain training samples [18]. Values of the input parameters calculated on the basis of traffic telemetry data according to formulas (3) and (6), namely the values of the speed of change of the moving average of the total number of packets on the web resource and the level of host load, are used to form matrices of the form (2) and (21). The data obtained under these conditions is divided into two parts: training and test. The data from the first set of matrices is fed to the input of neuro-fuzzy systems for training. A hybrid method based on a combination of the back-propagation method and gradient descent was selected as the training algorithm.

Table 1 presents a list of coefficients obtained as a result of training neurons of the fourth layer based on the observation of the behavioral characteristics of a host with a web resource when creating artificial abnormal events in the ITN segment by generating atypical traffic from various network nodes.

Data from the second set of matrices (2) and (21) are used for testing after the training. The result of successful training of ANFIS to detect a modified DDoS attack is the correct determination of the values of the output variable D when using the test data set. The number of training cycles is determined by estimating the permissible error in a series of studies. As a testing environment for the presented ANFIS, it is proposed to use the Matlab simulation environment [30].

Table 1
The coefficients of forth neuron layer

Rule number, k	The coefficients			
	y_1^k	y_2^k	y_3^k	y_4^k
1	y_1^1	y_2^1	y_3^1	y_4^1
2	y_1^2	y_2^2	y_3^2	y_4^2
3	y_1^3	y_2^3	y_3^3	y_4^3
4	y_1^4	y_2^4	y_3^4	y_4^4
5	y_1^5	y_2^5	y_3^5	y_4^5
6	y_1^6	y_2^6	y_3^6	y_4^6
7	y_1^7	y_2^7	y_3^7	y_4^7
8	y_1^8	y_2^8	y_3^8	y_4^8

After training, the data from the second test part is fed to the ANFIS input, and the output value is compared with the expected result. The permissible error is estimated in order to determine the frequency of ANFIS retraining. It is proposed to retrain the ANFIS if the number of matches is reduced to 98%.

6. Conclusion

The paper presents an approach for detecting modified DDoS attacks in ITM based on the use of ANFIS. It is demonstrated that such an approach is a promising ways to detect abnormalities in ITN. Neuro-fuzzy systems allow for the automation of the parameter settings for fuzzy inference systems, the adaptation of these settings during operation, and the automation of the process of developing rules for the knowledge base. The main stages of the method for solving the problem of a modified DDoS attack detection in Information and Telecommunication Networks are considered. It is shown that in addition to traffic telemetry data, it is necessary to take into account the behavioral characteristics of the host on which the web resource is deployed. Therefore, a feature of the synthesized neuro-fuzzy attack detection system is the consideration and using of the traffic abnormality coefficient, the level of host load, and the rate of change of the moving average of this value as input variables. ANFIS allow obtaining the value of the network traffic abnormality indicator, which provides a multi-stage attack detection procedure. We synthesize ANFIS to detect modified DDoS attacks. Algorithms for training this system on test data were selected and its effectiveness was investigated. The proposed method for detecting of modified DDoS attacks will allow security administrators to receive early warning information about modified threats in order to take the necessary measures to ensure the availability of web resources.

Further research should focus on generating statistics to effectively train the neuro-fuzzy system and conducting research with a different set of input parameters to detect modified DDoS attacks in various segments of the ITN.

References

[1] L. Decker, D. Leite, L. Giommi, and D. Bonacorsi, Real-time anomaly detection in data centers for log-based predictive maintenance using an evolving fuzzy-rule-based approach, in: International Conference on Fuzzy Systems (FUZZ-IEEE), IEEE, Glasgow, United Kingdom, 2020, pp. 1–8. doi:10.1109/FUZZ48607.2020.9177762.

[2] M. Roopak, S. Parkinson, G. Y. Tian, Y. Ran, S. Khan, and B. Chandrasekaran, An Unsupervised Approach for the Detection of Zero-Day DDoS Attacks in IoT Networks, IET Research Journals (2024) 1–9. doi:10.22541/au.170526630.07302484/v1.

