2011

Analysis of BGP security vulnerabilities

Muhammad Mujtaba
University of Technology, Sydney

Priyadarsi Nanda
University of Technology, Sydney

DOI: 10.4225/75/57b5493ecd8c9
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

ANALYSIS OF BGP SECURITY VULNERABILITIES

Muhammad Mujtaba and Dr Priyadarsi Nanda
Centre for Innovation in IT Services and Applications (iNext),
University of Technology, Sydney (UTS)
Muhammd.mujtaba@student.uts.edu.au, Priyadarsi.Nanda@uts.edu.au

Abstract

Border Gateway Protocol (BGP) is a dynamic routing protocol in the Internet that allows Autonomous System (AS) to exchange information with other networks. The main goal of BGP is to provide a loop free path to the destination. Security has been a major issue for BGP and due to a large number of attacks on routers; it has resulted in router misconfiguration, power failure and Denial of Service (DoS) attacks. Detection and prevention of attacks in router at early stages of implementation has been a major research focus in the past few years. In this research paper, we compare three statistical based anomaly detection algorithms (CUSUM, adaptive threshold and k-mean cluster) through experiment. We then carry out analysis, based on detection probability, false alarm rate and capture intensity (high & low) on the attacked routers.

Keywords
Statistical Detection Algorithm, IDS (Intrusion Detection System), Network monitoring, Anomaly Detection.

INTRODUCTION

Border Gateway Protocol (BGP) is the de-facto inter-domain routing protocol used across thousands of Autonomous Systems (AS) in the Internet. Internet connectivity plays a vital role in business, universities and government organisations. Large number of attacks on routers can cause misconfiguration and DoS (Denial of Service) attacks (Butler, Farley, McDaniel, & Rexford, 2010; Rick Kuhn 2007; Sengar, Xinyuan, Haining, Wijesekera, & Jajodia, 2009). DoS attack is the major security threat to the internet today, among which, is the TCP SYN flooding, the most common type of attack. The aim of the DoS attack is to consume large amounts of bandwidth (Butler, et al., 2010). Any system connected to the internet and using TCP services are prone to such attacks. Recent studies have shown that an increase in such attacks can cause billions of dollars of revenue loss. Intrusion detection system (IDS) and Intrusion Prevention system (IPS) are the processes used to detect malicious packets and to filter them out from the system. There are several ways to detect and separate malicious packets based on traffic patterns and behaviours. For instance signature-based, statistical-based and hybrid based (Siris & Papagalou, 2004). In this paper we present and evaluate three anomaly detection algorithms for detecting TCP SYN attacks (CUSUM, adaptive threshold and k-mean cluster). Our aim is to find and compare detection probability, false alarm rate and capture intensity of attacked packets.

This paper is organised as follows: In Section 2 we present related works. In section 3 we present introduction to Network Data Mining (NDM) and provide information on how experimental data is collected, processed and evaluated. Section 4 presents various types of BGP attacks and relates them to the algorithms presented in this paper. In section 5, we discuss various anomaly detection algorithms. In section 6 we perform experiments to check the efficiency and their performance. Section 7 presents the performance analysis and Section 8 presents the conclusion and future work.

RELATED WORKS

Anomaly detection has received considerable attention from researchers in the past few years. To detect anomalies packet, different methods are used by various researchers including signature based, rules based, pattern matching and finite state machines. (Ruth M. Mutebi 2010) used a combination of cumulative sum, the Source IP Monitoring algorithm (SIM) and the adaptive threshold to detect volume based traffic. CUSUM and SIM run parallel to detect attacks and the adaptive threshold algorithm is used to monitor the sources of high traffic or if any conflict is generated.

(Siris & Papagalou, 2004), compared cumulative sum and adaptive threshold algorithm and investigated detection probability, detection delay and false alarm rate. (Shaikh, Iqbal, & Samad, 2005), used the same algorithm to detect SYN flood attacks. In the case of high and low intensity attacks, CUSUM shows good

performance while adaptive threshold algorithm exhibits better performance in detecting high intensity attacks. (Cisar & Maravic Cisar, 2007) used Exponentially Weight Moved Average (EWMA) control charts to monitor the rate of occurrences of events based on the intensity of attacks by using the adaptive threshold algorithms. (Gerhard M¨unz; Li & Wang, 2009) used the same algorithm to calculate anomaly packets in real time by distributing profile traffic features and used entropy to differentiate between normal and anomaly packets. (Gerhard M¨unz) used Network Data Mining (NDM) techniques to capture the packets and used the K-means algorithm on captured training data to separate normal and anomalous packets in clusters.

