Utilization of Statistical Control Charts for DoS Network Intrusion Detection

Dimitris Sklavounos[1], Aloysius Edoh[2], George Paraskevopoulos[1]
[1]AMC College, 74 Sorou St, Amarousio 11525, Athens
[2]University of East London, 4-6 University Way, London E16 2RD
dsklavounos@mitropolitiko.edu.gr, gparsk@amc.edu.gr, edoh@uel.ac.uk

ABSTRACT

The present work proposes a new method for denial of service (DoS) intrusion detection, by utilizing two types of statistical control charts on the UDP and ICMP source bytes. The utilized control charts are: the tabular cumulative sum (CUSUM) chart and the exponential weighted moving average (EWMA) chart. Both mechanisms are applied on the captured source bytes of the aforementioned protocols of the experimental dataset NSL-KDD. Two intrusion scenarios were evaluated. In the first scenario intrusion occurred at a set time instance in the UDP packets in a first case, while in the second case the intrusion occurred in UDP and ICMP packets as they were examined in a concurrent manner. In both cases, a shift in the source bytes mean value took place after the intrusion and this was clearly depicted in the CUSUM chart. In the second scenario several intrusions occurred at various time instances in the above protocols' packets which have been clearly depicted in the EWMA chart. Thus, the intrusion detection in both scenarios was successfully achieved.

KEYWORDS

DoS intrusion detection, CUSUM chart, EWMA chart, NSL-KDD Dataset

1 INTRODUCTION

Denial of service (DoS) and its distributed type (DDoS) have been very serious security threats in computer systems and networks for several years. Although many research works have been carried out with satisfactory results, it continues to retain research interest in new detection methods. DoS attacks are very dangerous for systems and networks because they can cause serious delays in accessing servers and other resources due to the packet flooding. This means that in many cases servers must be shut down that causes huge problems in serviceability, especially in real-time applications such as e-commerce or banking [1].

A valuable contribution to research for the detection and confrontation of DoS and DDoS intrusions was the recording of network data, which has created very useful datasets like the Defence Advanced Research Projects Agency (DARPA) 1998 dataset and the later versions: the Knowledge Discovery and Data mining Competition (KDDCup) 1999 dataset and the NSL-KDD. These datasets were created to be utilized by the American Air Force and they have been widely used to evaluate performance of Intrusion Detection Systems (IDS).

The proposed method in the present work utilizes the NSL-KDD dataset which represents the latest version, focusing on the "source bytes" attribute of UDP and ICMP packets in order to achieve detection of DoS intrusion. Considering that the network is under normal operation (no attacks involved), in a certain training period where the mean value (μ_0) of the source bytes may be estimated. This value is set as the target mean for both types of the applied control charts.

For the CUSUM chart: assuming that the UDP and ICMP source bytes are normally distributed, with mean μ_0 and standard deviation σ. If after intrusion there is a shift in the mean value (μ_1) and $\mu_0 > \mu_1$ or $\mu_0 < \mu_1$ then the detection will be successfully achieved.

For the EWMA chart μ_0 represents the starting value of the sequence of estimation of the exponential weighted moving average ($\mathrm{EWMA_i} = \mathrm{Z_i}$) .

The rest of the paper is organized as follows: Section 2 presents the related work on intrusion detection, Section 3 presents the methodology including the theoretical elements of the utilized control charts, the experimental dataset and the proposed method. Section 4 contains the evaluation of the results and finally Section 5 presents the conclusion and further work.

