FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 32, N° 2, June 2019, pp. 249-265
https://doi.org/10.2298/FUEE1902249C

EWMA STATISTICS AND FUZZY LOGIC IN FUNCTION OF NETWORK ANOMALY DETECTION

Petar Čisar[1], Sanja Maravić Čisar[2]

[1]University of Criminal Investigation and Police Studies, Zemun-Belgrade, Serbia
[2]Subotica Tech, Deparment of Informatics, Subotica, Serbia

Abstract. *Anomaly detection is used to monitor and capture traffic anomalies in network systems. Many anomalies manifest in changes in the intensity of network events. Because of the ability of EWMA control chart to monitor the rate of occurrences of events based on their intensity, this statistic is appropriate for implementation in control limits based algorithms. The performance of standard EWMA algorithm can be made more effective combining the logic of adaptive threshold algorithm and adequate application of fuzzy theory. This paper analyzes the theoretical possibility of applying EWMA statistics and fuzzy logic to detect network anomalies. Different aspects of fuzzy rules are discussed as well as different membership functions, trying to find the most adequate choice. It is shown that the introduction of fuzzy logic in standard EWMA algorithm for anomaly detection opens the possibility of previous warning from a network attack. Besides, fuzzy logic enables precise determination of degree of the risk.*

Key words: *Network Anomaly Detection, EWMA, Fuzzy Rules, Membership Functions, Operators*

1. INTRODUCTION

Intrusion detection is an area of computer security that involves the detection of unwanted manipulations to computer networks. An intrusion detection system (IDS) is required to detect all types of malicious network traffic and computer usage that cannot be detected by a conventional firewall (Fig. 1).

This security method is needed in today's computing environment because it is impossible to keep pace with the current and potential threats and vulnerabilities in our computing systems. An IDS may be categorized by its detection mechanism on: anomaly - based, signature - based or hybrid (uses both of previous technologies).

Received October 4, 2018; received in revised form January 15, 2019
Corresponding author: Petar Čisar
University of Criminal Investigation and Police Studies, Cara Dušana 196, 11080 Zemun-Belgrade, Serbia
(e-mail: petar.cisar@gmail.com)

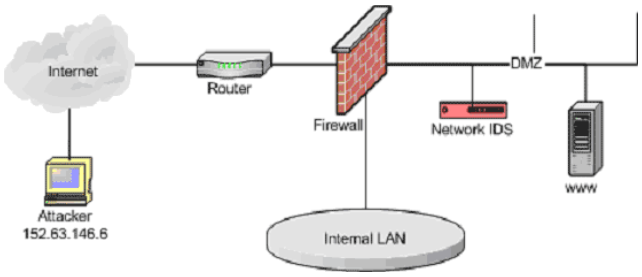

Fig. 1 IDS elementary configuration [1]

When the IDS identifies intrusions as unusual behaviour that differs from the normal behaviour of the monitored system, this analysis strategy is called anomaly detection [2]. The disadvantage of this method is the occurrence of a relatively large number of false alarms, i.e. network situations where the detection system indicates a non-existent attack. In order to reduce the appearance of false alarms, the measurement of the traffic activity is applied. The goal is to make a decision whether a network situation is attack or not. In order to make the correct decision, the behaviour profiles are defined: normal and abnormal profiles (simple thresholds (limit values) or complex statistical distributions). The false positive rate is considered one of the most important factors for performance evaluation of IDS.

Anomaly detection learns a statistical or neural network model to figure out what is normal. The following techniques can use: Bayesian statistics, neural networks, expert systems and statistical decision theory.

A number of anomalies are seen in changes in the intensity of events occurring in computer networks. Due to the ability of exponentially weighted moving average (EWMA) control chart to supervise the event-occurrence rate on the basis of their intensity, this statistic can be implemented in control limits based algorithms. The effectiveness of the performance of standard EWMA algorithm can be increased when one combines the logic of adaptive threshold algorithm and adequate application of fuzzy theory. Fuzzy logic enables precise adjustment of degree of exceeding limit values (expressed in form of percentage). Different aspects of fuzzy rules are described in this paper, including different membership functions, trying to define the most suitable choice. The aim of this paper is to show the theoretical opportunity and examine the possible way of implementing EWMA statistics and fuzzy logic to detect network anomalies.

EWMA statistics and fuzzy approach are not new in analyzing and detecting network anomalies and intrusions. Ye et al. [3] implemented Chi square distance metric to measure the deviation of the observed activities from the forecast of normal activities. The results indicate that the Chi square distance measure with the EWMA forecasting provides better performance in intrusion detection than that with the average-based forecasting method. Abdeh et al. [4] applied genetic fuzzy systems and showed that they are able to develop accurate and also interpretable intrusion detection systems. Yu et al. [5] developed a fuzzy model tuner, through which the user can tune the model fuzzily but yield much appropriate tuning. The results showed the system can achieve about 23% improvement. Works [6], [7] and [8] also point to the benefits of both approaches to improve the quality of transmission and predicting network anomalies. Senturk et al. in [9] combined popular control charts,

