Performance of EWMA and ANN-based Schemes in Detection of Denial of Service Attack

Y Minn¹ and A Hassan¹,²

¹Industrial Engineering Program, School of Mechanical Engineering, Faculty of Engineering Universiti Teknologi Malaysia, 81310, Johor Bahru Malaysia
²correspondence author: adnan@utm.my

Abstract. To ensure successful implementation of cyber-physical systems, industries require computer networks to be protected from malicious attacks. Despite various intrusion detection techniques being proposed by researchers, computer networks are still vulnerable to attacks. As new attacks becoming more complicated, more research is needed to develop more effective and reliable intrusion detection schemes. This study investigated the exponentially weighted moving average control charting technique for detection of malicious denial of service (DoS) traffic and compared it with artificial neural network (ANN) based scheme. Eight features from the Benchmark KDD Cup99 computer network datasets were extracted and their respective ARL₁ and false alarm rate were evaluated. The results suggest that EWMA technique is effective only for selective features and the ANN-based scheme is relatively consistent in handling variability in traffic data. This study opens new opportunities for further investigation to enhance performance of the proposed schemes.

1. Introduction

As manufacturing and supply chain activities move towards globalization, many industrial processes are connected internationally to Internet and computer networks. To ensure successful implementation of cyber-physical computer networks, industries demand safer computer networks from malicious attacks. Despite advances in the technology, computer networks are still vulnerable to malicious traffics while the volume of traffic data is increasing exponentially. There are many categories of computer network attacks, however, for simplicity this paper limits the discussion only on denial of service (DoS) attack. DoS attack appears when the perpetrator attempts to intrude the computer network by disrupting a host connected to the Internet. This may be accomplished by excessively loading the targeted machine with unnecessary requests. As such, the server will become overloaded and lead to denial of service to genuine users [1].

Several researchers have investigated statistical techniques for intrusion detection. Ye et al. [2] explored the effectiveness of EWMA techniques using different parameter settings. Cisar et al. [3] studied the feasibility of EWMA technique and fuzzy logic for detecting malicious traffics. Aggarwal [4] investigated six feature selection algorithms and reported their relative performance. Kabir et al. [5] reported that some researchers have used machine learning and statistical approach. Recently, Moustafa et al. [6] argued that machine learning could be one of the most effective tools for anomaly detection. Despite significant research works in this area, a huge challenge still exists. There is a need for a more effective and reliable intrusion detection schemes.
The dynamic nature of the computer attacks generates new variants to the existing reference profiles and causes the existing detection schemes to become ineffective. Early detection of intrusions is critical to avoid catastrophic failures and financial loses. To our knowledge, there has been limited work focusing on EWMA for feature selection and detection of malicious computer network traffic. The objective of this study is to address this gap and to explore the effectiveness of EWMA statistical features as input to the ANN-based scheme. The remaining of the paper is organized into five subsections namely, research methodology, EWMA control chart scheme, ANN-based Scheme, discussion, and finally conclusion.

2. Research methodology
This research was implemented in three main stages namely: (i) feature screening using histogram and time series plot (ii) DoS detection using EWMA control chart, and (iii) DoS detection using ANN. A comparative analysis was done to evaluate the relative merit of these two schemes for DoS detection.

2.1 Data source and feature selection
It is challenging to obtain sufficient real-life network intrusion detection data [7]. As such, the source of traffic data adopted in this study was the widely accepted de facto benchmark datasets from the KDDCUP99 which is publicly accessible online [8]. Only 10% of the data was used in this study from the original 4,940,000 connection records. Approximately 20% of these were normal traffic data, and 80% were malicious data. This database comprised of 41 network traffic features where the attacks were categorized into four classes in addition to normal traffic data. As noted above, this study only focused on Denial of Service (DoS) attack category. Symbolic and text features were excluded in the features screening. A total of one hundred normal traffic training data for each feature type were used to build reference normal profiles. On the other hand, the testing data set for each feature type consisted 60 normal traffics and subsequently followed by 40 malicious attack data. The testing datasets were injected with new unseen DoS attacks in addition to the existing attack data.