2 RELATED WORK

Several research works have been carried out focusing on the intrusion detection in networks and systems. Indicative related works are the following: The authors in [2] proposed a scheme for detecting distributed DoS attacks and their sources, especially when there are multiple attacks. Using a non-parametric CUSUM algorithm, proposed by Wang, they monitor the server traffic for high increase of requests coming from new IP-addresses. This situation indicates a fact of attack. The authors in [3] evaluated two anomaly detection algorithms (an adaptive threshold algorithm and a CUSUM change point detection algorithm), for detecting TCP SYN flood attacks. The main goal of the research focuses on how the parameters of the algorithms and the characteristics of the attacks affect the performance of detection systems like the above. The work in [4] focuses on the utilization of simple threshold detection and CUSUM change point detection algorithms for pin pointing anomalies in the signal to noise ratio. The main task of the work is to specify the balance between performance and intelligence. In [5] the authors proposed a simple and robust mechanism, called Change-Point Monitoring (CPM), to detect DoS attacks. The work utilizes the correlation between requests and replies of the internet protocol behaviour, which is being destroyed from the attacks. The non- parametric CUSUM algorithm detects deviations from normal protocol behaviours caused by DoS attacks. In [6] the authors have done a comparative work of detecting SYN floods in DoS attacks. The comparison is made between three commonly monitoring charts: the Shewhart chart, the CUSUM chart and the EWMA chart. The study was conducted using the 1999 DARPA dataset. One of our previous works [7] was dealing with the same type of control charts (CUSUM and EWMA) which were applied on the TCP packets for R2L intrusion detection. A limitation stated, which concerned both detection techniques (control charts) was that the examined TCP source bytes sizes were in the range of (0 - 1000). The authors in [8] have proposed an adaptive algorithm by utilizing EWMA chart in order to test if the traffic of packets exceeds a particular threshold over a given interval. The value of the threshold is adaptively set based on the mean number of packets as it has been computed from traffic measurement.

The work in [9] provides a multi-tier method for identifying and analyzing network intrusions. First of all, they create accurate patterns to detect and then categorize attacks. This was achieved with the use of reliable detection algorithms and categorization techniques like the Support Vector Machine (SVM) and the discrete wavelet transform (DWT) which is a signal processing technique. Finally they use iPCA, a tool which visualizes the above analysis for further understanding. The study in [10] focuses on increasing the accuracy and detection-time of network intrusion detection models. A hybrid approach of two parts has been proposed to elaborate the original NSL-KDD dataset as follows: in the first part, by applying the Vote algorithm the data was filtered in order to select the important features and in the second part a classification was made by applying a hybrid algorithm consisting of several classifiers.

3 METHODOLOGY

The proposed method is based on the idea of detecting shifts of the normal process of the UDP and ICMP source bytes during operation, when DoS attacks take place. Hence, the tabular Cumulative sum

(CUSUM) as well as the Exponential Weighted Moving Average (EWMA) control charts were evaluated and utilized for this purpose [11], [12].

3.1 The Tabular CUSUM Control Chart

The utilized CUSUM control chart in the present work is a type of tabular, with individual observations and it works as follows:
Assuming a normal distribution of a random variable X_i with mean μ_0 and a known or estimable standard deviation of σ. The Standard deviation σ is the square root of the variance σ^2 which is equal to:

$$\sigma^2 = \frac{\sum(x_i-\mu)^2}{N} \quad (1)$$

When the process is under control both moments (μ_0 and σ) of the distribution are maintained constant. The mean μ_0 may be taken as the target value of the quality characteristic X. During the operation of the tabular CUSUM chart, two statistics: the C_i^+ and C_i^- are applied to accumulate the deviations from μ_0. C_i^+ accumulates the deviations above target while C_i^- the deviations below target and they are estimated as:

$$C_i^+ = max[0, x_i - (\mu_0 + k) + C_{i-1}^+] \quad (2)$$

and

$$C_i^- = max[0, (\mu_0 - k) - x_i + C_{i-1}^-] \quad (3)$$

Initially $C_0^+ = C_0^- = 0$.

k is the reference value and it is estimated by:

$$k = \frac{|\mu_1 - \mu_0|}{2} \quad (4)$$

where μ_1 is the mean of the out of control values. $H = h * \sigma$ is the decision interval which means that if either of the two statistics $C_i^+$and C_i^- exceeds the value of H, then the process is out of control. Two reasonable values of h may be $h = 4$ or $h = 5$ [13].