EWMA control chart for univariate data with fuzzy environment. The fuzzy EWMA control charts (FEWMA) can be used for detecting small shifts in the original data represented by fuzzy numbers (unlike this paper, in which fuzzy logic is applied in the decision-making phase based on the original network values). The FEWMA control charts decreases number of false decisions by providing flexibility on the control limits. Dickerson et al. [10] explored using fuzzy systems as the correlation engine for an IDS. Fuzzy systems have several important characteristics that suit intrusion detection: fuzzy systems can readily combine inputs from widely varying sources, many types of intrusions cannot be crisply defined, the degree of alarm that can occur with intrusions is often fuzzy. Researchers [11] developed the Fuzzy Intrusion Recognition Engine (FIRE) using fuzzy sets and fuzzy rules. FIRE uses simple data mining techniques to process the network input data and generate fuzzy sets for every observed feature. The fuzzy sets are then used to define fuzzy rules to detect individual attacks. FIRE does not establish any sort of model representing the current state of the system, but instead relies on attack specific rules for detection. Instead, FIRE creates and applies fuzzy logic rules to the audit data to classify it as normal or anomalous. The authors found that the approach is particularly effective against port scans and probes. The primary disadvantage of this approach is the labor intensive rule generation process. Control charts have characteristics that can be successfully applied in detection of network anomalies - to detect shifts. In addition to the EWMA control charts, a CUSUM (cumulative sum) algorithm can be also used for monitoring of change-points, whose behaviour in the case of distributed denial of service (DDoS) attacks is described in [31]. The authors in [32] implemented EWMA to detect anomalous changes in the intensity of a jamming attack event by using the packet inter-arrival feature of the received packets from the wireless sensor nodes.

This paper consists of six sections. The introduction offers a terminological basis for the problem of intrusion detection, then in the second section a short overview of anomaly detection techniques is presented. The EWMA algorithm is described in the third section, followed by the fourth section dealing with the fuzzy approach. The simulation and results of analyzed algorithm and its various aspects in an adequate software environment are given in the fifth section. The sixth part elaborates the process of improving the results. Finally, this paper closes with the conclusion based on the analyzed cases.

2. INTRUSION DETECTION

The main challenge in intrusion detection is that of separating anomalous events from normal events. Anomalous events can include actual attacks against a computer system or more subtle and hence difficult to detect, probes that are aimed at information reconnaissance. Another challenge in ID is that of false positives. False positives in ID occur when an IDS reports an intrusion as occurring when in fact it has not. It has been argued that it is actually this false alarm rate that is the limiting factor in an IDSs performance.

The performance of a network IDS can be more effective if it includes not only attack signature matching but also traffic analysis at the same time. By using traffic analysis, anomalous traffic is identified as a potential intrusion. Traffic analysis does not deal with the payload of a message, but its other characteristics such as source, destination, routing, length of the message, time it was sent, the frequency of the communication etc. [2]. Traffic payload is not always available for analysis – the traffic may be encrypted or it may simply be against policy to analyze packet payload [12].

Anomaly detection techniques [13]:

- Protocol anomaly detection – Protocol anomaly refers to all exceptions related to protocol format and protocol behaviour.
- Application payload anomaly – Application anomaly must be supported by detailed analysis of application protocols. Application anomaly also requires understanding of the application semantics in order to be effective.
- Statistical anomaly – To fully characterize the traffic behaviour in any network, various statistical measures are used to capture this behaviour. Additionally, the implemented statistical algorithm must recognize the difference between the long – term (assumed normal) and the short – term observations to avoid generating false alarms on normal traffic variations.

Network statistical anomaly detection (NSAD) attempts to dynamically understand the network and statistically identify traffic that deviates from normal traffic usage and patterns. NSAD systems can be broken down further into threshold, baseline and adaptive systems, with each looking for different triggers to identify anomalous behaviour [2].

3. EXPONENTIALLY WEIGHTED MOVING AVERAGE

Many intrusions manifest in changes in the intensity of events occurring in computer networks. Because of the ability of EWMA control charts to monitor the rate of occurrences of events based on their intensity, this technique is appropriate for implementation in control limits based algorithms. The performance of standard EWMA algorithm can be made more effective combining the concept of adaptive threshold algorithm and adequate application of fuzzy logic.

The following section containing the theoretical background has already been discussed in previous works [14], [15], [16] yet it is vital for the comprehension of the entire paper to summarize it again.

The exponentially weighted moving average is a statistic for monitoring the process that averages the data in a way that gives less and less weight to data as they are further removed in time. For the EWMA control technique, the decision regarding the state of control of the process depends on the EWMA statistics, which is an exponentially weighted average of all prior data, including the most recent measurements.

The statistics that is calculated is:

$$EWMA_t = \lambda Y_t + (1 - \lambda) EWMA_{t-1} \tag{1}$$

for t = 1, 2, ...n

where

- $EWMA_0$ is the mean of historical data
- Y_t is the observation at time t
- n is the number of observations to be monitored including $EWMA_0$
- $0 < \lambda \leq 1$ is a constant that determines the depth of memory of the EWMA.

This equation is formulated by Roberts [17]. By the choice of weighting factor λ, the EWMA control procedure can be made sensitive to a small or gradual drift in the process. The parameter λ determines the rate at which "older" data enter into the calculation of the EWMA statistic. A value of $\lambda = 1$ implies that only the most recent measurement influences the EWMA. Thus, a large value of $\lambda = 1$ gives more weight to recent data and less weight to

older data - a small value of λ gives more weight to older data [18]. The value of λ is usually set between 0.2 and 0.3 [19] although this choice is somewhat arbitrary. Lucas and Saccucci [20] have shown that although the smoothing factor λ used in an EWMA chart is usually recommended to be in the interval between 0.05 to 0.25, in practice the optimally designed smoothing factor depends not only on the given size of the mean shift δ, but also on a given in-control Average Run Length (ARL). ARL represents the average number of determined process points before the first point indices the appearance of out-of-control state (exceeding one of the control limits).