Histogram and time series plots were employed to visually analyse the shapes of traffic features and to identify any sudden changes in the time series data. This approach was used during feature selection stage. This is an important step in this study since an effective feature set would significantly contribute to a better performance for both EWMA and ANN-based schemes. Section 3 elaborates further on this.

2.2 Proposed intrusion detection schemes
Two approaches for intrusion detection refers to as exponentially weighted moving average (EWMA) scheme and ANN-based scheme were developed and tested. The EWMA statistical approach is widely used in manufacturing process monitoring where it has the capability to detect small shift in process mean. In this study, this statistical technique was used to detect anomalous changes in computer network usage pattern. Each of the selected quantitative feature was transformed into EWMA ($Z_i$) statistics where $Z_i = \lambda x_i + (1- \lambda) Z_{i-1}$, parameter $\lambda$ is a smoothing constant and $x_i$ is an observation value. EWMA statistics integrate previous and current traffic data using a weighted average where the importance of older data decreases exponentially as it gets older [9]. The control limits for the EWMA control chart were constructed according to equation (1).

$$\text{Control Limits} = \bar{x} \pm L\sigma \sqrt{\frac{1 - (1 - \lambda)}{2 - \lambda}}$$

$L$ is a constant typically set slightly less that 3 for small values of $\lambda$. Its selection is critical since it influences the control limits. The rational subgroup standard deviation ($\sigma$) and the central line ($\bar{x}$) were estimated from a stable or non-attack traffic.

Then, artificial neural network (ANN) scheme was developed, trained and implemented where the minimal features subset selected in section 2.1 was used as input data representation. Further discussion on ANN-based scheme is provided in section 4.
2.3 Performance measure
The performance of the investigated schemes was assessed based on average run length (ARL) and false alarm rate (FAR). The ARL measures the speed to detect an attack and it should be as quick as possible. A smaller ARL indicates a better performance [11]. FAR measures a probability for normal usage traffic to be wrongly detected as an attack [9]. The FAR was determined by equation (2).

\[
FAR = \frac{\text{Total False Alarms}}{\text{Total Normal Traffic}} \times 100.
\] (2)

The accuracy of detection is measured as percentage ratio between a summation of True Positive (TP) and True Negative (TN) against a summation of TP, TN, False Positive (FP) and False Negative (FN) as shown in equation (3).

\[
\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \times 100
\] (3)

EWMA was chosen in this study since this statistical technique has been proven effective in monitoring variability and deviation in manufacturing processes. Furthermore, EWMA does not require the data to be normally distributed [14]. The multilayer perceptron ANN was chosen since it has been effectively applied in diverse areas such for product quality classification, banking fraud detection and biometric verification among others.

3. EWMA control chart scheme for detection of DoS attack

3.1 Histogram and time series plot for feature selection
It is critical to reduce the dimensionality of computer network traffic data by removing redundant features and trivial information. For this purpose, a total of 100 time series data comprising 60 normal traffic and 40 attack traffic for each feature type were used for plotting histograms and time series charts. The purpose of these plots is to demonstrate distribution shapes that can differentiate between normal and attack traffics. Examples of a histogram plot for Feature C and control chart time series plot for Feature H are given in figures 1 and 2. The histogram plots in figure 1 clearly show that feature C can distinguish between normal traffic and attack traffic. Meanwhile, figure 2 clearly illustrates that after the 60th observation, the attack traffic begins to emerge. All the alternative traffic features were plotted into these graphs before a minimal significant features subset was decided. Finally, eight features were selected and used in the detection of malicious traffic, namely, features dst_bytes (A), logged_in (B), count (C), srv_count (D), dst_host_count (E), dst_host_srv_count (F), dst_host_same_srv (G), and dst_host_same_src_port_rate (H).