[3] A. A. Alashhab, M. S. M. Zahid, M. Abdullahi, and M. S. Rahman, Real-time Detection of Low-Rate DDoS Attacks in SDN-based Networks using Online Machine Learning Model, in: 7th Cyber Security in Networking Conference (CSNet), IEEE, Montreal, QC, Canada, 2023, pp. 95–101. doi:10.1109/CSNet59123.2023.10339791.

[4] K. Sornalakshmi, Detection of DoS attack and zero day threat with SIEM, in: International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, Madurai, India, 2017, pp. 1–7. doi:10.1109/ICCONS.2017.8250515.

[5] S. Onyshchenko, A. Yanko, A. Hlushko, O. Maslii, A. Cherviak, Cybersecurity and improvement of the information security system, Journal of the Balkan Tribological Association 29, 5 (2023) 818–835.

[6] S. Onyshchenko, A. Yanko, A. Hlushko, O. Maslii, V. Skryl, The mechanism of information security of the national economy in cyberspace, in: V. Onyshchenko, G. Mammadova, S. Sivitska, A. Gasimov (Eds.), Proceedings of the 4th International Conference on Building Innovations, ICBI 2022, volume 299 of Lecture Notes in Civil Engineering, Springer, Cham, 2023, pp. 791–803. URL: https://doi.org/10.1007/978-3-031-17385-1_67.

[7] Q. Li, L. Meng, Y. Zhang, J. Yan, DDoS Attacks Detection Using Machine Learning Algorithms, in: Proceedings of the 15th International Forum on Digital TV and Wireless Multimedia Communications, IFTC 2018, volume 1009 of Communications in Computer and Information Science, Springer, Singapore, 2019, pp. 205–216. URL: https://doi.org/10.1007/978-981-13-8138-6_17.

[8] P. V. Campos Souza, A. J. Guimarães, T. S. Rezende, V. J. Araujo, V. S. Araujo, Detection of Anomalies in Large-Scale Cyberattacks Using Fuzzy Neural Networks, AI 1, 1 (2020) 92–116. doi:10.3390/ai1010005.

[9] M. Almseidin, J. Al Sawwa, M. Alkasassbeh, Anomaly-based Intrusion Detection System Using Fuzzy Logic, in: International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 290–295. doi:10.1109/ICIT52682.2021.9491742.

[10] D. Javaheri, P. Lalbakhsh, M. Hosseinzadeh, A Novel Method for Detecting Future Generations of Targeted and Metamorphic Malware Based on Genetic Algorithm, IEEE Access 9 (2021) 69951–69970. doi:10.1109/ACCESS.2021.3077295.

[11] Y. Zdorenko, V. Fesoha, Neuro-fuzzy system of intrusions detection in information and telecommunication network, Collection of scientific works of VITI 3 (2018) 31–37.

[12] S. Velliangiri and H. M. Pandey, Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms, Future Generation Computer Systems 110 (2020) 80–90. doi:10.1016/j.future.2020.03.049.

[13] M. Masdari and H. Khezri, A survey and taxonomy of the fuzzy signature-based intrusion detection systems, Applied Soft Computing 92, 106301 (2020). doi:10.1016/j.asoc.2020.106301.