The estimated variance of the EWMA statistics is approximately:

$$\sigma_{EWMA}^2 = \frac{\lambda}{2-\lambda}\sigma^2 \tag{2}$$

when *t* is not small, where σ is the standard deviation calculated from the historical data.

The center line for the control chart is the target value or $EWMA_0$. The upper and lower control limits are [21]:

$$UCL = EWMA_0 + k\sigma_{EWMA} \tag{3}$$

$$LCL = EWMA_o - k\sigma_{EWMA} \tag{4}$$

where the factor *k* is either set equal 3 (the 3-sigma control limits) or chosen using the Lucas and Saccucci tables [20].

EWMA control chart is especially efficient in detecting small shifts of the monitored process – less than 1.5σ.

Control charts are specialized time series plots, which assist in determining whether a process is in statistical control. Some of the most widely used forms of control charts are X-R charts and Individuals charts. These are frequently referred to as "Shewhart" charts after the control charting pioneer Walter Shewhart who introduced such techniques. These charts are sensitive to detecting relatively large shifts in the process (i.e. of the order of 1.5σ or above). In computer network practice, shifts can be caused by intrusion or attack, for example. Two types of charts are usually used to detect smaller shifts (less than 1.5σ), namely CUSUM charts and EWMA charts. A CUSUM chart plots the cumulative sums of the deviations of each sample value from a target value. An alternative technique to detect small shifts is to use the EWMA methodology. This type of chart has some very attractive properties, in particular [14], [16]:

1. Unlike X-R and Individuals charts, all of the data collected over time may be used to determine the control status of a process.
2. Like the CUSUM, the EWMA utilizes all previous observations, but the weight attached to data exponentially decreases as the observations become older and older.
3. The EWMA is often superior to the CUSUM charting technique due to the fact that it detects larger shifts better.
4. EWMA schemes may be applied for monitoring standard deviations in addition to the process mean.
5. EWMA schemes can be used to forecast values of a process mean.
6. The EWMA methodology is not sensitive to normality assumptions.

In real situations, the exact value of the shift size is often unknown and can only be reasonably assumed to vary within a certain range. Such a range of shifts deteriorates the performance of existing control charts.

Calculating the optimal value of parameter λ is based on the study of authentic samples of network traffic. Random variations of network traffic are normal phenomena in the observed sample. In order to decrease or eliminate the influence of individual random variations of network traffic on occurrence of false alarms, the procedure of exponential smoothing is applied, as an aspect of data preprocessing.

For any time period t, the smoothed value S_t is determined by computing:

$$S_t = \lambda y_{t-1} + (1 - \lambda) S_{t-1} \tag{5}$$

where $0 < \lambda \leq 1$and $t \geq 3$.

This is the basic equation of exponential smoothing. The formulation here is given by Hunter [19]. It should be noted that there is an alternative approach, in which, according to Roberts [17], y_t is used instead of y_{t-1}.

This smoothing scheme starts by setting S_2 to y_1 (there is no S_1), where S_i stands for smoothed observation or EWMA, and y_i stands for the original observation. The subscripts refer to the time periods 1, 2, ..., n. For example, the third period is $S_3 = \lambda y_2 + (1 - \lambda) S_2$ and so on.

There is no generally accepted statistical procedure for choosing λ. In that situation, the method of least squares might be adequate to determine the optimal value of λ for which the sum of the squared errors (SSE) $(S_{n-1} - y_{n-1})^2$ is minimized.

The method of least squares represents a standard approach to the approximate solution of over-determined systems (i.e. sets of equations in which there are more equations than unknowns). The most important application is in data fitting. The best fit in the least squares sense minimizes the sum of squared residuals, a residual being the difference between an observed value and the fitted value provided by a model.

Here is an illustration of this principle through an example [15]. Consider the following data set consisting of n observations of data flow over time – for starting $\lambda = 0.1$:

Table 1 Smoothing scheme

Time	Flow (y_t)	S_t	Error ($S_t - y_t$)	Error squared
1	y_1			
2	y_2	y_1	E_2	E_{22}
3	y_3	S_3	E_3	E_{32}
...	...	...	...	...
n	y_n	S_n	E_n	E_{n2}
				SSE_n

The sum of the squared errors (SSE) is then $SSE_{0.1}$. After that, the SSE is calculated for $\lambda = 0.2$. If $SSE_{0.2} < SSE_{0.1}$ then $SSE_{0.2}$ is better value for λ. This iterative procedure is related to the range of λ between 0.1 and 0.9. In this way, the best initial choice for λ is determined and then, for getting more precise value, search optionally continues between $\lambda - \Delta\lambda$ and $\lambda + \Delta\lambda$, where Δλ is an arbitrarily small interval around λ (for instance, in practical applications, ± 10% around optimal λ).

The initial EWMA plays an important role in computing all the subsequent EWMA's. There are several approaches to define this value:

1. Setting S_2 to y_1
2. Setting S_2 to the target of the process
3. Setting S_2 to average of the first four or five observations

It can also be shown that the smaller the value of λ, the more important is the selection of the initial EWMA.

The sensitivity of standard EWMA algorithm can be improved by implementing the logic of adaptive threshold algorithm [22]. Namely, network anomaly in adaptive algorithm is detected only in case when for multiple consecutive time intervals (in the figure below marked with #) the threshold is exceeded (if # > *k*, where the factor *k* is set by network security administrator). The sensitivity of this algorithm also depends on the value of the threshold exceeding ($\beta\mu_t$, where where μ_t represents the measured mean in some observation period).