![Figure 1. Histogram plot for Feature C for normal traffic and attack traffic data.](image-url)
3.2 EWMA normal traffic profile
The normal profiles of $Z_i$ for the selected features were plotted on EWMA control charts derived from equation (1). The procedure for preparing the EWMA reference profiles is summarised as below:

i. Select representative significant features for traffic monitoring and detection
ii. Select training data, limited to normal traffic data
iii. Select design parameters for EWMA control chart ($\lambda$ and $L$)
iv. Calculate $Z_i$ for the selected features in step (i)
v. Calculate the target mean and standard deviation
vi. Established the upper control limit (UCL) and lower control limit (LCL) using equation (1)

Reference normal traffic profile is established
The parameter values $L = 2.814$ and $\lambda = 0.1$ were used in the establishment of EWMA normal traffic profiles. These values were recommended by Lucas and Saccucci as noted in Montgomery [10]. At this setting, the expected $\text{ARL}_0 \approx 500$ for normal traffics and $\text{ARL}_1 = 10.3$ for malicious traffics having estimated mean shifts of one $\sigma$.

3.3 Procedure to detect DoS attack
The procedure for monitoring and detection of DoS malicious traffics is as listed below:

i. Extract representative features from unknown network traffic data
ii. Calculate $Z_i$ for the selected features in (i)
iii. Compare $Z_i$ to the UCL and LCL of the reference profile as noted in section 3.2 (step vii)
iv. If $Z_i$ exceeds either UCL or LCL, an anomaly DoS attack is detected. Otherwise, the traffic is a legitimate usage.

The above procedure was implemented during testing phase using 60 normal usage traffic and followed by 40 continuous DoS attack traffic.

3.4 Performance of EWMA Scheme
Figures 3 to 10 show results of malicious DoS attack as monitored using EWMA ($Z_i$) for the selected eight representative features. All the figures show the selected features were able to clearly differentiate between normal usage traffic and malicious attack traffic. All the graphs show attack traffic emerges starting from 60th observation onwards. The scale between UCL and LCL for each feature varies widely. This has resulted the $Z_i$ values for Features $C$ and $D$, and their respective control limits were invisible as shown in figures 5 and 6. Features $B$, $C$, $D$, $F$ and $G$ were capable to rapidly signalled the malicious traffic with $\text{ARL}_1$ less than 5. In particular, Features $C$ and $D$ detected the attack instantly as it emerged ($\text{ARL}_1 = 1$). However, these two features generated high FAR ($C=38\%$, $D=33\%$).
Figure 3. Monitoring and detection of DoS attack based on feature \textit{dst bytes} (A).

Figure 4. Monitoring and detection of DoS attack based on feature \textit{logged\_in} (B).

Figure 5. Monitoring and detection of DoS attack based on feature \textit{count} (C).

Figure 6. Monitoring and detection of DoS attack based on feature \textit{svc\_count} (D).

Figure 7. Monitoring and detection of DoS attack based on feature \textit{dst\_host\_count} (E).
Figure 8. Monitoring and detection of DoS attack based on feature \( dst\_host\_svc\_count (F) \).

Figure 9. Monitoring and detection of DoS attack based on feature \( dst\_host\_same\_srv\_rate (G) \).

Figure 10. Monitoring and detection of DoS attack based on feature \( dst\_host\_same\_src\_port\_rate (H) \).

The performance of EWMA scheme in term of ARL\(_1\) and FAR are summarized in table1. Features A (3%), B (7%) and H (5%) resulted in relatively low FAR compared to Features C, D, E, F and G.