Our work is a combination of the above algorithms (CUSUM, adaptive threshold and k-mean cluster) by using the Network Data Mining (NDM) method which evaluates detection probability, strengths & weaknesses and false alarm rates. Furthermore, these patterns in the database can be used as a signature to capture the incidents in the future.

NETWORK DATA MINING

Network data mining (NDM) is useful for two different purposes. First, we gain knowledge about different types of data which then allows us to identify outlier within the data records that can be considered as malicious or suspicious. Secondly, NDM can be deployed to define the set of rules that are typical for specific kinds of traffic, for example, normal internet traffic or DoS attack traffic. These rules and patterns can be used as a signature to analyse the new set of data and compare them against the original data (Gerhard M¨unz; Huang, 1996).

Experiment Model

For our experiment purpose we use the KDD model. Knowledge Discovery and Data Mining (KDD) is an interdisciplinary area focusing upon methodologies for extracting useful patterns from data. Data mining is becoming an increasingly important tool in transforming this data into information. This information is further used in a wide range of scientific discoveries. Following the KDD model is shown in Figure 1.

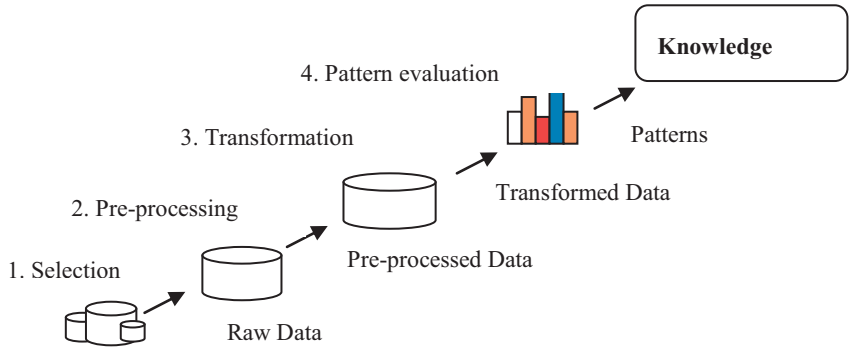


Figure 1: KDD process model.

1. ***Raw data****:* Data is recorded in the database for a specific interval of time.
2. ***Pre-processing****:* After collecting the raw data it is necessary to perform filtering on the data in order to remove unwanted data.
3. ***Transformation****:* At this stage, we apply the algorithm on pre-processed data to transform it into meaningful information for example a bar graph.
4. ***Evaluation****:* In this step we compare the outcomes of our algorithm with the original data using patterns and then turn them into knowledge.

TYPES OF ATTACK

BGP carries large amounts of traffic without proper security measures and training the data might be subject to an attack. Hence it is necessary to understand the types of attacks and its behaviour (Butler, et al., 2010; Rick Kuhn 2007). Following are the types of attacks which BGP routers encounter in a network:

Origin Attack

In this type of attack AS (Autonomous System) advertises modified or false information through BGP UPDATE message which passes through neighbour router who can claim it from the originator, also known as the prefix hijack.

Path Subversion

It is a special case of an origin attack in which the attacker modifies the content of the BGP UPDATE message (insert or delete) which can cause routing delays or allow false AS to modify the internet traffic, which makes it very difficult to detect the origin of such attacks (Butler, et al., 2010; Rick Kuhn 2007).

Denial of Service

In the Denial-of-Service (DoS) attack, an attacker attempts to send a large number of false traffic to routers, which causes the router to go offline or create a black hole. Meanwhile, if the neighbour router did not receive KEEPALIVE message from the offline router, then it causes route instability or flapping (Butler, et al., 2010; Rick Kuhn 2007).