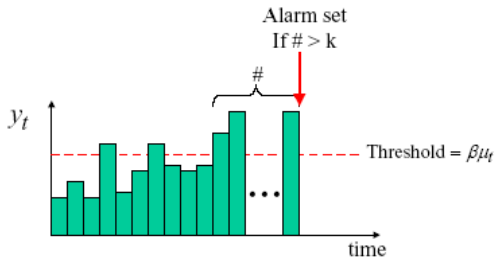

Fig. 2 Adaptive threshold algorithm

With the theme of statistical anomaly detection in computer networks and implementation of EWMA statistics in network environment have dealt also the publications [23], [13], [15] and [24].

4. Fuzzy Approach

The intrusion detection problem is viewed in the misuse or signature model as a classification problem: the goal is to classify patterns of the system behaviour in two categories (normal and abnormal), using patterns of known attacks, which belong to the abnormal class and patterns of the normal behaviour. With fuzzy rules, the solution of this classification problem is based on fuzzy logic concepts.

Fuzzy systems have several important characteristics that suit intrusion detection very well [10]:

- Fuzzy implementations had been showed to possess ability to readily combine inputs from widely varying sources (For instance, digital cameras are usually equipped with auto-focusing feature that estimates the distance. For this purpose, camera's fuzzy control system uses several different inputs).
- Many types of intrusions cannot be crisply defined (e.g. the value of adaptive (variable) alarm threshold or network values, including intrusions, which in most real cases do not belong to a set of predefined values).

- The degree of alert that can occur with intrusions is often fuzzy - because there is no clear distinction between normal and anomaly traffic behaviour in a network.

In fuzzy logic, fuzzy sets define the linguistic notions and membership functions define the truth-value of such linguistic expressions [25]. A collection of fuzzy sets, called fuzzy space, defines the fuzzy linguistic values or fuzzy classes that an object can belong to. For instance, a fuzzy space of five sets (LOW, MED-LOW, MEDIUM, MED-HIGH and HIGH) is shown in the following figure [26].

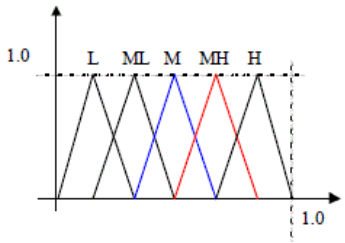

Fig. 3 Fuzzy space of five sets

With fuzzy spaces, fuzzy logic allows an object to belong to different classes at the same time. This possibility is helpful when the difference between classes is not well defined. It is the case in the intrusion detection task, where the difference between the normal and abnormal class are not well defined [27].

The approach to the problem of anomaly detection by inducting the fuzzy logic into time based EWMA algorithm can be realized through several phases:

Definition of set of possible values of the state (inputs) in multiple categories

The basic concept of the analyzed algorithm is the following: for the input network traffic samples, correspondent EWMA values are calculated and observe as many consecutive values of how many sets the fuzzy space is composed. For the purposes of this analysis, the fuzzy space consists of three sets. It implies that the set of regular EWMA values of network traffic is divided, depending on the intensity, on three categories. For instance: low, medium and high EWMA value (in accordance with the defined membership function - in relation to the threshold, shown in Fig. 2).

In addition to the criteria of traffic intensity, it is possible in a similar way to set the other variable criteria for anomaly detection as well - number of consecutive threshold (in this case, upper control limit) overcomes #. Since by its nature it represents a crisp value that can not be fuzzified, this paper will, for reasons of simplification of analysis - without loss of generality, accept the value of # = 3. This means that the fuzzy algorithm analyzes a block of three consecutive EWMA values (EWMA1, EWMA2 and EWMA3) and depending on their values, formulates the conclusion about the type of output. With implementation of exceeding parameter (the parameter that indicates the percentage above upper threshold; e.g. 0.5), fine tuning of the algorithm is provided, additionally eliminating false alarms.

Definition of set of possible actions (or output types) in a few sets or categories

In the case of anomaly detection, the possible set of output actions could be attack alarm, warning alarm and indication of normal condition. In this way, fuzzy outputs are

determined. In order to do this, it is necessary first to set up the empirical definition of fuzzy rules ("if - then" rules) or fuzzy relations. Fuzzy rules in this case may look like this:

- If all three EWMA values of traffic are high (vrednost veća od thresholda), then attack alarm is generated.
- If two values are high, and one is medium, then warning alarm is generated.
- All other cases represent normal traffic situations.

The next step is defining the membership function that describes the fuzzy sets. A membership function is a curve that defines how each point in the input space is mapped to a membership value (or degree of membership) between 0 and 1.

There are different types of membership functions. The only condition a membership function must really satisfy is that it must vary between 0 and 1. The function itself can be an arbitrary curve whose shape is defined as a function that suits from the point of view of simplicity, convenience, speed, and efficiency.

Fuzzy inference is the actual process of mapping from a given input to an output using fuzzy logic.

5. Simulation and Results

For simulation of described fuzzy EWMA algorithm the software package “Matlab” - Fuzzy Logic Toolbox 2.0 was used. The basic simulation scheme of algorithm consists of three consecutive input EWMA values and one output value (Fig. 4).