3.2 The EWMA Control Chart

The EWMA control chart belongs to the statistical techniques for process control, like the Shwehart and the Cumulative sum (CUSUM) charts. This is often used to detect small to moderate shifts in a process and its statistic is defined as:

$$\mathrm{EWMA_i} = \mathrm{Z_i} = \lambda \mathrm{X_\iota} + (1-\lambda)\mathrm{Z_{\iota-1}} \quad (5)$$

where λ is the weight assigned to the current observation, it is $0 < \lambda \leq 1$ and it’s called smoothing constant or sensitivity parameter.
As Hunter pointed out in 1986 [14], the closer to zero (0) is the value of λ, the closer to CUSUM chart is the behaviour of the EWMA chart. Whereas, the closer to one (1) is the value of λ, the closer to Shewhart chart is its behaviour.
The starting value $\mathrm{Z_0}$ is set to be equal to the target mean μ_0. The EWMA structure has two control limits, the upper control limit ($\mathrm{UCL_i}$) and the lower control limit ($\mathrm{LCL_i}$) which are defined as:

$$\mathrm{UCL_i} = \mu_0 + \mathrm{L}\sigma\sqrt{\frac{\lambda}{(2-\lambda)}[1-(1-\lambda)^{2t}]} \quad (6)$$

$$\mathrm{LCL_i} = \mu_0 - \mathrm{L}\sigma\sqrt{\frac{\lambda}{(2-\lambda)}[1-(1-\lambda)^{2t}]} \quad (7)$$

where L is a width coefficient between $\mathrm{UCL_i}$ and $\mathrm{LCL_i}$. By varying the values of L and λ the sensitivity of the chart will be affected. In the present work different values of these two parameters were used for the UDP and ICMP source bytes, in order to achieve satisfactory detection. For the UDP source bytes detection, the EWMA chart acted closer to CUSUM chart, while for the ICMP detection acted closer to Shewhart chart as presented in Sections 4.3 and 4.4.

3.3 The NSL-KDD Dataset

The data set used for this work is the NSL-KDD that consists of 42 attributes. It does not contain duplicate instances as they have been removed from the previous version (KDD'99) and so, it represents an improved type of data sets. A number of NSL-KDD data set versions are available: the 20% of the training data identified as “KDDTrain+_20Percent” with 25192 instances, as well as the “KDDtest+” with 22544 instances. The number of attributes in each version is 42 with the 42nd attribute labeled as ‘class’ to indicate whether a given instance is normal connection or an attack [15]. The dataset files have been downloaded from [16]. The dataset used for the evaluation was the "KDDtrain20percent" with 42 attributes where the 42nd attribute named “xattack” contains a numbering which indicates the type of the attack as follows: (1) is the DoS, (2) is the User to Root (U2R), (3) is the Remote to User (R2L), (4) is the Probe and (5) is the normal operation packets. The files are also formatted for the machine learning program “WEKA”.

3.4 Proposed Method

A network that operates normally has been considered as an initial situation, supported with a data recording mechanism. The data recording mechanism captures the required information, which in this case are the source bytes. Assuming that the UDP and ICMP source bytes are normally distributed, with a mean μ_0 and standard deviation σ. Then a case is considered in which at some instance a DoS intrusion occurs in either the UDP or ICMP packets. By applying the CUSUM control chart as described in Sec 3.1, If after the intrusion there is a shift in the mean value (μ_1) and $\mu_0 > \mu_1$ or $\mu_0 < \mu_1$, then the intrusion will be successfully detected.

The above attacking situation has been also detected by the EWMA control chart (Sec. 3.2) by adjusting the weighting factor λ to the current observation, as well the width coefficient L between the upper and lower limits.

