EWMA Algorithm in Network Practice

P. Čisar, S. Bošnjak, S. Maravić Čisar

Petar Čisar
Telekom Srbija
Prvomajska 2-4, Subotica, Serbia
E-mail: petarc@telekom.rs

Saša Bošnjak
Faculty of Economics
Segedinski put 9-11, Subotica, Serbia
E-mail: bsale@eccf.su.ac.yu

Sanja Maravić Čisar
Subotica Tech
Marka Oreškovića 16, Subotica, Serbia
E-mail: sanjam@vts.su.ac.rs

Abstract: Abstract: Intrusion detection is used to monitor and capture intrusions into computer and network systems which attempt to compromise their security. Many intrusions manifest in changes in the intensity of events occuring in computer networks. Because of the ability of exponentially weighted moving average (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 paper also gives a review of a possible optimization method. The validation check of results will be performed on authentic network samples.
Keywords: intrusion detection, EWMA, control limits, optimization, autocorrelation

1 Introduction

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 statistic, which is an exponentially weighted average of all prior data, including the most recent measurements.

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 statistic that is calculated is the following:

$$EWMA_t = \lambda Y_t + (1 - \lambda)EWMA_{t-1} \qquad t = 1, 2, \ldots, n \tag{1}$$

where

- $EWMA_0$ is the mean of historical data (target)

- Y_t is the observation at time t

- n is the number of observations to be monitored including $EWMA_0$

- $0 < \lambda \le 1$ is a constant that determines the depth of memory of the EWMA.

This equation has been established by Roberts as described in [4].

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. The value of λ is usually set between 0.2 and 0.3 [2] although this choice is somewhat arbitrary. Lucas and Saccucci [3] 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).

The estimated variance of the EWMA statistic is approximately:

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

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:

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

where the factor k is either set equal 3 (the 3-sigma control limits) or chosen using the Lucas and Saccucci tables (ARL = 370).

In addition to the aforementioned authors, the publications [6]-[13] have also dealt with the topic of EWMA statistics and statistical anomaly detection in computer networks.

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 primarily used to detect smaller shifts (less than 1.5σ), namely cumulative sum (or 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:

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 better detects larger shifts.

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. One of the algorithms for determining the maximal shift in normal traffic is described in [17].

The paper describes the process of application of EWMA algorithm for one major user, given as an example. It can be shown that the obtained results are valid for the other analyzed users as well. This research uses samples of authentic network traffic (i.e. traffic intensity in a unit of time). Traffic analysis is realized in the form of statistical calculations on samples which derives from traffic curve. From the appropriate pattern of Internet traffic, 35 samples of local maximums are taken in order to ensure that the statistical analysis is performed on a large sample (number of samples $n > 30$), thus supporting and leading to general conclusions.

The aim of this research is to determine those allowed EWMA values of traffic, that when they are exceeded, it will be considered as the appearance of a statistical anomaly suspected to attack. In this sense, the choice of only local maximums for analysis can be accepted as logical, because the critical point of maximum value of aggregate traffic is in this way also included.

The proposed method of calculating the overall optimal value Λ is applied to traffic patterns, on the basis of which the lower and upper control limits of traffic are determined. For statistical detection of an attack the primary interest is the appearance of a situation in which the upper control limit is exceeded. The overstepping of the lower control limit can be understood as a statistical anomaly, but in the case of this research, it is only related to the local maximum (and not to the aggregate network traffic) and as such does not endanger the security of the computer network in general. Therefore, the situation in which the value of network traffic falls below some lower limit is not considered to be a suspicious event or attack, because the initial presumption of this research is the increase of traffic during an external attack. For the observed pattern of traffic, EWMA values are calculated and if these values are outside of the control limits, that situation is interpreted as a statistical anomaly. Emphasis in this work is placed on determining the occurrence of false alarms, as an important security feature of applied algorithm.

2   Optimized Exponential Smoothing

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:

$$S_t = \lambda y_{t-1} + (1 - \lambda)S_{t-1} \quad \text{where} \quad 0 < \lambda \leq 1 \text{ and } t \geq 3 \tag{4}$$

This is the basic equation of exponential smoothing. The formulation here is given by Hunter [2].