In the fuzzy logic toolbox, there are five parts of the fuzzy inference process:

- Fuzzification of the input variables
- Application of the fuzzy operator (AND or OR) in the antecedent
- Implication from the antecedent to the consequent
- Aggregation of the consequents across the rules
- Defuzzification

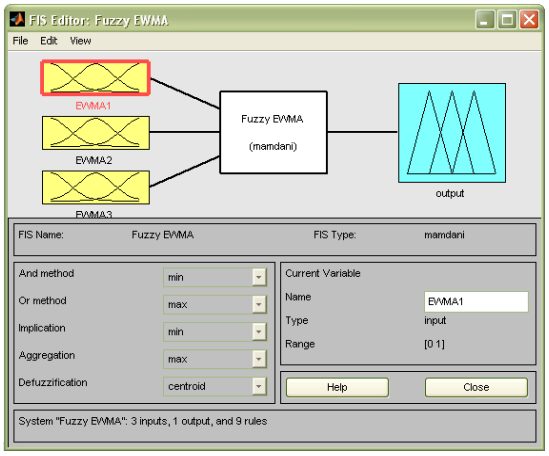

Fig. 4 Basic simulation scheme

Two types of fuzzy inference systems (FIS) is possible to implement in the toolbox: Mamdani-type and Sugeno-type. These two types of inference systems vary somewhat in the way outputs are determined. Sugeno (or Takagi-Sugeno-Kang) method of fuzzy

inference is similar to the Mamdani method in many respects. The first two parts of the fuzzy inference process, fuzzifying the inputs and applying the fuzzy operator, are exactly the same. The main difference between Mamdani and Sugeno is that the Sugeno output membership functions are either linear or constant. Mamdani-type inference, as defined for the toolbox, expects the output membership functions to be fuzzy sets. After the aggregation process, there is a fuzzy set for each output variable that needs defuzzification [28], [29].

The membership functions for inputs and output are determined according to the following figures:

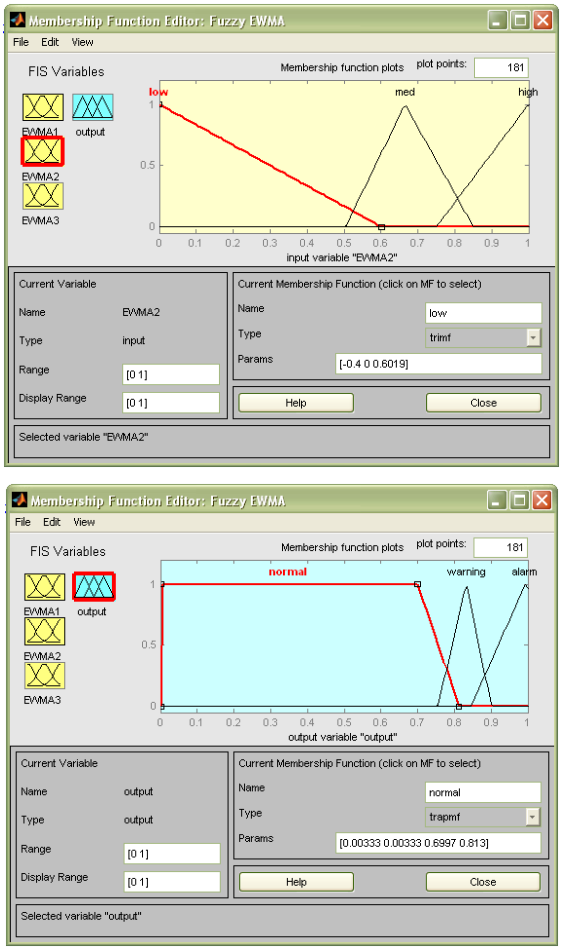

Fig. 5 Input and output membership functions

After creation of membership functions, the next step is formulation of fuzzy rules, which is realized using rule editor (Fig. 6).

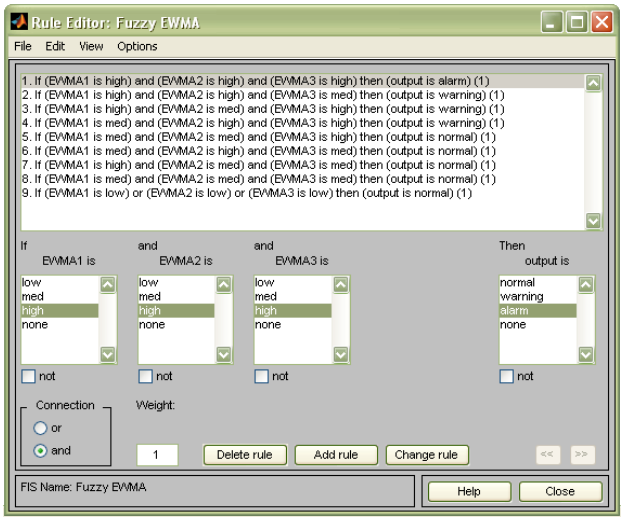

Fig. 6 Fuzzy rules

The first check of this fuzzy algorithm is made in such way that input values (EWMA1 = EWMA2 = EWMA3 = 0.91) are selected with intention to generate an alarm situation. It was expected, in accordance with defined rules, to get relatively high output value, which was also actualized (output = 0.945). The practical choice of input values is realized by scrolling the vertical line that indicates the value, while the program automatically recalculates the value of output.

Fig. 7 Rule viewer (alarm condition)

The form analysis of membership functions is done for selected combination of input values that generates warning and alarm indication. The situation in case of chosen input values that generates a warning condition, is given by Fig. 8.