For both types of control charts, the calculation of the target mean μ_0 is crucial. Thus, a training period is set in order this value would be computed. A hypothetical training period may be the one in which the UDP and ICMP packets of the NSL-KDD dataset were recorded with the network in normal operation (without attacks involved). Thus, the target mean value was calculated from the entire sequence of the UDP and ICMP source byte values of the whole dataset. Thereafter, two intrusion scenarios were examined: one with CUSUM and one with EWMA control charts. In each scenario, two cases were evaluated: first case with intrusions in the UDP packets and a second case with intrusions in the ICMP packets as presented in Section 4. For the first detection scenario with the use of the CUSUM chart, for both cases the assumption made was, that in an initial stage the network was in a normal operation (with no attacks) for n instances. Afterwards, an attack occurred for a very small number of instances n_1. The target mean for both UDP and ICMP normal source bytes was $\mu_0 = 79$. For the above cases, the CUSUM algorithm of the form:

$$C_i = \sum_{j=1}^{i} (\overline{x_j} - \mu_0) \qquad (8)$$

was applied initially for the detection of the mean shift and then the tabular CUSUM control chart, as described in Sec. 3.1, for more analytical process of the detection.

For the second detection scenario with the use of the EWMA control chart, as described in Sec. 3.2, the same assumption was made that the network was in a normal operation. Thereafter, several attacks were applied at certain time instances where all have been detected by the EWMA chart as presented in Sections 4.3 and 4.4.

4 Evaluation of Results

4.1 CUSUM chart detection of DoS attack based on the UDP packets.

The first stage of the method was the training period for the calculation of the mean value of the UDP source bytes. Thus, the entire set of source bytes instances of the original NSL-KDD dataset were used, considering that the network is in normal operation with no attacks involved. The estimated mean value of the entire UDP source bytes of the training period was $\mu_0 = 79$. The first evaluation was the case where the first 100 instances ($n = 100$) contained source bytes of normal operation, and in sequence with them there were added $n_1 = 3$ instances of attack packets. According to the NSL-KDD dataset, the size of the UDP attacking source bytes is of 28 bytes. This value betrays the emptiness of the packets' payload (data part). As the UDP packets are encapsulated into the IP packets and constitute the data section of it, the value of 28 represents the sum of the bytes of the IP and UDP headers (20B + 8B = 28B). Applying the CUSUM algorithmic test of (eq.8) for 150 instances a change in mean was observed as depicted in Figure 1.

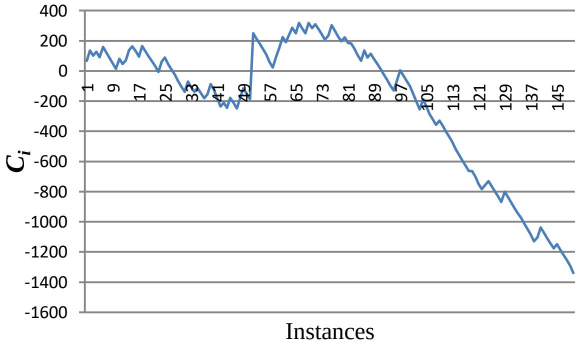

Figure 1. Drift of test statistic of the cumulative sum in (5) with three attack instances after the 100th instance

In cases where n takes a lower value ($n < 100$), the detection will be also achieved, but as the mean of the source byte values is closer to the target mean value the detection is clearer depicted. So, a conservative value of n ($n = 100$) was selected in order for the detection to be clearly achieved and depicted. As observed from the graph in Fig. 1, the drift initially fluctuates around zero, and after instance 97 takes a negative direction. This is due to the downward shift of the mean μ_1 ($\mu_0 > \mu_1$) after the attack.

Furthermore, the statistic in (eq. 3) was applied for 150 instances and it is depicted in Fig. 2. As shown in the graph, the slope of C_i^- from the 100th instance, where the attack occurred, until the 150th, takes a permanently positive direction. This change of the slope is due to the change in mean of the values after 100 and this means that the process is out of control. So, the detection is made.