[14] D. Kwon, H. Kim, J. Kim, S. Suh, I. Kim, K. Kim, A survey of deep learning-based network anomaly detection, Cluster Computing 22, 5 (2019). doi:22. 10.1007/s10586-017-1117-8.
[15] A. Banitalebi Dehkordi, M. Soltan Aghaei, F. Zamani Boroujeni, A Hybrid Mechanism to Detect DDoS Attacks in Software Defined Networks, Majlesi Journal of Electrical Engineering 15, 1 (2021) 1–8. doi:10.52547/mjee.15.1.1.
[16] P. A. R. Kumar, S. Selvakumar, Distributed denial of service attack detection using an ensemble of neural classifier, Computer Communications, 34, 11 (2011) 1328–1341. URL: https://doi.org/10.1016/j.comcom.2011.01.012.
[17] S. Ahmed, S. M. Nirkhi, A Fuzzy approach for forensic analysis of DDoS attack in manet, International Journal of Advanced Computer Science and Applications 4, 6 (2013) 193–198. doi:10.14569/IJACSA.2013.040626.
[18] O. Yavanoglu, M. Aydos, A review on cyber security datasets for machine learning algorithms, in: International Conference on Big Data (Big Data), IEEE, Boston, MA, USA, 2017, pp. 2186–2193. doi:10.1109/BigData.2017.8258167.
[19] C. Balarengadurai, S. Saraswathi, Fuzzy Based Detection and Prediction of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network, International Journal of Trust Management in Computing and Communications 1, 3–4 (2013) 243–260. doi:10.1504/IJTMCC.2013.056424.
[20] P. Pajila, E. G. Julie, Y. H. Robinson, FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks, Wireless Personal Communications 122, 4 (2022) 3053–3083. URL: https://doi.org/10.21203/rs.3.rs-217674/v1.
[21] N. N. Iyengar, A. Banerjee, G. Ganapathy, A Fuzzy Logic Based Defense Mechanism against Distributed Denial of Services Attack in Cloud Environment, International Journal of Communication Networks and Information Security (IJCNIS) 6,3 (2022). URL: https://doi.org/10.17762/ijcnis.v6i3.864.
[22] A. Khare, J. Rana, R. Jain, R. Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology, International Journal of Computer Network and Information Security 9 (2017) 29–35. doi:10.5815/ijcnis.2017.07.04.
[23] L. A. Zadeh, Toward a theory of fuzzy information granulation and ITM centrality in human reasoning and fuzzy logic, Fuzzy sets and systems, 90, 2 (1997) 111–127. URL: https://doi.org/10.1016/S0165-0114(97)00077-8.
[24] D. Javaheri, S. Gorgin, J.-A. Lee, M. Masdari, Fuzzy Logic-Based DDoS Attacks and Network Traffic Anomaly Detection Methods: Classification, Overview, and Future Perspectives, Information Sciences 626 (2023) 315–338. doi:626. 10.1016/j.ins.2023.01.067.
[25] S. Velliangiri, H. M. Pandey, Fuzzy-Taylor elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms, Future Generation Computer Systems 110 (2020) 80–90. URL: https://doi.org/10.1016/j.future.2020.03.049.
[26] G. F. Scaranti, L. F. Carvalho, S. Barbon, M. L. Proença, Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-Defined Networks, IEEE Access 8 (2020) 100172–100184. doi:10.1109/ACCESS.2020.2997939.
[27] O. Rahman, M. A. G. Quraishi, C.-H. Lung, DDoS Attacks Detection and Mitigation in SDN Using Machine Learning, in: World Congress on Services (SERVICES), IEEE, Milan, Italy, 2019, pp. 184–189, doi:10.1109/SERVICES.2019.00051.

[28] I. Subach, Y. Zdorenko, V. Fesokha, Method for detecting cyber-attacks of the JS (HTML) / ScrInject type based on the use of the mathematical apparatus of the theory of fuzzy sets, Collection scientific works MITI 4 (2018) 125–131.
[29] Y. Zdorenko, O. Lavrut, T. Lavrut, Y. Nastishin, Method of Power Adaptation for Signals Emitted in a Wireless Network in Terms of Neuro-Fuzzy System, Wireless Personal Communications 115, 1 (2020) 597–609. URL: https://doi.org/10.1007/s11277-020-07588-5.
[30] S. N. Sivanandam, S. Sumathi, S. N. Deepa, Introduction to Fuzzy Logic using MATLAB, Springer Berlin, Heidelberg, 2007. URL: https://doi.org/10.1007/978-3-540-35781-0.