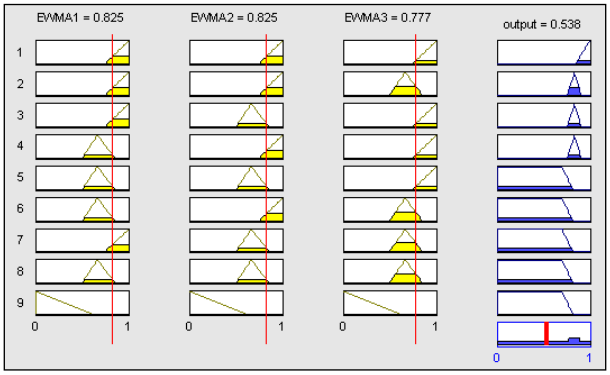

Fig. 8 Rule viewer (warning condition)

Changing the offered membership functions [30], the output values were examined and compared. In case of warning, for „warning“ segment, the following output values are confirmed:

Table 2 Output values - warning

Membership function	Output value
triangular (trimf)	0.538
generalized bell (gbellmf)	0.533
Gaussian curve (gaussmf)	0.535
two-sided composite Gaussian curve (gauss2mf)	0.533

Similarly, in case of alarm, for „alarm“ output segment, the following values are confirmed:

Table 3 Output values - alarm

Membership function	Output value
triangular (trimf)	0.945
sigmoidal (sigmf)	0.943
difference between two sigmoidal functions (dsigmf)	0.944
product of two sigmoidal functions (psigmf)	0.943

Looking at the results from these tables, insignificant differences can be found in output values. However, triangular membership function provides the largest output value and may be concluded that it is the most appropriate shape for application in case of this security algorithm.

Simulation of algorithm in conditions of network anomaly

As an illustration of the functioning of the described anomaly detection algorithm, the samples of network traffic (acknowledgement (ACK) numbers in TCP headers) can serve in observation time period with the parameters calculated on the basis of historical data: $EWMA_0 = 50$ and $\sigma = 2.0539$, with λ accepted to be 0.3 (often used value).

The control limits are in this case:

$UCL = 50 + 3*(0.4201)*(2.0539) = 52.5884 \approx 52.6$
$LCL = 50 – 3*(0.4201)*(2.0539) = 47.4115 \approx 47.4$

Data from Table 4 derive from local server using a packet sniffer (Wireshark) that captures and filters packets according to specific protocol. In order to see only captured packets using the TCP protocol, in the Filter field is necessary to enter "tcp" as shown in Figure 9 (example). Extracting the ACK numbers of packets (rounded data values) is realized 35 times, at equal time intervals (5 minutes).

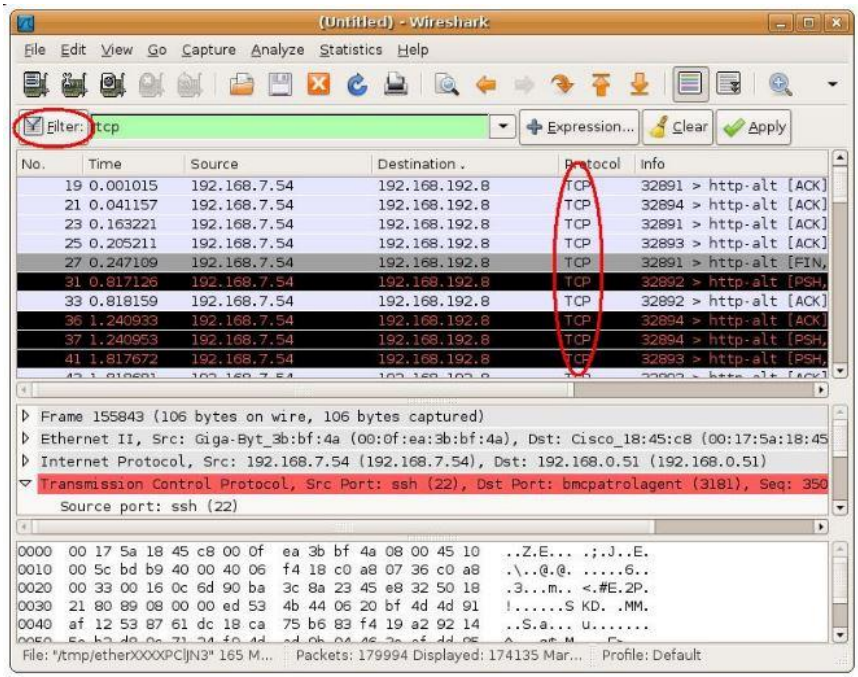

Fig. 9 Filtering TCP packets

Table 4 Network traffic samples and EWMA values

Sample	Data	EWMA
0		50.00
1	52	50.60
2	47	49.52
3	53	50.56
4	49.3	50.18
5	50.1	50.16
6	47	49.21
7	51	49.75
8	50.1	49.85
9	51.2	50.26
10	50.5	50.33
11	49.6	50.11
12	47.6	49.36
13	49.9	49.52
14	51.3	50.05
15	47.8	49.38
16	51.2	49.92
17	52.6	50.73
18	52.4	51.23
19	53.6	51.94
20	52.1	51.99
21	53.9	52.56
22	53	52.69
23	52.9	52.76
24	52.5	52.68
25	51.8	52.42
26	49.7	51.60
27	50.5	51.27
28	49.9	50.86
29	48.5	50.15
30	49.6	49.99
31	51.2	50.35
32	48.3	49.74
33	50	49.81
34	50.4	49.99
35	51.6	50.47

Analyzing the values in the table above, it should be noted that three consecutive values of network traffic in the marked samples 21-23 are above the UCL (the 19th sample is a single case that is not of interest for analysis), simulating in this way the situation suspicious to alarm. These elevated traffic values result in expected increase in the three consecutive EWMA values (22-24 - marked), which also exceed the UCL value.