Misconfiguration

Configuring BGP router is a complex and an error prone task. During the configuration process, a command line error can cause route instability (Ali & Boutaba, 2009; Butler, et al., 2010; Wuzuo WANG, 2010).

Basically all the attackers share common characteristics of the attack to send a large number of traffic and then create instability in the router. Their primary target are the port address, ip address and AS (routing table).Port scan (Butler, et al., 2010; Wuzuo WANG, 2010) is one of the most common techniques for attackers to discover the services then break into the network. All hosts connected to the network uses TCP and UDP port services. Port scan does not make any direct damage but it helps the attackers identify which port is available to launch various attacks on. Figure 2(a) exhibits such a case where the source port, scans the destination port and sends a large number of traffic to the destination port.

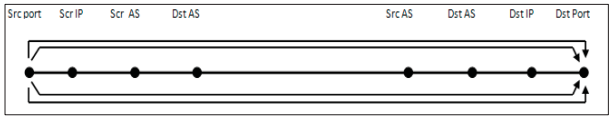


Figure 2(a) Port attack

Denial of service is one of the most common types of attacks in which the attacker attempts to make the network resource unavailable for the host (Wuzuo WANG, 2010). Figure 2(b) illustrates one of the most common types of attacks which is also known as the “SYN Flood” attack, in which the source host floods the destination host with SYN packets which consumes a large bandwidth of data and resources from the network. Denial of service also happens incidentally due to poor programming or misconfiguration.

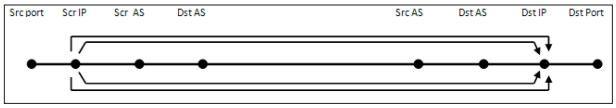


Figure 2(b) IP address attack

A malicious route injection involves the transmission of routes to unallocated prefixes. These prefixes are the sets of IP addresses which are unassigned. During the BGP update messages, a host router can inject a wrong prefix to the destination router which can cause route instability. Figure 2(c) shows that attackers hijack the internet traffic path by advertising a false path to destination AS (Butler, et al., 2010; Wuzuo WANG, 2010).

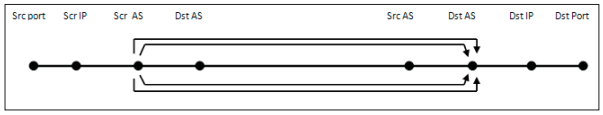


Figure 2(c) false route injection

ANOMALY DETECTION ALGORITHMS

The Border Gateway Protocol (BGP) is a routing protocol which was designed to route IP packets over large networks (Butler, et al., 2010). BGP runs over TCP and is a core routing protocol which requires a valid three-way handshaking before the host can establish a connection with any neighbouring device, such as router. Port scanning is one of the most common techniques used by the attacker to discover the services running on the host device. Since BGP messages communicate over the well known TCP port i.e. 179, it is much easier for an attacker to flood SYN packets over the network.

In this section, we present three statistical anomaly detection algorithms that detect SYN flood attacks and also provide protection to DoS attacks. The first algorithm is a widely used anomaly detection, based on the change point detection theory. The second and third are simple algorithms that detect anomalies based on violation of a specific threshold (Ruth M. Mutebi 2010; Shaikh, et al., 2005; Siris & Papagalou, 2004).

5. Cusum (Cumulative Sum) Algorithm

CUSUM or (cumulative sum) is a simple algorithm to detect the anomaly packets if the numbers of packets or traffic exceeds a particular threshold. An alarm is raised to detect an anomaly packet. The formula below is used to calculate CUSUM used in the algorithm (Ruth M. Mutebi 2010; Shaikh, et al., 2005; Siris & Papagalou, 2004).

$$Cusum_i = \sum_{j=1}^{i} \overline{x}_j - x_i$$

Algorithm

1. Calculate $x_i = \frac{(x1+x2+x3+\ldots..+xn)}{n}$
2. Define upper and lower limit of CUSUM threshold.
3. UPPER _LIMIT ←max(0,x_i-k) + C_UPPPER_LIMIT i-1
4. LOWER _LIMIT ← max (0, x_i -k) + C_LOWER_LIMIT i-1
5. Define threshold level (k)
6. For i=1… j do
7. CUSUM=x_j-x_i
8. If (CUSUM < k) then
9. Sound alarm
10. Else return to step 5
11. End.