This smoothing scheme begins by setting S_2 to y_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 S_1. The optimal value for λ is the value which results in the smallest mean of the squared errors (MSE).

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 user would be well-advised to try several methods before finalizing the settings.

For different input values of initial parameter S_2, an application in "Matlab" is created which calculates and plots the dependence of SSE and partial value of λ in range of $0 \div 1$, with adjustable step. In addition, the optimal value λ_{opt} is also calculated. For the optimal value, in accordance with the smoothing scheme, that particular value is taken for which the SSE is minimal. The following figure shows an example for calculating the optimal value of the parameter λ for a specific S_2.
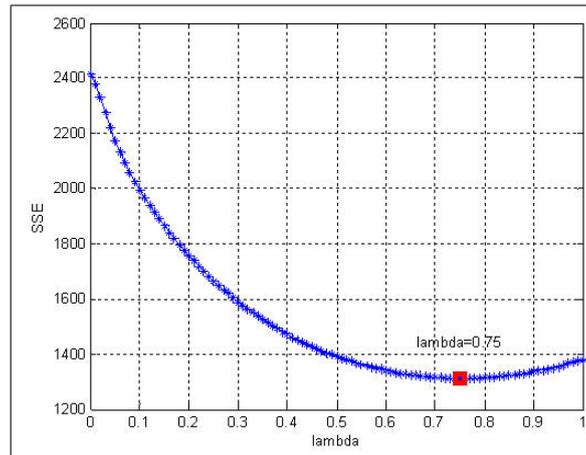

Figure 1: Calculation λ_{opt} (SSE)

Due to the lack of an exact method of calculation in available publications about the determination of the initial S_2 in the procedure of exponential smoothing, the authors of this paper have dealt with researching the link between selection of $S_2 = y_1$ and λ_{opt}, i.e. $S_2(\lambda_{opt})$. In that sense, the range of S_2 is determined using the lowest to the highest sample value during the period of observation. This research was conducted on an authentic sample of network traffic of an Internet service provider and the segment of observation was the range of values of local maximums (in this concrete case from 8 to 34 Mb/s), with a large enough number of values $n = 33 > 30$, taking into account the generality of conclusions. The period of observation was one month. The next table (Table 1) shows the numerical and graphical dependence $S_2(\lambda_{opt})$.

Since a set of different results has been obtained for partial values of λ_{opt}, the authors suggest for the overall optimal parameter λ_{opt} to accept the average of all the partial results (in this particular case it is 0.75).

3 Autocorrelation

Autocorrelation or serial correlation of time series means that the value of the observed variable in a time unit depends on values which appear prior to or later in series. In practical situations, autocorrelation of the first order is usually examined, which may be shown by a simple correlation coefficient or so-called autocorrelation coefficient. Let R_t be the time series data, where $t = 1, 2, \ldots, T$, then the autocorrelation coefficient of the first order is given by:

	S_2	λ_{opt}
1	8	0.72
2	9	0.72
3	10	0.72
4	11	0.72
5	12	0.71
6	13	0.71
7	14	0.72
8	15	0.72
9	16	0.72
10	17	0.72
11	18	0.72
12	18.5	0.73
13	19	0.73
14	19.5	0.73
15	20	0.73
16	20.5	0.73
17	21	0.74
18	21.5	0.74
19	22	0.74
20	22.5	0.75
21	23	0.75
22	23.5	0.75
23	24	0.75
24	25	0.76
25	26	0.77
26	27	0.77
27	28	0.78
28	29	0.79
29	30	0.8
30	31	0.8
31	32	0.81
32	33	0.82
33	34	0.82

Table 1: Calculation of $S_2(\lambda_{opt})$

$$\rho(R) = \frac{\sum_{t=2}^{T} R_t R_{t-1}}{\sqrt{\sum_{t=2}^{T} R_t^2 \sum_{t=2}^{T} R_{t-1}^2}} \qquad \text{-1} \le \rho \le 1 \qquad (5)$$