Table 1. Performance of EWMA scheme.

| Feature | \( dst\_bytes (A) \) | \( logged\_in (B) \) | \( count (C) \) | \( srv\_count (D) \) | \( dst\_host\_count (E) \) | \( dst\_host\_srv\_count (F) \) | \( dst\_host\_same\_srv\_rate (G) \) | \( dst\_host\_same\_src\_port\_rate (H) \) |
|---------|----------------------|----------------------|-----------------|----------------------|--------------------------|-------------------------------|--------------------------|--------------------------|
| FAR     | 3%                   | 7%                   | 38%             | 33%                  | 39%                      | 17%                          | 21%                      | 5%                       |
| ARL\(_1\) | 12                   | 3                    | 1               | 1                    | 9                        | 4                            | 4                        | 7                        |

4. ANN-based scheme for detection of DoS attack

4.1 Design and Training of ANN-Based Scheme

A multi-layer perceptron (MLP) neural network was adopted in this study to recognise and differentiate between normal use and DoS attack traffic. The design and experimental procedure in
this section was adopted from Hassan et al. [12]. The ANN structure had an input layer with 8 nodes to accommodate all the eight selected features. The hidden layer comprised 20 nodes and the output layer was allocated one node. A supervised learning approach based on trainlm (Levenberg-Marquardt) algorithm was used. A total of 400 traffic data was used where 70% allocated for training, and 30% for validation and in-training testing. The ANN-based scheme was developed and implemented using the ANN toolbox available in MATLAB®2017a.

The key steps in the development of ANN-based scheme involved the selection of MLP structure (input, hidden and output nodes), transfer function, and training algorithm. Since the feature values vary widely, they were normalised to be within [-1, 1] range. The training stopping criteria were set to a maximum of 50 epoch with an error goal of 0.1 to avoid overfitting. The trained ANN scheme was accepted when the mean squared error during the training phase was less than 0.01. Later, the performance of trained ANN scheme was tested using two testing sets having 200 fresh traffic data each including unseen new types of DoS attacks.

4.2 Performance of ANN-based Scheme
The trained ANN classifier was used to detect the malicious attack traffic and normal use traffic. Its performance was evaluated in term of detection accuracy, sensitivity, specificity and FAR. The overall performance of ANN-based scheme when tested using two different data sets is given in table 2. This result suggests that the ANN-scheme performed relatively better on testing set 1 compared to testing data set 2. This suggest that more fine tunings are needed to enhance its robustness and consistency in performance.

Table 2. Performance of ANN-based scheme.

| Testing set | Accuracy | Sensitivity | Specificity | FAR  |
|-------------|----------|-------------|-------------|------|
| 1           | 82.3%    | 92.5%       | 72.0%       | 17.8%|
| 2           | 80.7%    | 95.1%       | 66.3%       | 19.3%|

5. Discussion
The traditional univariate EWMA control chart technique was able to monitor one individual feature at any single instance, while the ANN-based scheme was capable to concurrently employed all the eight features. Table 3 provides a limited comparison between EWMA and ANN approaches for the FAR performance. The results suggest that the FAR for EWMA scheme varies widely depending on the specific feature implemented. Feature A (dst_bytes) scored relatively good FAR (3%) but poorer ARLₜ (12) compared to Feature B (logged_in) with FAR (7%) and ARLₜ (3). Overall, the ANN-based scheme scored a moderate and relatively consistent FAR performance (17.8 – 19.3%). The above results suggest that the EWMA scheme has capability to rapidly detect sudden change especially for features C (count), and D (srv_count). However, these features resulted in high FAR.

Table 3. FAR performance for EWMA and ANN-based Schemes

| EWMA Scheme | Feature Label | A  | B  | C  | D  | E  | F  | G  | H  |
|-------------|---------------|----|----|----|----|----|----|----|----|
| FAR         | 3%            | 7% | 38%| 33%| 39%| 17%| 21%| 5% |
| ANN-based   | FAR (test set 1) | 17.8% |    |    |    |    |    |    |
| Scheme      | FAR (test set 2) | 19.3% |    |    |    |    |    |    |