6. Adaptive Threshold Algorithm

The adaptive threshold algorithm is relatively simple. Its' working mechanism is similar to CUSUM. If the number of packets increases the threshold level, then an alarm is raised (Butler, et al., 2010; Ruth M. Mutebi 2010; Shaikh, et al., 2005; Siris & Papagalou, 2004; Wuzuo WANG, 2010).

This relies on testing whether the traffic measurement, number of SYN packets in our case, over a given interval, exceeds a particular threshold. In order to account for seasonal (daily and weekly) variations and trends, the value of the threshold is set adaptively based on an estimate of the mean number of SYN packets, which is computed from recent traffic measurements. If xn is the number of SYN packets in the nth time interval, and μn−1 is the mean rate estimated from measurements prior to n, then the alarm condition is given by:

If $x_n \geq (\alpha + 1)\overline{\mu n}-1$ then ALARM signalled at time n

Where, $\alpha > 0$ is a parameter, this indicates the percentage above the mean value that we consider to be an indication of an anomalous behaviour. The mean μn can be computed over some past time window or by using an exponentially weighted moving average (EWMA) of previous measurements.

$$\overline{\mu}_n = \Gamma\overline{\mu}_{n-1} + (1 - \beta)x_n$$

Where, Γ is the EWMA factor. Direct application of the above algorithm would yield a high number of false alarms (false positives). A simple modification that can improve its performance is to signal an alarm after a minimum number of consecutive violations of the threshold. In this case the alarm condition is given by (Butler, et al., 2010; Ruth M. Mutebi 2010; Shaikh, et al., 2005; Siris & Papagalou, 2004; Wuzuo WANG, 2010).

$$\sum_{i=n-k+1}^{n} 1\{x_i \geq (\alpha + 1)\mu_i - 1\} \geq k$$

Then, ALARM at time n, where k > 1 is a parameter that indicates the number of consecutive intervals the threshold must be violated to sound an alarm. The changeable parameter of the above algorithm are the threshold factor α for calculating the successive threshold, the number of successive threshold violations k before signalling an alarm, the EWMA factor Γ, and the length of the time interval over which SYN packets are diagnosed.

Algorithm

1. SELECT the total number of host → sumhost
2. SELECT the number of hosts with degree xi →numberofhost[i]
3. Count rows of different degree →numdiffdegree
4. for i:= 1 to numberofhost do
5. numberof host[i]/sumhost →f(xi)
6. Compute and normalize the A(x) →yi
7. Repeat 1-6
8. Rule out yi which beyond the threshold
9. avg(y1,y2,…,y60)→ μ
10. avg((Y- μ)^2)→σ^2 Z=y_k, k=1,2,…
11. setup threshold: $m \pm 2 * \sigma$

7. K-mean Cluster Algorithm

K-means clustering is an algorithm which targets to partition n data points of the same values into k clusters [3]. Data points which are close to centroid, share the same feature value (Ali & Boutaba, 2009; Gerhard M¨unz; Li & Wang, 2009; Meng, Shang, & Bian, 2009; Silveira & Diot, 2010).

$$j = \sum_{j=1}^{k} \sum_{m \in S_j} |x_n - \mu_j|^2$$

Algorithm

1. Define the number of clusters K.
2. Place the K cluster to its nearest centroids by Euclidean distance.
3. Recalculate the positions of each K to its nearest centroids.
4. Repeat step2 and step3 until all the centroids converge.

The distance between each similar point is calculated by distance function, Euclidean distance is the most common distance function which is defined as:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (xi - yi)2}$$

Where $x=(x_1, x_2 \ldots x_n)$ and $y= (y_1, y_2 \ldots y_n)$ are the two input vector. As we choose initial value K=1 considering that normal traffic. The distances from cluster centroids are calculated by the weighted Euclidean distance function which is given below.

$$d(x, y) = \sqrt{\sum_{i=1}^{n} \left(\frac{xi - yi}{si}\right)2}$$

An object is to be classified as normal if it is close to the normal cluster centroids, otherwise anomalous, if it's far from the normal cluster centroid. Figure 3(a) shows before cluster algorithm is applied where P1, P2 and P3 are classified as anomaly packet whereas, in figure 3(b) where diameter of centroid is increased so P1 and P3 are considered as normal while P2 is anomaly packet(Ali & Boutaba, 2009; Gerhard M¨unz).