One of the standard features of traffic time series is that increasing rates of traffic R_t are not mutually significantly autocorrelated, ie. the value of autocorrelation coefficient is near zero. At the same time, this means that the distribution of positive and negative values of increasing rates is random and that does not follow a specific systematic regularity. Positive autocorrelation implicates that the positive values are followed by mainly positive values and negative values by negative ones and then is $\rho \approx +1$. In the case of negative autocorrelation, there is often a change of sign, i.e. the positive rate in most cases leads to a negative rate and vice versa and then is $\rho \approx -1$. Since there is no typical scheme, on the basis of positive rate in particular time period there is now way of concluding (it can not be concluded) with a significant probability that in the next period either a growth or decline will appear. The same applies to the situation for the negative rate.

Researchers in [5] dealt with the influence of autocorrelated and uncorrelated data on the behavior of intrusion detection algorithm. In their work they came to conclusion that EWMA algorithm for autocorrelated and uncorrelated data works well in the sense of intrusion detection in some information systems. The advantage of EWMA technique for uncorrelated data is that this technique (as opposed to the case of autocorrelated data) can detect not only rapid changes in the intensity of events, but also small changes in the mean value realized through the gradual increase or decrease of the intensity of events. However, in EWMA for uncorrelated data, the initial value of smoothed intensity events is to be reset after intrusion detection, in order to avoid the impact of current values of parameters on future results (*carry-over effect*). In case of EWMA for autocorrelated data this reset is not necessary, because EWMA automatically adjusts the upper and lower control limits. Generally, the smoothing constant should not be too small, so that a short-term trend in the intensity of events in the recent past can be detected.Other

publications have also shown the need for taking into account the autocorrelation of input data. As it is emphasized in [18], in the case of dynamic systems the autocorrelation in variables is taking into account incorporating time lags of the time series during the modeling stage.

Samples of network traffic were obtained by network software "MRTG" (Multi Router Traffic Grapher) version 2.10.15. This software generates three types of graphs:

- Daily - with calculation of 5-minute average

- Weekly - with calculation of 30-minute average

- Monthly - with calculation of 2-hour average

The graphs also enable numerical information on the maximum and average traffic for the appropriate period of time.

Daily, weekly and monthly graphs of the first measurement will be used for calculation of initial historical data, while the application of EWMA statistics, with aim of checking the validity of certain parameters, will be realized on daily, weekly and monthly traffic graphs of the second measurement.

For the application of exponential smoothing method to network traffic it is necessary first to determine the historical values: $EWMA_0$ and standard deviation σ_0. For this purpose, it is necessary to collect appropriate traffic samples to perform adequate calculations. This study will use a total of 105 samples of local maximum: 35 samples from the daily traffic graph, 35 samples from the weekly traffic graph and 35 samples from the monthly traffic graph (Table 2).

Time	y_t (daily)	y_t (weekly)	y_t (monthly)
1	12	21	23
2	10.5	22.5	30
3	8.5	23	27
4	10.5	20	27
5	18	20.5	25
6	22	23.5	27
7	25.5	24	22
8	20	21	24
9	33.9	23	23
10	25	25	20
11	24	25.5	24.5
12	26.5	24.5	26.5
13	27.5	22	28
14	23	25.5	27
15	25	27	23
16	24	28	22.5
17	23	27	26.5
18	23	28	31
19	22	25.5	22.5
20	23	30	22.5
21	23	29	27
22	23	26.5	25
23	23	29	26
24	16	26.5	28
25	16	27.5	21
26	9	26	24
27	11.5	25	22
28	8.5	24	22
29	8.5	23.5	22
30	14	22	23
31	23	22.5	27
32	23	24	29
33	20	24	25
34	23	25	25
35	23	23	22

Table 2: Network samples

On the basis of the data presented in the table the following can be calculated: $EWMA_0 = 23.10$ and $\sigma_0 = 4.87$.