Accepting that each network value that is for 20% or more greater than UCL (threshold = 1.2*UCL, analogy with Fig. 2) is a situation which can be interpreted as a certain alarm, and bearing in mind the form of membership functions (Fig. 5), the situation of warning is at about 80% (between 0.75 and 0.9 more precisely) of the alarm situation, which is 0.8*0.2 = 0.16. It gives an alarm threshold value of 52.75 (UCL + 0.16). Among the three marked EWMA values that exceeded the threshold, only one was greater than 52.75. Deciding on

the basis of the majority logic (one alarm situation and two warnings), it is concluded that the analyzed network situation can be interpreted as a warning.

6. IMPROVEMENT OF RESULTS

In further phase of research, the improvement possibility of previously obtained results will be examined. In that sense, the idea was to predefine some of the built-in fuzzy operators, because Fuzzy logic toolbox offers this opportunity. The situation when all three inputs have high values was analyzed. Firstly, it is found that the choice of some other Or method and aggregation does not affect the output value. In And method, the options "min" and "prod" were examined and determined the correspondent output values 0.945 (min) and 0.934 (prod). In this research, instead of function "min", the function of square root of minimum is proposed and tested its impact on the output value. This function is defined in file *customand.m* as:

function y=customand(x)
y=sqrt(min(x)),

and gave the output result 0.949, which is better than "min" function's result.

In addition to this, research has shown that "prod" function from Implication part generates higher output signal then "min" function, which represents another improvement.

Similarly, it is shown that "mom" option (mean of maximum) instead of popular "centroid" from Defuzzification part has the greatest impact on output.

Considering the previous improvements, testing the output values was performed with the following selected options (Fig. 10). The final result of this research is given by Fig. 11.

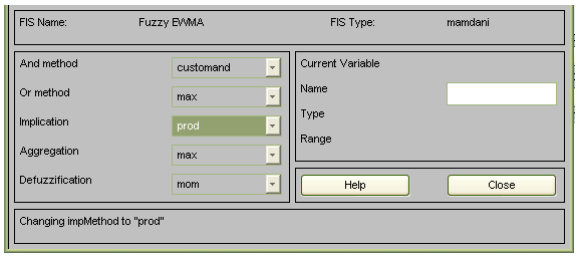

Fig. 10 The final fuzzy inference options

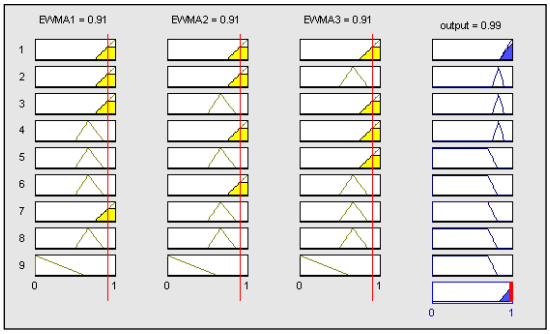

Fig. 11 The final result

Analyzing the last figure, it is necessary to emphasize the greatest value of output (0.99), which proves the correctness of presented conclusions. The percentage of improvement compared to the previous case (0.945) is about 5%.

7. CONCLUSION

On the basis of elaboration presented in this paper it can be concluded that the introduction of fuzzy logic in standard EWMA algorithm for anomaly detection - the so-called fuzzy EWMA (FEWMA) algorithm - opens the possibility of previous warning from a network attack, which contributes to raising the level of security. Standard EWMA algorithm does not have this opportunity. Besides, fuzzy logic enables precise determination (fine tuning) of degree of the risk (expressed in form of percentage).

It is important to emphasize that here proposed improvement of standard EWMA algorithm can be applied to other algorithms based on threshold, since EWMA algorithm in its basis, is security algorithm with fixed threshold.

The future work will focus on creating opportunities for practical testing of the presented approach in real time. This involves enabling the automation of algorithm functioning by creating the appropriate software for taking live-network traffic samples, calculating EWMA values and real-time decision-making, and linking these functions with fuzzy module that has the ability to adjust the membership functions of the input and output.

REFERENCES

[1] S. Drew, *Intrusion Detection FAQ: What is the Role of Security Event Correlation in Intrusion Detection?*, SANS Institute, http://www.sans.org/security-resources/idfaq/role.php

[2] P. Čisar and S. Maravić Čisar, "Network Statistical Anomaly Detection Based on Traffic Model. Annals of Faculty Engineering Hunedoara", *International Journal Of Engineering, Tome X-Fascicucle* 3, , pp. 89–96, 2012.

[3] N. Ye, Q. Chen and C.M. Borror, "EWMA forecast of normal system activity for computer intrusion detection", *IEEE Transactions on Reliability*, vol. 53, no. 4, pp. 557–566, 2004.

[4] M.S. Abadeh, H. Mohamadi and J. Habibi, "Design and analysis of genetic fuzzy systems for intrusion detection in computer networks", *Expert Systems with Applications*, vol. 38, no. 6, 2011, pp. 7067–7075.