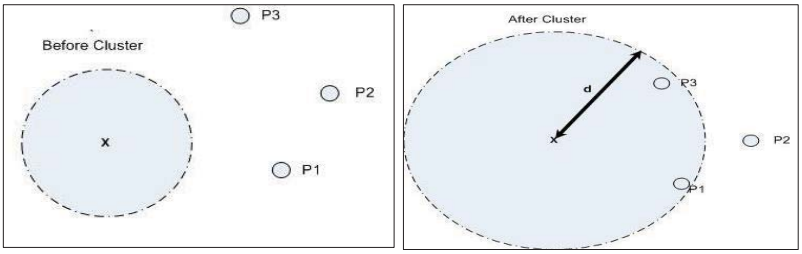


Figure 3(a) Before clustering *Figure 3(b) After clustering*

PERFORMANCE EVALUATIONS

For the experimental analysis we extracted the dataset from the MIT-Lincoln Labs, KDD CUP 99 which is available publicly. The dataset contains a standard set of normal and attacked data which is useful for testing the algorithm performance. Our performance evaluation is based on three major experiments. In the first experiment scenario, the attacker sends illegitimate traffic (high intensity attack packets) which can cause a buffer overflow or a black-hole process. In the second scenario, we reduced the amplitude of our traffic by 50% to check the

efficiency of an algorithm at low intensity of attacks. In the last scenario we evaluate our experiment data on Receiver Operate Curve (ROC) which shows the trade-off between detection probability and false alarm rate.

A. High intensity Attacks

In first experimental scenario we considered high intensity of attacks where attacker sends large number of SYN packets which eventually can causes buffer overflow or denial of service (Gerhard M¨unz; Shaikh, et al., 2005; Siris & Papagalou, 2004).

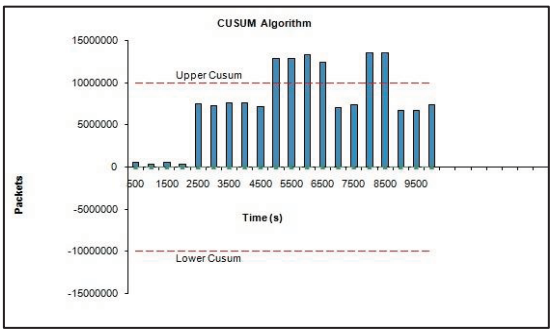


Figure 4(a) CUSUM

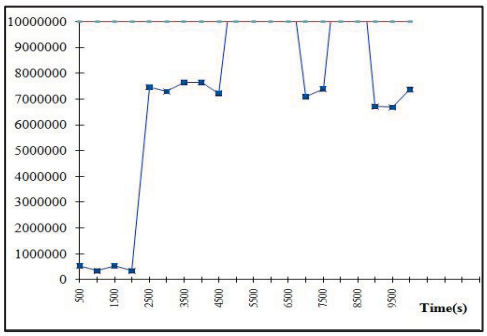


Figure 4(b) Adaptive threshold

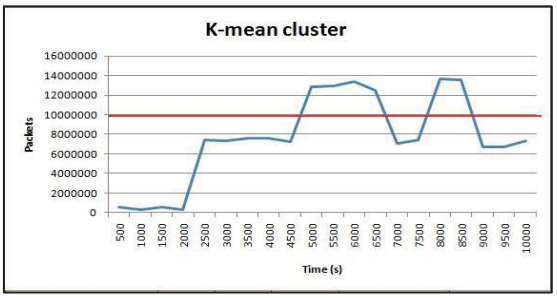


Figure 4(c) K mean

Figure 4(a), 4(b) and 4(c) shows the results for the CUSUM, adaptive threshold and k-mean cluster, respectively. The horizontal axis in these figures represents time interval seconds started from 0 to 10000 while vertical axis shows the number of packets. The above graphs show that all of our algorithms exhibit excellent performance and high intensity attacks detection probability of a 100% and 0% alarm rate ratio.