In accordance with the method described above and to justify the usage of EWMA statistics, it is important to determine the statistical independence of samples, which will be examined by checking the existence of correlation between data. For this purpose, Pearson's correlation coefficient will be used, which is supplied as a ratio of covariances of two variables and the product of their standard deviations:

$$\rho_{xy} = \frac{Cov(X,Y)}{\sigma_x \sigma_y} \qquad -1 \le \rho_{xy} \le 1 \qquad\qquad (6)$$

Other authors proposed different interpretation ways of correlation coefficient. Cohen [1] noted that all the criteria are based on the greater or lesser extent of arbitrariness and should not be kept too strictly. Yet, one often used interpretation of these coefficients is given below, as described in [16]:

- ρ between 0 and 0.2 - no correlation or is insignificant

- ρ between 0.2 and 0.4 - low correlation

- ρ between 0.4 and 0.6 - moderate correlation

- ρ between 0.6 and 0.8 - significant correlation

- ρ between 0.8 and 1 - high correlation

The value of correlation coefficient ρ_{xy} can be calculated using the statistical function CORREL (array1, array2) in MS Excel. When examining the table above, it is possible to identify three series of data (daily, weekly and monthly) and in this sense three different correlation coefficients can be calculated:

- correlation coefficient for daily - weekly series: $\rho_1 = 0.28 \rightarrow$ low correlation

- correlation coefficient for daily - monthly series: $\rho_2 = 0.04$

- correlation coefficient for weekly - monthly series: $\rho_3 = -0.04$

Beside testing the correlation coefficient within a single measurement, it is important to check the existence of correlation between corresponding periods from different measurements. For that purpose, values of correlation coefficient of two daily (weekly, monthly) intervals are checked and the following results are obtained:

- correlation coefficient for daily - daily series: $\rho_4 = -0.15$

- correlation coefficient for weekly - weekly series: $\rho_5 = 0.11$

- correlation coefficient for monthly - monthly series: $\rho_6 = -0.02$

As all calculated coefficients are with low degree of correlation, or without it, it can be concluded that the used data are statistically independent and that the application of EWMA statistics is justified.

4 Network Practice

Values $EWMA_0$ and σ_0 are calculated for the period of one month. It can be reasonably assumed that these values in another monthly period of observation would be different, having in mind the various unpredictable traffic situations and accidental nature of network traffic as a process. Therefore, in the further phase of research, the extent of change of these values will be studied.

The determination of maximum changes of characteristic traffic values (maximum and average) is based on the analysis of numerical data of several larger Internet users that derives from the popular network software MRTG, which is related to the period of one day, week and month. Without the loss of generality, the graphical presentation of curves from three users is given below, noting that the observed traffic curves of other users do not deviate significantly from the forms shown here.
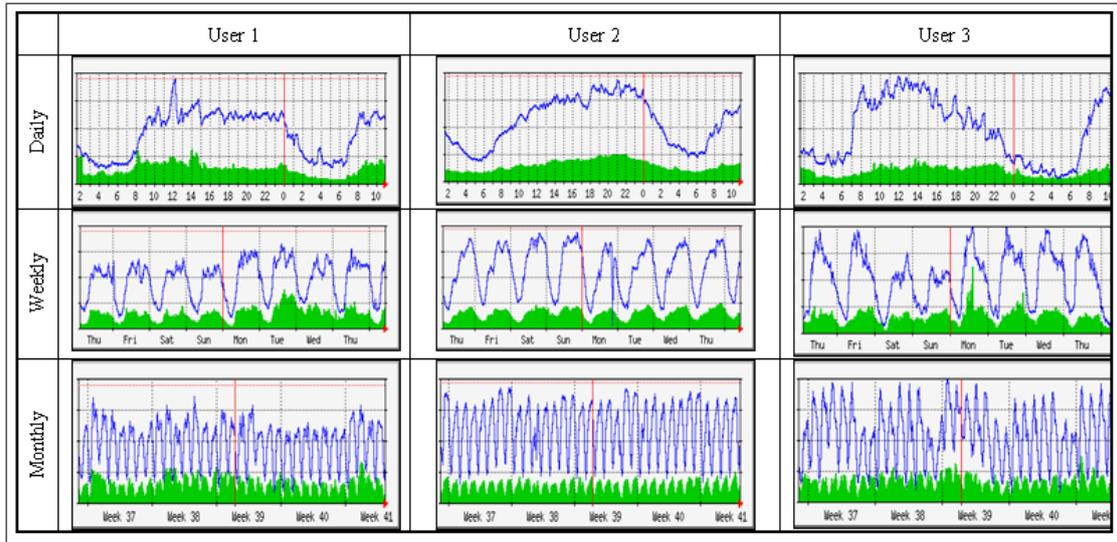
Figure 2: Traffic curves of different users