[5] Z. Yu and J. Tsai, "Fuzzy Model Tuning for Intrusion Detection Systems", In Proceedings of the International Conference on Autonomic and Trusted Computing, ATC 2006, 2006, pp. 193-204.

[6] G. Spathoulas and S. Katsikas, "Reducing false positives in intrusion detection systems", *Computers & Security*, vol. 29, no. 1, pp. 35–44, 2010.

[7] A. Silva, E. Pontes and F. Zhou, "PRBS/EWMA based model for predicting burst attacks (Brute Froce, DoS) in computer networks", In Proceedings of the International Conference on Digital Information Management (ICDIM), 2014.

[8] H.H.W.J. Bosman, Anomaly detection in networked embedded sensor systems. University of Technology, Eindhoven, 2016

[9] S. Senturk, N. Erginel, I. Kaya and C. Kahraman, "Fuzzy exponentially weighted moving average control chart for univariate data with a real case application", *Applied Soft Computing*, vol. 22, pp. 1–10, 2014.

[10] J.E. Dickerson, J. Juslin, O. Koukousoula, and J.A. Dickerson, "Fuzzy intrusion detection IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS)", In Proceedings of the International Conference, Vancouver, British Columbia, vol. 3, 2001, pp. 1506-1510.

[11] J.E. Dickerson and J.A. Dickerson, "Fuzzy Network Profiling for Intrusion Detection", In Proceedings of the NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta, 2000, pp. 301-306.

[12] K. Liston, Intrusion Detecion FAQ: Can you explain traffic analysis and anomaly detection?" SANS Institute, http://www.sans.org/security-resources/idfaq/anomaly_detection.php

[13] G. Fengmin, Deciphering Detection Techniques: Part II Anomaly–Based Intrusion Detection. White Paper, McAfee Security, 2003, https://secure.mcafee.com/japan/products/pdf/Deciphering_Detection_Techniques-Anomaly-Based_Detection_WP_en.pdf
[14] P. Čisar and S. Maravić Čisar, "Optimization Methods of EWMA Statistics", *Acta Polytechnica Hungarica*, vol. 8, no. 5, pp. 73–87, 2011.
[15] P. Čisar, S. Bošnjak and S. Maravić Čisar, "EWMA-based threshold algorithm for intrusion detection", Computing and Informatics, vol. 29, Institute of informatics, Slovak academy of sciences, Bratislava, Slovakia, pp. 1089–1101, 2010.
[16] P. Čisar, S. Bošnjak and S. Maravić Čisar, "EWMA Algorithm in Network Practice", *Int. J. of Computers, Communications & Control*, vol. V, no. 2, 2010, pp. 160–170.
[17] S.W. Roberts, Control Chart Tests Based on Geometric Moving Averages. Technometrics, 1959
[18] NIST/SEMATECH e-Handbook of Statistical Methods (2008). http://www.itl.nist.gov/div898/handbook/pmc/section3/pmc324.htm
[19] J.S. Hunter, The exponentially weighted moving average. Journal of Quality Technology 18, 1986, pp. 203–210.
[20] J.M. Lucas and M.S. Saccucci, Exponentially Weighted Moving Average Control Schemes: Properties and Enhancements. Technometrics Vol. 32, No. 1, 1990, pp.1-29.
[21] Engineering Statistics Handbook–EWMA Control Charts, http://www.itl.nist.gov/div898/handbook/pmc/section3/pmc324.htm
[22] V. Siris and F. Papagalou, Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks, 2004, http://www.ist-scampi.org/publications/papers/siris-globecom2004.pdf
[23] S. Sorensen, Competitive Overview of Statistical Anomaly Detection. White Paper, Juniper Networks, 2004
[24] P. Čisar and S. Maravić Čisar, Network Statistics in Function of Statistical Intrusion Detection. Springer Publication, Studies in Computational Intelligence, Volume 313, Springer Verlag publication, 2010, pp. 27–35.
[25] M. Hellmann, Fuzzy logic introduction. a Laboratories Antennas Radar Telecom, F.R.E CNRS 2272, Equipe Radar Polarimetrie, 2000, France
[26] S.M.A. Naqshbandi and V.W. Samawi, "One-Rule Genetic-Fuzzy Classifier", In Proceedings f the 2012 IEEE International Conference on In Computer Science and Automation Engineering (CSAE), vol. 2, 2012, pp. 204–208.
[27] K. Subramanian, "Emerging intuitionistic fuzzy classifiers for intrusion detection system", *Journal of Advances in Information Technology 2.2*, pp. 99–108, 2011.
[28] Matlab & Simulink, "What Is Sugeno-Type Fuzzy Inference?", http://www.mathworks.com/help/fuzzy/what-is-sugeno-type-fuzzy-inference.html
[29] B. Lazzerini, Fuzzy Logic Toolbox, http://www.unife.it/ing/lm.infoauto/tecniche-controllo/FIS_Estratto.pdf
[30] Fuzzy Logic Toolbox User's Guide, http://www.mathworks.com/help/pdf_doc/fuzzy/fuzzy.pdf
[31] O. Osanaiye, K.K.R. Choo and M. Dlodlo, "Change-Point Cloud DDoS Detection using Packet Inter-Arrival time", In Proceedings of the 8th IEEE Computer Science & Electronic Engineering Conference (CEEC'16), Sept 28th -30th 2016, Essex, UK.
[32] O. Osanaiye, A.S. Alfa and G.P. Hancke, "A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks", Sensors, vol. 18, no. 6, p. 1691, 2018.