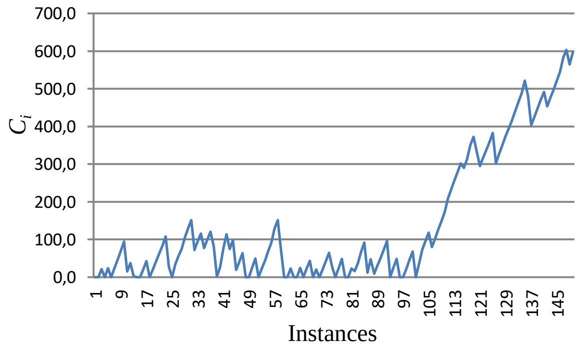

Figure 2. Drift of test statistic of C_i^- in (3) with three attack instances after the 100th instance

Analytically, the out of control mean is estimated as $\mu_1 = \mu_0 + \delta\sigma = 54{,}2$, (where $\delta\sigma = \mu_1 - \mu_2 = 24{,}8$). From (eq. 4) the parameter $k = 12{,}4$ and the interval $H = 4 \times 75 = 300$. At instance 115 comes the first signal for out of control process and a second one comes at instance 117 to 120. From instance 122 until the end of the process all values are greater than 300 and this means that from this point the process is out of control (Table 1).

Table 1. Indicative values of the C_i^- slope of Figure 2

Instances	C_i^-	N
1	0	0
2	0	0
3	21,6	1
…	…	…
…	…	…
…	…	…
114	278,1	13
115	301,7	14
116	290,3	15
117	313,9	16
118	350,5	17
119	372,2	18
120	333,8	19
121	295,4	20
122	317,0	21
123	337,6	22
124	359,3	23
125	382,9	24

126	302,5	25
127	327,1	26
…	…	…
130	395	29
…	…	…
150	596,4	49

At instance 122 the value of $= 21$, so $122 - 21 = 101$ which means that at instance 101 the shift in mean started to be created (Fig. 1). If $H = 5 \times 75 = 375$ is taken, then the first signal for out of control process comes at the instance 125, and then from instance 130 until the end, the process is permanently out of control. This result shows that, the better choice of the decision interval may be the case when $h = 4$.

4.2 *CUSUM chart detection of DoS attack based on the UDP and ICMP packets concurrently.*

The same method with the previous section (Sec. 4.1) was applied for the detection of UDP and ICMP source bytes in a concurrent manner. This is because as it has been observed; both protocols' source bytes size lies within the same range. Examining the ICMP source bytes size in attack classification, a large diversion upwards from the size in normal was showed. Thus, in this case there is an opposite situation from the UDP detection where there was a deviation downwards.

For this concurrent type scenario the detection of the UDP attacks has the same form as the one presented in the previous Section (Sec 4.1) and thus, only the ICMP detection will be presented.

For this detection the same scenario as in Sec 4.1 was applied, as far as the sequence of the instances is concerned.

The CUSUM test of (eq. 8) for the same number of instances (150) showed a change in mean as depicted in Figure 3. This is because there is a positive shift of the mean the statistic C_i^+ (eq. 2) was applied. As depicted in Figure 4, there is a sharp change of the slope after the 100th instance and this indicates the change in the mean. In this case $\mu_0 = 79$ (the mean for both UDP and ICMP source bytes is 79), $\mu_1 = 97{,}5$, $\delta\sigma = 18{,}5$ the parameter $k = 9{,}26$ and the interval $H = 4 \times 115 = 459$.

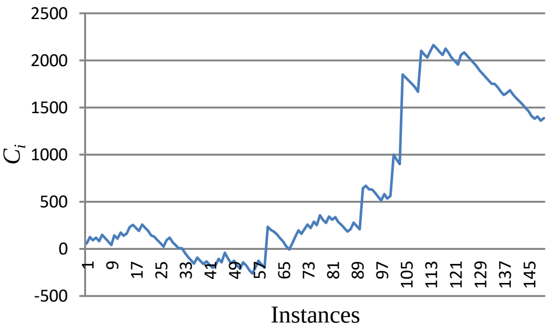

Figure 3. Drift of test statistic of the cumulative sum in (5) with four (2 ICMP & 2 UDP) attack instances after the 100th instance

The first signal for out of control process came at instance 91 until 95 and then from instance 101 until 150 the process was out of control.