	Daily1 [Mb/s]	Daily2 [Mb/s]	Diff. [%])	Weekly1 [Mb/s]	Weekly2 [Mb/s]	Diff. [%]	Monthly1 [Mb/s]	Monthly2 [Mb/s]	Diff. [%]
User 1									
Max	33.9	33.1	-2.4	29.7	33.4	12.4	9.7	9.8	1
Average	16.5	19.1	15.8	17.0	21.1	24.1	6.01	6.6	9.8
User 2									
Max	3.94	3.63	-7.8	3.98	3.68	-7.5	48.2	49.2	2
Average	2.35	2.09	-11	2.28	2.09	-8.3	30.9	30	-3
User 3									
Max	9.31	10.0	7.4	9.71	9.99	2.9	9.9	9.7	-2
Average	5.71	6.01	5.2	5.63	6.64	17.9	5.4	4.9	-9.2
User 4									
Max	9.69	9.99	3.1	10.0	9.91	-0.9	10	10	0
Average	4.96	5.14	3.6	5.2	4.94	-5	7.4	7.6	2.7
User 5									
Max	48.2	46.3	-3.9	48.5	45.2	-6.8	1.8	1.8	0
Average	29	24.4	-15.9	30.4	26.4	-13.1	0.14	0.14	0
User 6									
Max	10.1	10.1	0	10.0	10.0	0	3.94	3.66	-7.1
Average	7.78	7.95	2.2	7.43	8.14	9.6	1.9	2.03	6.8
User 7									
Max	3.98	3.97	-0.02	3.94	3.99	1.2	3.9	3.9	0
Average	1.74	1.79	2.9	1.88	1.99	5.9	1.9	2	5.2

Table 3: Differences in characteristic values of traffic

The maximum and average values of traffic are calculated twice in the period of a month. The results are arranged in the following table:

By analysis of the numerical data it can be concluded that the maximum change of mean value p is not greater than 25%. Namely, that is the largest deviation of size in both measurements.

Since the main idea of this research is to find out the maximum and minimum tolerant EWMA values of local maxima, in further calculations the following values will be used (for the accepted p = 0.25):

$EWMA_{0max} = (1+p)EWMA_0 \approx 1.25EWMA_0$

$EWMA_{0min} = (1-p)EWMA_0 \approx 0.75EWMA_0$

Similarly, $\sigma_{0max} \approx 1.25\sigma_0$ and $\sigma^2_{EWMA} = (\Lambda/(2-\Lambda))\sigma^2_{0max}$.

Previously calculated values of parameters $EWMA_0$ and Λ_{opt}, as well as the values of UCL and LCL from the first measurement will be verified in different situations of daily, weekly and monthly traffic from the second measurement. UCL value is given by $EWMA_{0max} + k\sigma_{EWMA}$, while LCL is $EWMA_{0min} - k\sigma_{EWMA}$. The following results are obtained:

