Detecting Denial of Service Attacks on High Speed Networks using Kolmogorov Smirnov Test and its Variants

Qasim Javed [1,2], Muhammad Shoaib Alam [1,2], Muhammad Bilal Anwer [1,2], Muhammad Raza ur Rehman [1,2]
Dr Saeed Murtaza[2] , Faisal Anwar [2,3], Dr M Akbar[2].
[1]{qasim_nust, shoaib_alam, mbanwer82, netwizio}@yahoo.com
[2] Military College of Signals, National University of Sciences and Technology, Pakistan.
[3] Manager Operations NSS PTCL Pakistan.

Abstract

The inherent insecure nature of the core Internet protocols has led to many problems but none of them is as problematic as the denial of service attacks. Denial of Service (DoS) attacks are easier to perpetrate and difficult to mitigate. Even a bunch of teenage hackers can bring down connectivity of a web server for hours by clogging its bandwidth with unwanted packets. This situation is much more aggravated by the inherent unpredictable and ever changing nature of Internet traffic. Hence detection of quality of service breaches by Denial of Service attacks requires special modeling and model updating techniques. Kolmogorov Smirnov Test (KS test) seems an ideal test for detecting variations in the high speed networks, a situation where no assumption can be made about the nature of the input data. Kolmogorov Smirnov Test tries to determine if the two probability distribution functions differ significantly. KS Test is distribution free and non-parametric. In this paper we compare the results of the application of the KS test and its variants like Anderson Darling to detect the denial of service attacks on high speed networks.

Key Words

Denial of Service (DoS) attacks, Network Traffic Modeling, Kolmogorov Smirnov Test, Anderson Darling Test, and Goodness of Fit Tests.

Introduction

The increased dependency of man on computers has rendered him with great conveniences. But on the other hand it has also made him the victim of many attacks related to the computers and networks, which can cause him, financial and even in some cases, fatal damages. The dependency of man on computers has made him vulnerable to what can be called Cyber Terrorism. This situation is much more aggravated by the insecure nature of the core internet protocols and the lack of the computer security

concern amongst the masses. The vulnerabilities in the computer systems can be divided into two types on the basis of their sources

1. The vulnerabilities in the software
2. Flaws in the protocols

Both can be devastating at one time or the other. But flaws in the protocols are much more critical because they need the entire protocols to be changed.

One of the vulnerabilities that have come in the limelight in the recent years has been the Denial of Service Attacks. Denial of Service Attacks can be defined as malicious attempts by a single person or a group of persons to cripple an online service such as the messaging and emailing services etc. Denial of Service Attacks can be regarded as the most devastating form of computer security breaches because both the vulnerabilities in the software and the flaws in the protocols are combined to execute them, with some exceptions.

Denial of Service attacks are easy to perpetrate, hard to stop and difficult to mitigate. The history of the denial of service attacks shows that even a 13 year hacker can cause the whole website to remain offline for hours. Further more the motives behind the denial of service attacks can be varying. These might be political such as the attacks on the Pakistan government sites by the Indian hackers [2]. The denial of service attacks can be for economical reasons like [3]. The denial of service attacks have become so much prevalent that companies have lose business due to them [4] and many companies have been forced to change their policies due to the them. In short the greatest menace to the internet related industries have been the denial of service attacks for some years.

Network Faults and Goodness of Fit Techniques

The network faults can be divided into two types namely: hard failures, the failures in which the network, some part of it or the other, fails to deliver the traffic; soft failures, the faults in which the network undergoes some sort of anomaly or degradation in the performance like increased packet delay and the increase (why is it here)in bandwidth etc. Hard failures are easy to detect because they cause the network traffic to cease to flow but the soft failures are difficult to detect.

Software failures result from the excess of some thing or the deficiency of some thing. As examples to this fact the increase in packet rate, decrease in bandwidth, increase in packet delay and the increase in number of packets are all the examples of the soft failures. In short soft failures result in the deviation of the parameter’s probability density (or distribution) function (defining the probability of occurrence of different points in the graph) from the normal (the parameter varies according to the situation). This fact is demonstrated by the graphs in the figure 1. Figure1 shows the point beyond which the service totally fails.