A comparison between results from this study and Idhammad et al. [13] suggests that the ANN-based scheme is comparable to the later in term of accuracy (except HSV-ANN) and sensitivity as summarised in table 4. However, further improvement is needed to reduce the FAR and increase the specificity measures.
Table 4. Performance comparison between this study and Idhammad et al. [13]

| Authors     | Scheme     | Accuracy (%) | Sensitivity (%) | Specificity (%) | FAR (%) |
|-------------|------------|--------------|-----------------|-----------------|---------|
| Idhammad et. al [13] | u-MLP      | 83.5         | 90.0            | 93.0            | 11.0    |
|             | NSL-ANN    | 81.2         | 96.0            | 70.0            | 32.0    |
|             | HSV-ANN    | 92.0         | -               | -               | 15.0    |
| This study  | ANN (test data 1) | 82.3   | 92.5            | 72.0            | 17.8    |
|             | ANN (test data 2) | 80.7   | 95.1            | 66.3            | 19.3    |

Results from this study should be treated with cautious since more tests are needed using bigger data size before the above findings can be generalized.

6. Conclusion
The preliminary findings as presented above indicate that the EWMA and ANN-based schemes are promising procedures for detection of malicious computer network traffic. The results show that the EWMA scheme has selective effectiveness where some features are able to give rapid detection (low ARL,) but high false alarm. Generally, feature logged-in is the best among the investigated features. The ANN-based scheme employing eight selected features scored relatively moderate performance with FAR (17.8 – 19.3%) and accuracy (80.7 - 82.3%). Limitations reveal in this study open opportunity for investigation into multivariate EWMA control chart for anomaly detection. ANN-based scheme was found to be more accommodating in handling variability in traffic data. Further research should focus on adaptive schemes for addressing dynamic and changing computer network environment. Development of anomalies detection schemes for cloud network and IoT devices would be a useful future research direction.

Acknowledgements
The authors would like to thank Ministry of Higher Education Malaysia (MOHE) and Research Management Centre (RMC), Universiti Teknologi Malaysia for financial support through UTM FR Grant No: Q.J130000.2551.21H58.

References
[1] Security Tip (ST04-015): Understanding Denial-of-service Attacks 20 Nov 2019 (https://us-cert.cisa.gov/ncas/tips/ST04-015) Retrieved 9 July 2020
[2] Ye N, Vilbert S and Chen Q 2003 Computer intrusion detection through EWMA for autocorrelated and uncorrelated data. IEEE transactions on reliability 52 1 pp 75-82
[3] Čisar P and Čisar S M 2019 EWMA statistics and fuzzy logic in function of network anomaly detection, Electronics and Energetics 32 2 pp 249-265
[4] Aggarwal M 2013 Performance analysis of different feature selection methods in intrusion detection International Journal of Scientific & Technology Research 2 6 pp 225-231
[5] Kabir E, Hu J, Wang H and Zhuo G 2018 A novel statistical technique for intrusion detection systems Future Generat. Comput. Syst 79 pp 303-318
[6] Moustafa N, Hu J and Slay A J (2019) Holistic review of network anomaly detection systems: a comprehensive survey J. Netw. Comput. Appl. 128 pp 33-55
[7] Goonatilake R, Bachnak R and Herath S 2011 Statistical quality control approaches to network intrusion detection International Journal of Network Security & Its Application 3 6 pp 115-124
[8] KDD Cup 1999 Data: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[9] Kadri, F., Harrou, F., Chaabane, S., Sun, Y., & Tahon, C. (2016). Seasonal ARMA-based SPC charts for anomaly detection: Application to emergency department systems. Neurocomputing 173 pp 2102-2114
[10] Montgomery D C 2019 Statistical Quality Control 8th ed Wiley (New York)
[11] Park Y, Baek S H, Kim S H and Tsui K L 2014 Statistical process control-based intrusion detection and monitoring Quality and Reliability Engineering International 30 2 pp 257-273

[12] Hassan A, Baksh M S N, Shaharoun A and Jamaluddin H 2003 Improved spc chart pattern recognition using statistical features International Journal of Production Research 41 7 pp 1587-1603

[13] Idhammad M, Afdel K and Belouch M 2017 DoS detection method based on artificial neural networks Int. J. of Advanced Computer Science and Applications 8 4 pp 465-471

[14] Ye N (2008), Secure computer and network systems: modelling, analysis and design: John Wiley & sons.