It is important to notice that according to the previous figure in case of appropriately determined EWMA parameters, there is no situation of threshold exceeding, which eliminates the appearance of false alarms.
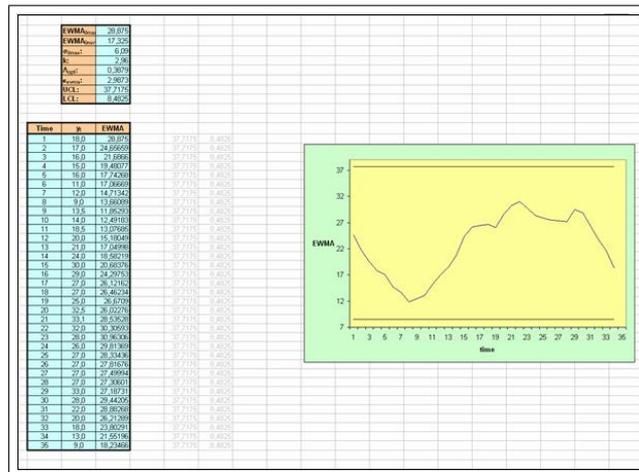
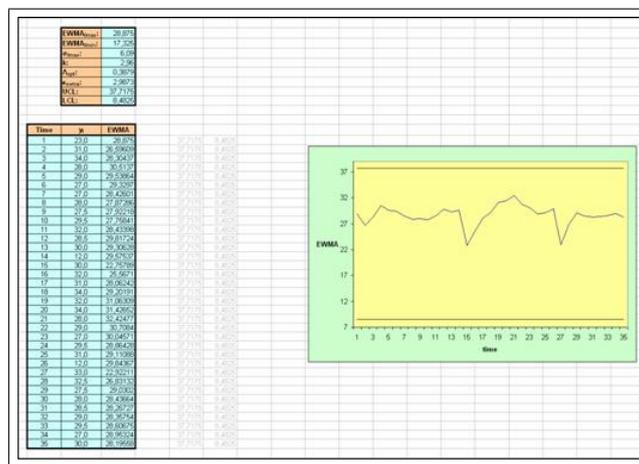Figure 3: Verification (daily traffic, second measurement)

Figure 4: Verification (weekly traffic, second measurement)

5 Conclusions

The aim of this research was to examine the possibility of applying EWMA statistics in intrusion detection in network traffic.

The research has shown that direct application of this algorithm on computer network traffic, as applied in industrial processes, does not provide acceptable results. Namely, often proposed values for exponential smoothing factor in case of network application of the algorithm, may in some circumstances lead to the creation of false alarms, thus endangering the security level of system. Due to the lack of an acceptable precise method for determination of initial value of the coefficient in exponential smoothing procedure in available publications, this research has been directed towards establishing a relation between the choice of initial ratio and optimal value for smoothing. By creating the appropriate application, the practical way was presented for testing the impact of different values of parameters on the level of anomaly detection. This enabled the establishment of graphical presentation of input depending on output sizes, which all contributed to the creation of proposed method for calculating the optimal value of smoothing factor.

Before the start of the implementation of statistical analysis of traffic, the extent of autocorrelation between the used data has to be examined, by calculating the correlation coefficients. One of the impor-
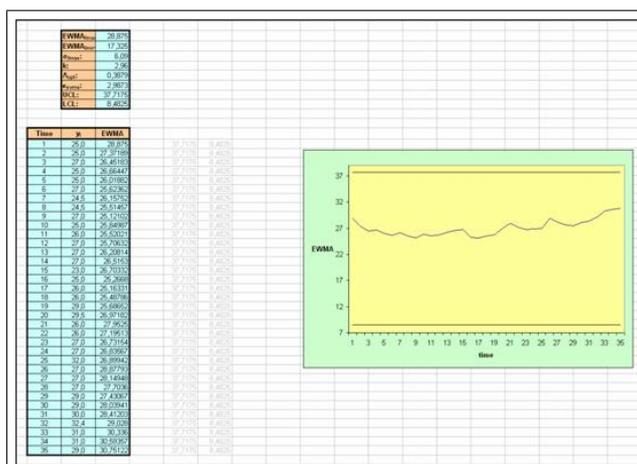
Figure 5: Verification (monthly traffic, second measurement)

tant results is that it is shown that analysis of properties of network traffic based on individual patterns of daily traffic only is not recommended, because of the increased level of autocorrelation. For this reason, when calculating the historical parameters, network traffic must be viewed in a wider context of time, taking into account the weekly and monthly periods. Using the network monitoring software, it is also necessary to determine the maximum variations of basic traffic characteristics (average and maximum).

To make this algorithm properly applicable in network environment it is necessary to perform previous processing of historical data, in order to obtain initial values of key parameters.

Based on the proof lent by the obtained results it can be concluded that the choice of EWMA parameters significantly affects the operation of this algorithm in network environment. Therefore, the optimization process of parameters before the application of the algorithm is of particular importance.