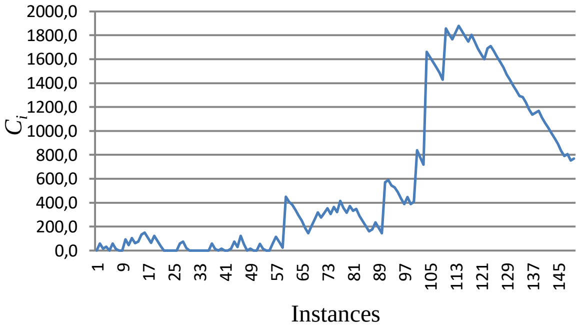

Figure 4. Drift of test statistic in (2) with four (2 ICMP & 2 UDP) attack instances after the 100th instance

From a list of values with the same logic as Table 1 (not quoted here), at instance 101, $N = 46$. Thus, at instance 55 the shift in mean started to be created. For $h = 5$ the decision interval $H = 5 \times 115 = 575$ then the first signal for out of control process comes at instance 92. Then again from instance 101 until the end, the process is permanently out of control. This result leads to the fact that, both values of h (4 or 5) give a decision interval H with the almost the same effectiveness.

4.3 EWMA chart detection of DoS attack based on the UDP packets.

The first stage of the method was the training period for the calculation of the mean value of the UDP source bytes. Hence, the entire set of the UDP source bytes of the original NSL-KDD dataset under normal operation was used. The same consideration is also valid that the network works normally with no attacks involved. The estimated mean value of the entire UDP source bytes in the above range of the training period was $\mu_0 = 79$ with a standard deviation $\sigma = 75$.

The detection of UDP attacks with the EWMA chart may be possible when its behaviour approaches the CUSUM chart. This is because the attacking source bytes value (28 bytes) belongs to the range of values of the normal UDP source bytes and they may be considered as a value of the same distribution. Thus, a sequence of attacking instances (more than one) may be a case of detection as the weighted moving average by a value close to zero, will reaches or exceeds the $\mathrm{LCL_i}$. In equation (5), using a value of $\lambda = 0{,}3$ (a value close to 0) most of the weights are not placed on the most recent values, but on the previews ones instead. Thus, in this kind of attacking situation the value of $\mathrm{Z_i}$ will exceed the lower limit $\mathrm{LCL_i}$ of (eq.7). The sequential attacking instances represent a usual situation according to the NSL-KDD dataset where most of the attacks were of more than one instance. In the present evaluation three attacking instances have been applied as minimum. Again, for greater effectiveness of the EWMA chart, it is also necessary to ignore outliers (values greater than of 200 bytes) since the attacks will be made from the lower control limit (LCLi) of the chart .

With the above limitations the EWMA chart was applied and it is depicted in Figure 5.

The EWMA graph of Figure 5 shows several detected UDP random attacks of the following form: three attacks at instances 22 to 24, four attacks at instances 78 to 81, the attacks at the same instances as in Sec 4.2 (101 to 103), and finally another four attacks at instances 111 to 114. All the attacks were of 28 bytes size. The corresponding values of $\mathrm{EWMA_i} = \mathrm{Z_i}$ for the above attacking instances are shown in Table 2.

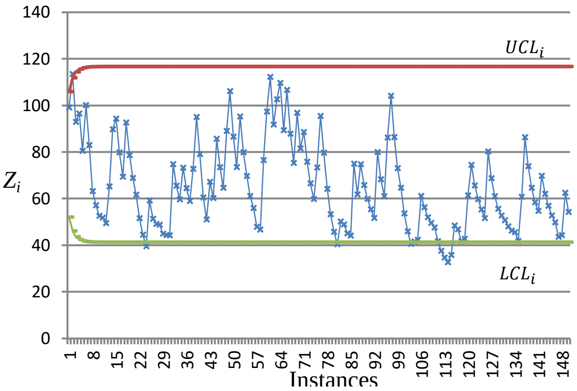

Figure 5. Drift of test statistic of the EWMA with UDP attacks at instances: 22 to 24, 78 to 81, 101 to 103 and 111 to 114