B. Low Intensity Attacks

In second scenario we reduced the amplitude of the attack by 50% of the actual mean rate to check the performance of our algorithm for low intensity attacks. Detection of low intensity attacks is important for two reasons: Firstly, it enables protection to take action at an earlier stage. Secondly, the attacker can be easily tracked because it's closer to the source (Gerhard M¨unz; Siris & Papagalou, 2004). Placement of such detection algorithms can help us to identify the hosts which are participating in denial of service attacks.

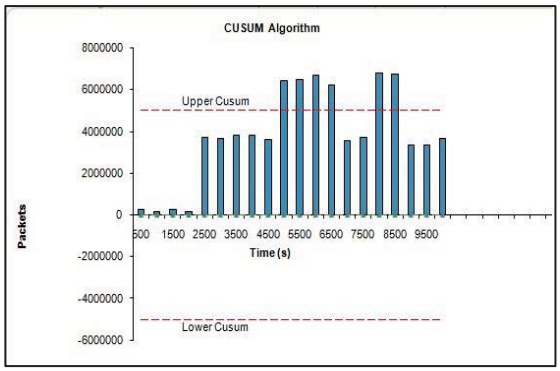


Figure 5(a) CUSUM

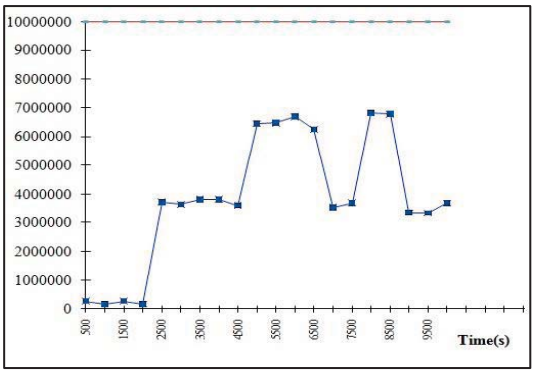


Figure 5(b) Adaptive threshold

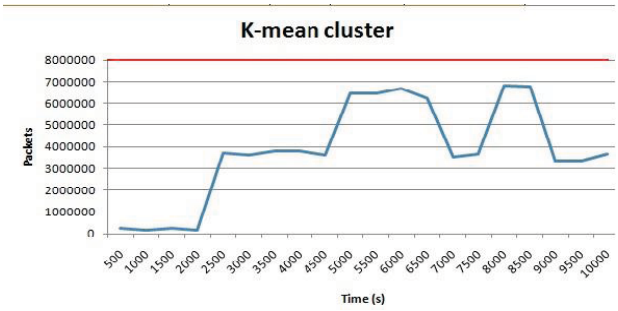
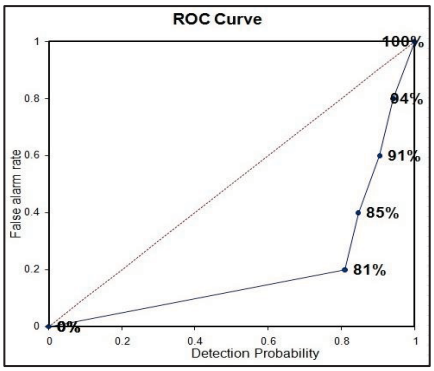


Figure 5(c) K mean

Figure 5(a), 5(b) and 5(c) illustrates the performance of CUSUM, adaptive threshold and the k-mean cluster algorithms respectively for low intensity attacks. Figure 5(a) shows that the performance of the CUSUM algorithm which is much better in detecting the low intensity of attacks. On the other hand, figure 5(b) & 5(c) shows that the deteriorated performance of the adaptive threshold and k-mean cluster algorithms are used for detecting low intensity of attacks.