Bibliography

[1] J. Cohen, Statistical power analysis for the behavioral sciences (2nd ed.), Lawrence Erlbaum Associates, Hillsdale, New Jersey, 1998.

[2] J.S. Hunter, The exponentially weighted moving average, Journal of Quality Technology 18: 203-210, 1986.

[3] J.M. Lucas, M.S. Saccucci, Exponentially weighted moving average control schemes: Properties and enhancements, Technometrics 32, 1-29., 1990.

[4] S.W. Roberts, Control Chart Tests Based on Geometric Moving Averages, *Technometrics*, 1959.

[5] Ye et al., Computer Intrusion Detection Through EWMA for Autocorrelated and Uncorrelated Data, *IEEE Transactions on Reliability* vol. 52, No. 1, 2003.

[6] G. Fengmin, Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection, *White Paper, McAfee Security*, 2003

[7] S. Sorensen, Competitive Overview of Statistical Anomaly Detection, *White Paper, Juniper Networks*, 2004.

[8] V. A. Mahadik, X. Wu and D. S. Reeves, Detection of Denial-of-QoS Attacks Based on χ^2 Statistic And EWMA Control Charts, *http://arqos.csc.ncsu.edu/papers/2002-02-usenixsec-diffservattack.pdf*

[9] A. S. Neubauer, The EWMA Control Chart: Properties and Comparison with other Quality-Control Procedures by Computer Simulation, *Clinical Chemistry,* *http://www.clinchem.org/cgi/content/full/43/4/594*

[10] D. Seibold, Enterprise Campus Security-Addressing the Imploding Perimeter, *http://www.itsa.ufl.edu/2003/presentations/IntSec.ppt*

[11] A. Vasilios, S. and F. Papagalou, Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks, *http://www.ist-scampi.org/publications/papers/siris-globecom2004.pdf*

[12] J. Viinikka and H. Debar, Monitoring IDS Background Noise Using EWMA Control Charts and Alert Information, *http://viinikka.info/ViiDeb2004.pdf*

[13] Y. Zhao, F. Tsung and Z. Wang, Dual CUSUM Control Schemes for Detecting a Range of Mean Shifts, *IEEE Transactions, http://qlab.ieem.ust.hk/qlab/download/papers/paper%2035.pdf*, 2005

[14] Engineering Statistics Handbook-EWMA Control Charts, *http://www.itl.nist.gov/div898/handbook/pmc/section3/pmc324.htm*

[15] Engineering Statistics Handbook−Single Exponential Smoothing, *http://www.itl.nist.gov/div898/handbook/pmc/section4/pmc431.htm*

[16] Savannah State University, Office of Institutional Research & Planning, *http://irp.savstate.edu/irp/glossary/correlation.html*

[17] P. Čisar, S. Maravić Čisar, A first derivate based algorithm for anomaly detection, *International journal of computers, communications & control, 3(S):238-242, 2008*

[18] J. Mina, C. Verde, Fault Detection for Large Scale Systems Using Dynamic Principal Components Analysis with Adaptation, *International journal of computers, communications & control, 2(2):185-194, 2007..*

Petar Čisar was born on September 08, 1965. He graduated at the Faculty of Electrical Engineering in Belgrade. Master's study completed in information engineering at the Faculty of Economics in Subotica. Currently works on PhD thesis. The spheres of his interest are mobile technologies, as well as the development of security methods in network environments.

Saša Bošnjak was born on December 31, 1961. He is a associate professor of Computer Science at the Faculty of Economics Subotica. He holds a range of courses in information engineering. His research interests are database, software development, computer networks, reuse methodology, ebusiness and internet technology. He earned a PhD degree in Information System Faculty of Economics Subotica in 1995.

Sanja Maravić Čisar was born on August 03, 1970. She graduated at the Faculty of Electrical Engineering in Belgrade. Master's study completed at the Technical Faculty in Zrenjanin. She works as lecturer at Subotica Tech at following courses: Visual programming, Object-oriented based programming, JAVA and Multimedia systems. Currently works on PhD thesis.