Figure 1 A pdf describing the point of total service failure

Hence the statistical goodness of fit test are the optimum tool for the detecting the soft failures because they can enable us to find that whether the input data is comparable to the sample pdf or not; and to which extent the two data sets are varying as compared to each other.

Denial of Service Attacks, an example of soft network failure, has been the subject of active study in the mathematical computer science in the recent times. Most of these systems base their analysis on averages. But the averages mean more generalization in analysis hence some lost of precision. So, as a result the average based systems are being abandoned with other systems like the probability density functions (PDF) or others. The use of probability distribution function can be much more informative and robust as indicated by the figure 1 in which the point of total failure. Similarly the PDF based statistics also make it easy to calculate other features like maximum deviation can be easily calculated. The robustness of Kolmogorov Smirnov (KS) test and its variants is based on the same principle i.e. the PDF based calculation can be more robust and intuitive. Further KS and its variants are parameter and distribution independent which makes them more suitable for the detection of the soft failures in networks and hence the denial of service attacks.

Kolmogorov Smirnov Test was used first in [5] to model and detect network anomaly patterns, [6] used a variant of Kolmogorov Smirnov Test for the generalized fault and anomaly detection in the wireless networks. In this paper we highlight and contrast the working of the Kolmogorov Smirnov test and the Anderson Darling Test and the variant used in the [6] (hereafter called Manikopoulos Test).

Kolmogorov Smirnov Test

Kolmogorov Smirnov Test is based on the empirical cumulative distribution function (ECDF).

Given N ordered data points y_1, y_2, y_3... y_N the ECDF can be defined as

$$E_m = n_m/N$$

Where n_m is the number of points less than y_m where m=1,2…N. The two sample KS test is elaborated by the following equation [7]

$$D=\max_{-\infty<x<\infty}|T(x)-S(x)|$$

Where the T(x) and S(x) are the two ECDFs to be analyzed by the KS test. The calculation of KS is illustrated by the figure 4.

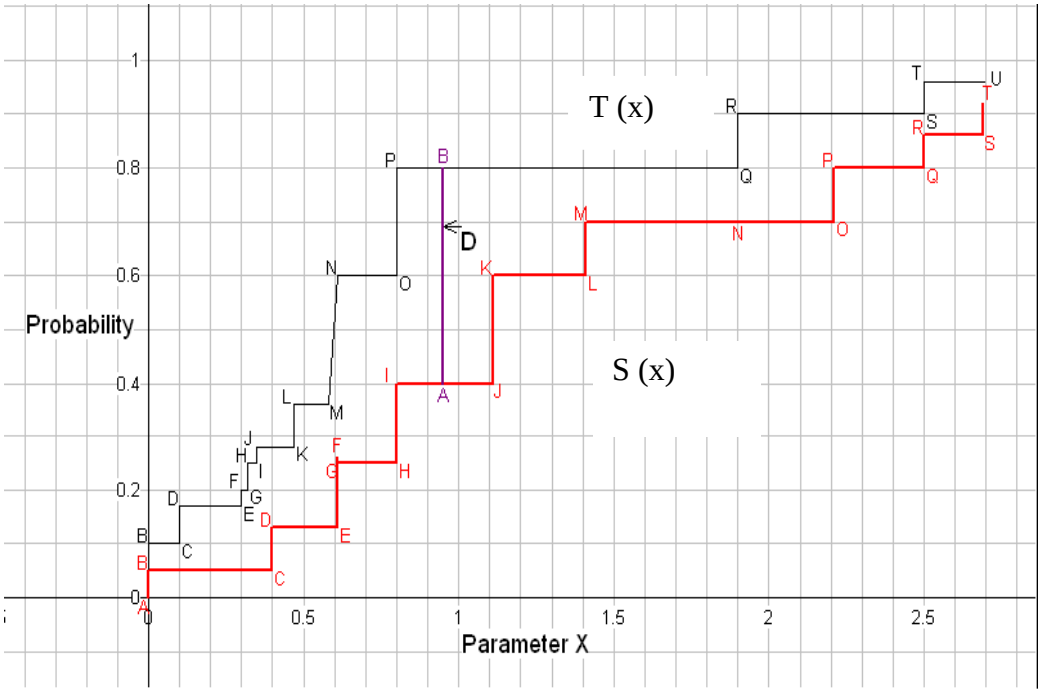

Figure 3 The Kolmogorov Smirnov Test

The KS test has many advantages like that it is not dependent on the underlying cumulative distribution function and further it is in exact test (does not depend on the number of data points). But it has certain limitations also like that it is more sensitive near the center than at the tails.