Table 2. Values of Z_i at the attacking instances

Attacking instance	Detection instance	Z_i	LCL_i
22 - 24	24	40	41
78 - 81	81	40	41
101 - 103	103	40	41
111 - 114	112	38	41
111 - 114	113	35	41
111 - 114	114	33	41

As depicted in Figure 5, all the normal UDP source bytes at all instances are located within the two limits, while the attacking bytes at the aforementioned instances are beyond the lower control limit *(LCL_i).*

The values of the weight λ as well as the width coefficient L are: $\lambda = 0{,}3$ and $L = 1{,}2$. These values provided the appropriate sensitivity to the chart to achieve detection of the attacks. The upper and lower limits are: $UCL_i = 117$ and $LCL_i = 41$.

It is worth commenting that the formation of the values of Z_i in the last two sequences of attacks (101 – 102 and 111 – 114). As shown in Table 1 the value of Z_i at the instances 112 to 114 is exceeding further to the $LCL_i = 41$, with the values of 38, 35 and 33 respectively. This signifies the fact that, using the above values of λ and L, the closer in time the attacks are, the more effective the detection may be.

4.4 *EWMA chart detection of DoS attack based on the ICMP packets.*

The first stage of the method was the training period for the calculation of the mean value of the ICMP source bytes. Hence, the entire set of the ICMP source bytes of the original NSL-KDD dataset under normal operation was used. The same consideration is also valid that the network works normally with no attacks involved. The estimated mean value of the entire ICMP source bytes in the above range of the training period was $\mu_0 = 79$ with a standard deviation $\sigma = 60$.
The EWMA graph of Figure 6, besides the attacks at the same instances as in Sec 4.2, it also shows several detected ICMP random attacks of the following form: One 520 bytes attack at instance 24, one 520 bytes attack at instance 44, another one of the same value at instance 69, two 520 bytes attacks ay instances 91 and 92 followed by another one of the same value at instance 100 and finally one attack of 1032 bytes at instance 113.

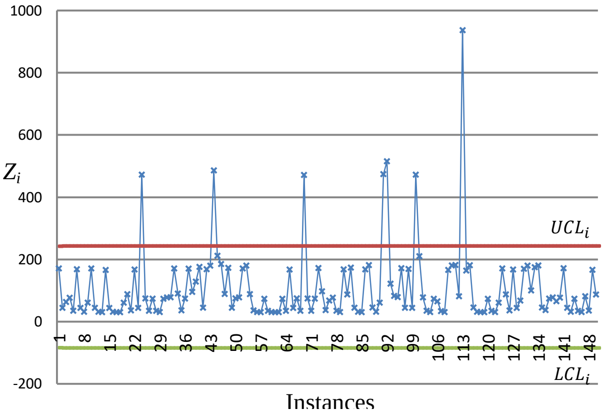

Figure 6. Drift of test statistic of the EWMA with ICMP attacks at instances: 24, 44, 69, 91, 92 and 100

The corresponding values of $EWMA_i = Z_i$ (eq. 5) for the above attacking instances are shown in Table 3.

Table 3. Values of Z_i at the attacking instances

Attacking instance	**Detection instance**	$\boldsymbol{Z_i}$	$\boldsymbol{UCL_i}$
24	24	472	243
44	44	486	243
69	69	471	243
91	91	474	243
92	92	515	243
100	100	472	243
113	113	937	243

As depicted in Figure 6, all the normal ICMP source bytes at all instances are placed within the two limits, while the attacking bytes at the aforementioned instances are beyond the upper control limit *(UCL$_i$)* of equation (6).
The values of the weight λ as well as the width coefficient L are: $\lambda = 0{,}9$ and $L = 3$. The upper and lower limits are: $UCL_i = 243$ and $LCL_i = -85$. As the value of λ is close to zero (0), the behaviour of the EWMA chart is close to Shewhart.