C. False Alarm & Detection Probability

To validate the efficiency of the above algorithms, we tested high and low intensity of attacks on the Receiver Operate Curve (ROC). On the horizontal axis we labelled the detection probability which is the percentage of attacks while alarms were raised and on the vertical axis, we labelled the false alarm rate (FAR) (Siris & Papagalou, 2004), which is the probability of the false detection that did not correspond to the actual attack. We calculated high and low intensity attacks on the ROC graph for the first five intervals for each algorithm. Figure 6(a) & 6(b), illustrates that the CUSUM algorithm demonstrates good performance on both low and high intensity attacks with 100% detection rate and a false alarm rate of 0%.



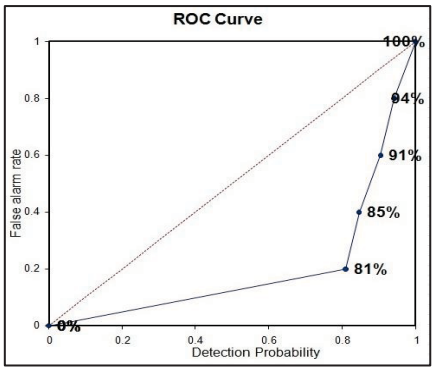
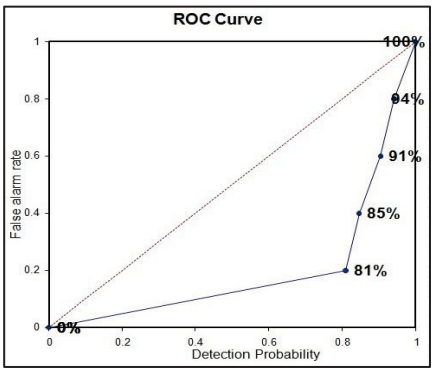


Figure 6(a): CUSUM high intensity *Figure 6(b) CUSUM low intensity*



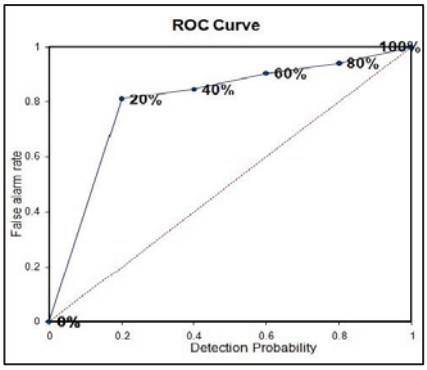
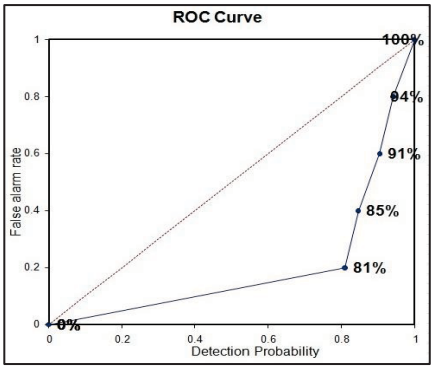


Figure 7(a) Adaptive threshold high intensity *Figure 7(b) Adaptive threshold low intensity*



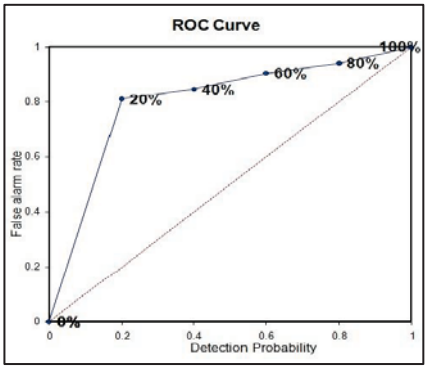


Figure 8(a) K mean high intensity attack.

Figure 8(b) K mean low intensity attack

Figure 7 (a,b) & 8 (a,b) shows that in both the algorithms, the adaptive threshold and k mean cluster have better performance in the case of high intensity attacks with better detection probability (Cisar & Maravic Cisar, 2007; Shaikh, et al., 2005; Siris & Papagalou, 2004). On the other hand, for low intensity, both algorithms show the worst performance with high alarm rate.