Anderson Darling Test (AD)

The Anderson Darling test was an attempt to improve the faults in the Kolmogorov Smirnov Test i.e. the KS test is more sensitive at the center than the tails. So

give the same weight to the tails also provided the following modifications were presented by Anderson Darling in the KS test[7]. The AD test is given below

$$A=\max_{-\infty<x<\infty}(|T(x)-S(x)|)*(T(x)(1-T(x))^{-1/2}$$

Manikopoulos Test

Manikopoulos [6] modified the KS test to especially cater for denial of service attacks. Denial of Service attacks detection should be robust against the misclassifications of the normal traffic and the subtle variations in the traffic. So to cater for this Manikopoulos modified the KS and added the difference of the area between the two curves to the original KS D factor so the Manikopoulos test is given by

$$M=\max_{-\infty<x<\infty}\{|T(x)-S(x)| + f(N)* (\Sigma_{i=1\ldots k}|T(x)-S(X)|)\}$$

Where f (N) is the function catering for the total no of observations in the following analysis time window. Diagrammatically it can be represented by the figure 4

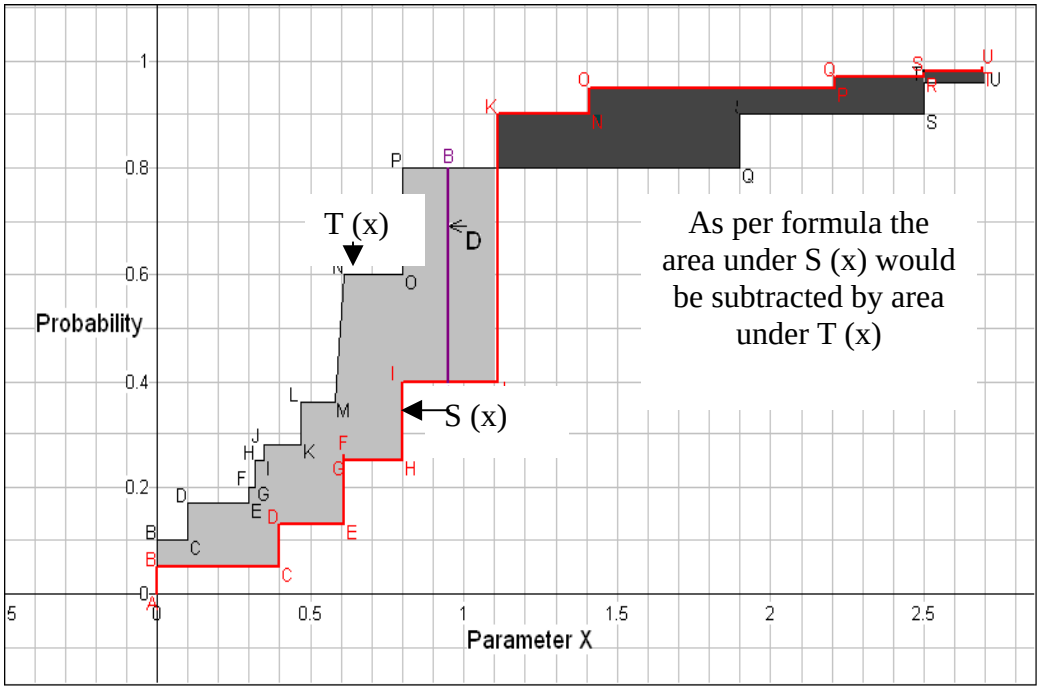

Figure 4 Manikopoulos Test

Our Testing Approach

In this paper we demonstrate our results on the denial of service attacks resulting from the SYN flooding (a specific DoS attack) only . A probe module counts the no of

packets for each type of DoS attack and after a predetermined number of such observations we give the data to the corresponding statistical module being tested. These no of observations constitute the analysis window.