5 Conclusions and Future Work

A new DoS intrusion detection method has been proposed. The method was based on the source bytes of the UDP and ICMP protocols as they have been recorded in the NSL-KDD dataset. The mechanisms utilized for the detection were: the tabular CUSUM chart, as well as the EWMA chart which gave satisfactory results since they successfully detected the intrusions in both UDP and ICMP packets. The EWMA chart detected the attacks on the UDP packets after being adjusted (with certain set of values of λ and L) so that its behaviour was closer to CUSUM and for the ICMP detection closer to Shewhart chart.
Further to this work the cases of moving average as well as subgroup averages will be examined for the intrusion detection. Also, detection evaluation will be carried out on the TCP packets by applying statistical normalization on the bytes' sizes and new methods of detection will be proposed by utilizing possible upcoming newer versions of datasets.

4 REFERENCES

[1] Hovav, Anat, and John D'Arcy, "The impact of denial-of-service attack announcements on the market value of firms", Risk Management and Insurance Review 6.2 (2003):97-121.

[2] Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao, "Detecting Distributed Denial of Service Attacks Using

Source IP Address Monitoring", In Proceedings of the Third International IFIP-TC6 Networking Conference Networking 2004.

[3] Vasilios A. Siris, Fotini Papagalou, "Application of anomaly detection algorithms for detecting SYN flooding attacks", Computer Communications 29 (2006) 1433–1442, Elsevier.

[4] Alexandros G. Fragkiadakis, Vasilios A. Siris, and Nikolaos Petroulakis, "Anomaly-Based Intrusion Detection Algorithms for Wireless Networks", E. Osipov et al. (Eds.): WWIC 2010, LNCS 6074, pp. 192-203, 2010.

[5] Haining Wang, Danlu Zhang, Kang G. Shin, "Change-Point Monitoring for Detection of DoS Attacks", IEEE Transactions on Dependable and Secure Computing (Volume: 1, Issue: 4, Oct.-Dec. 2004).

[6] Benamar Bouyeddou, Fouzi Harrou, Ying Sun, Benamar Kadri, "Detecting SYN flood attacks via statistical monitoring charts: A comparative study", Boumerdes (ICEE-B), 2017 5th International Conference.

[7] Dimitris Sklavounos, Aloysius Edoh, Markos Plytas, "Statistical Approach Based on EWMA and CUSUM Control Charts for R2L Intrusion Detection", Cybersecurity and Cyberforensics Conference (CCC), 2017, IEEE computer society.

[8] Petar Cisar, Sasa Bosnjak, Sanja Maravic Cisar, "EWMA Based Threshold Algorithm For Intrusion Detection", Computing and Informatics, Vol. 29, 2010, 1089–1101

[9] Soo-YeonJi, Bong-Keun Jeong, Seonho Choi, Dong Hyun Jeong, "A multi-level intrusion detection method for abnormal network behaviours", Journal of Network and Computer Applications 62 (2016) 9–17.

[10] Shadi Aljawarneha, Monther Aldwairia, Muneer Bani Yasseinaa, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model", Journal of Computational Science (2017).

[11] V. V. Koshti, "CUMULATIVE SUM CONTROL CHART", International Journal of Physics and Mathematical Sciences ISSN: 2277-2111 (Online).

[12] Duttadeka, S, Gogoi, B, "A Study on Exponentially Weighted Moving Average Control Chart with Parametric and Nonparametric Approach", Journal of Agriculture and Life Sciences ISSN 2375-4214.

[13] D. R. Prajapati, "Effectiveness of Conventional CUSUM Control Chart for Correlated Observations", International Journal of Modeling and Optimization, Vol. 5, No. 2, April 2015.

[14] Hunter, J. Stuart, "The Exponentially Weighted Moving Average" (1986, ASQC) Princeton, NJ, Journal of quality technology, Vol. 18, No. 4, Oct. 1986.

[15] Preeti Aggarwala, Sudhir Kumar Sharma, "Analysis of KDD Dataset Attributes- Class wise For Intrusion Detection" 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015), Elsevier

[16] https://github.com/FransHBotes/NSLKDD-Dataset, (10/7/2016).