PERFORMANCE ANALYSES

	CUSUM	Adaptive Threshold	K-Cluster
Detection Probability	Slow	Fast	Fast
High Intensity Attacks (HIA)	1.	2.	3.
Low Intensity Attacks (LIA)	4.	X	X

According to the data analysis above, we can see that the adaptive threshold and k-mean cluster have fast detection probability in capturing high intensity of attacked packets while cusum detects but with slow performance. On the other hand, cusum detects low intensity attack packets while the other two algorithms show poor performance in capturing low intensity attacks.

The experimental results show that the cusum algorithm has better performance in capturing anomaly in low traffic network while the adaptive threshold and the k-cluster is good for high traffic networks.

CONCLUSION

In this paper, we presented three statistical algorithms which detected SYN flooding attacks namely CUSUM, adaptive threshold and k-mean cluster for detecting anomaly packets in real time. The algorithms were implemented and their performances were tested using KDD CUP 99 dataset. Our investigations considered different parameters i.e. detection rate, false alarm rate, and intensity of attacks.

Based on the above experiments, the CUSUM algorithm has better performance in capturing high and low intensity attacks with high detection probability and low false alarm rate .On the other hand, the adaptive threshold and k-mean cluster showed better performance in capturing high intensity anomaly packets while in the case of low intensity attacks its performance deteriorated with high alarm rate.

Our ongoing research primarily focuses on traffic anomalous features of inbound and outbound traffic of production networks and it also provides us with a defensive mechanism at an earlier stage of the attacks which causes a denial of service.

REFERENCES

Ali, K., & Boutaba, R. (Eds.). (2009) Information Infrastructure Symposium, 2009. GIIS '09. Global.

Butler, K., Farley, T. R., McDaniel, P., & Rexford, J. (2010). A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE, 98(1), 100-122.

Cisar, P., & Maravic Cisar, S. (2007, June 29 2007-July 2 2007). EWMA Statistic in Adaptive Threshold Algorithm. Paper presented at the Intelligent Engineering Systems, 2007. INES 2007. 11th International Conference on.

Gerhard M¨unz, S. L., Georg Carle. Traffic Anomaly Detection Using K-Means Clustering.

Huang, G. J. W. a. Z. (1996). Modelling the KDD process.

Li, T., & Wang, J. (2009, 25-27 Dec. 2009). Research on Network Intrusion Detection System Based on Improved K-means Clustering Algorithm. Paper presented at the Computer Science-Technology and Applications, 2009. IFCSTA '09. International Forum on.

Meng, J., Shang, H., & Bian, L. (2009, 15-17 May 2009). The Application on Intrusion Detection Based on K-means Cluster Algorithm. Paper presented at the Information Technology and Applications, 2009. IFITA '09. International Forum on.

Rick Kuhn , K. S. D. M. (2007). Border Gateway Protocol Security [Report.].

Ruth M. Mutebi , I. A. R. (2010). An Integrated Victim-based Approach against IP Packet Flooding Denial of Service

Sengar, H., Xinyuan, W., Haining, W., Wijesekera, D., & Jajodia, S. (2009, 13-15 July 2009). Online detection of network traffic anomalies using behavioural distance. Paper presented at the Quality of Service, 2009. IWQoS. 17th International Workshop on.

Shaikh, R. A., Iqbal, A. A., & Samad, K. (2005, 27-27 Aug. 2005). Review Over Anomaly Detection Algorithms for Detecting SYN Flooding Attacks. Paper presented at the Engineering Sciences and Technology, 2005. SCONEST 2005. Student Conference on.

Silveira, F., & Diot, C. (2010, 14-19 March 2010). URCA: Pulling out Anomalies by their Root Causes. Paper presented at the INFOCOM, 2010 Proceedings IEEE.

Siris, V. A., & Papagalou, F. (2004, 29 Nov.-3 Dec. 2004). Application of anomaly detection algorithms for detecting SYN flooding attacks. Paper presented at the Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE.

T.Bates, J. H. a. (1996). Guidelines for Creation, Selection, and Registration of an Autonomous System (AS). [RFC 1930].

Wuzuo WANG, W. W. (2010). Online Detection of Network Traffic Anomalies Using Degree Distributions. www.scirp.org/journal/PaperDownload.aspx?paperID=1272...pdf.