The actual KS test and the AD test also calculate some critical value to check whether the hypothesis is right. As the distribution of the internet traffic is indeterminate and ever changing so instead of relying on the critical value some other options can be used. These include the usage of some specific thresholds as measure of the anomaly or the usage of the neural network to decide upon the test results of the KS test or other tests or any other expert system. This deciding module is hereafter called the decision engine. In this test we use expert system to decide upon the output of the statistical tests. But as the traffic profile has to be updated regularly we adopt the same normal traffic profile updating formula.

Let p_{old} be the reference model before updating, p_{new} be the reference model after updating, and p_{obs} be the observed user activity within a time window. The formula to update the reference model is

$$P_{new}=P_{old}\,(1-s*a)+P_{obs}*s*a$$

Where

a=predefined learning rate

s= output of the decision engine (0 in the case of attack).

Results and Analysis

Table 1 shows that the detection rates etc. for all the three tests.

Table 1 Comparison of KS test AD test and Manikopoulos test

Test Name	KS	Test Name	AD	Test Name	Manikopoulos
Learning rate	0.01	Learning rate	0.01	Learning rate	0.01
Total attacks	100	Total attacks	100	Total attacks	100
Attacks Detected	76	Attacks Detected	79	Attacks Detected	86
No of False Positives*	10	No of False Positives	10	No of False Positives	6
% Attack Detection	66%	% Attack Detection	69%	% Attack Detection	80%
% False Positives	10%	% False Positives	10%	% False Positives	6%

* False Positives corresponds to the normal traffic misclassified as attacks.

The table shows that the KS and AD test are quite similar in performance. The attacks detection is superior in the AD test but they suffer with the same percentage of false positives. The reason is that the AD test analyzes the tails of the PDF better while

the KS test is on. Hence the KS test is able to better judge the attacks in the start and the end of the analysis window.

The Manikopoulos Test is superior to both in the DoS detection. The reason being that it accommodates the difference of the area between the two curves. Hence it is able to better accommodate even the subtle differences in the two pdf. For the same reason the false positives in the case of Manikopoulos test are far low. But the Difference of the area of the two curves in the Manikopoulos test makes it much more robust to the flash crowds than the other two tests.

Another important point to be considered is the effect of the learning rate on the DoS Detection rate. It is demonstrated in the following table.

Table 2 Effect of Learning Rate on Manikopoulos Test

Learning rate	0.01	0.05	0.1	0.2
Total Attacks	100	100	100	100
Attacks Detected	86	84	81	70
False Positives	6	6	2	2
%attack Detection	80%	78%	79%	68%
% false positives	6%	6%	2%	2%

Table 2 shows that the % of attack detection and the % of false positives are very much dependant upon the selection of optimum learning rate.

Conclusion:

From the above research and experimentation it can be concluded that the non-parametric goodness of fit test can help not only in the real time detection and hence prevention of the denial of service attacks but also the detection of the other soft network failures. For optimum results some minute changes (depending upon the specific situation) in the goodness of fit tests are required. Furthermore according to our results shows that Manikopoulos Test is a viable technique for the intrusion detection with high attack detection rate and low false positives. Furthermore the Manikopoulos test is less in computation as compared to other computation intense methods.

Future Works

Future works include some other optimizations in the Manikopoulos test for flash crowd robustness. In future we also intend to apply the results of our this experimentation to other soft network failures like the bandwidth problems, packet delay etc. Further this work can also be applied to the soft computer failures also.

References

[1] The strange Tale of Denial of Service Attacks against GRC.com
http://grc.com/dos/grcdos.htm
[2] Indian Hackers crack Pakistani Sites
http://www.vnunet.com/News/1133119
[3] BT hacked: revenge for crap service
http://www.theregister.co.uk/content/1/12097.html
[4] How Cloud Nine wound up in Hell
http://www.wired.com/news/business/0,1367,50171,00.html
[5] Statistical Traffic Modeling for Network Intrusion Detection
Cadbrera, Mehra, Ravichandran.
[6] Architecture of Generalized Network Anomaly and Fault Thresholds
Zheng Zhang, C. Manikopoulos, Jay Jorgenson
[7] Kolmogorov Smirnov Two Sample
http://www.itl.nist.gov/div898/software/dataplot/refman1/auxillar/ks2samp.htm
[8] Anderson Darling Test
http://www.itl.nist.gov/div898/handbook/eda/section3/eda35e.htm