ISSN : 2231-0711

Md. Ariful Hoque et al | International Journal of Computer Science Engineering and Technology(IJCSET) | March 2015 | Vol 5, Issue 3, 44-47

Anomaly Based Intrusion Detection Systems Using SNMP Data

Md. Ariful Hoque & Barnali Chakraborty

Department of Post & Numerify

Abstract-This paper discusses a statistical algorithm to detect DOS attacks on computer net- works. DOS attacks hamper the network by making resources unavailable to genuine users. The algorithm presented here use SNMP data in order to detect incoming flooding attack on a computer or network. The data to be monitored depends on the class of flooding attacks that is intended to be detected. In this paper we focus on detecting ICMP, UDP, TCP and IP type of flooding attacks on various network interfaces.

1. INTRODUCTION

Anomaly literally means abnormality. Anomaly detection refers to detecting patterns in a given data set that do not conform to an established normal behavior. The patterns thus detected are called anomalies and often translate to critical and action- able information in several application domains. Anomaly detection is widely researched area. It can be broadly classified to be either *network based* or *host based*. This paper discusses an algorithm that can be used for both *a network based as well as host based anomaly detection technique* using SNMP data.

The primary aim of this paper is to detect flooding attacks using SNMP data. Some re- search has been carried out in this field. A statistical method for anomaly detection is described in [7]. In this paper MAID technology was used to monitor 27 MIB II supplied network traffic parameters. A probability density function (PDF) was constructed for each parameter and compared statistically to a reference normal parameter using a similarity metric. Then the result was combined into an anomaly status vector that is classified by a neural network classifier. The paper gives a comparative study of several similarity metrics such as $\chi 2$ test (CST), Kolmogorov Smirnov test (KST), Kupier's KS type statistic (KKS), a combined area-KS type test (AKS), and a simpler fractional deviation from the mean statistic (FDM). In another paper [4], a review has been done on the various anomaly detection methods. This includes anomaly detection using statistical analysis of SNMP MIB. This paper is divided into various sections. The next section gives a walk-through of the proposed algorithm. The third section de- scribes the environment where experiments were carried out in order to test the algorithm. The subsequent sections discuss the results and conclusion.

2. PROPOSED MODEL

2.1 About KS Test

In statistics, the Kolmogorov Smirnov Test (KS Test) is a non parametric test. This means that it does not rely on data that belongs to any particular distribution and does not assume that the structure of a model is fixed. Kolmogorov Smirnov Test of two types

a. One Sample KS Test.

b. Two Sample KS Test.

One Sample KS Test: This test is used to test whether the sample comes from same reference distribution or not. It compares the cumulative distribution functions for a variable with a specific theoretical distribution, the distribution may be normal, uniform, Poisson or exponential. It tests whether the observed distribution is identical to the specified reference distribution.

Two Sample KS Test: This test is used to test whether two samples come from the same distribution. The distribution may be normal, uniform, Poisson or Exponential.

In this paper, we are using Exponential distribution for our algorithm. The Two Sample KS Test is a variant of One Sample KS Test. Instead of comparing a cumulative distribution function to a theoretical distribution function, it compares two cumulative distribution functions of two different data samples. More formally KS Test can be defined as follows.

H_0 = The two samples come from a common distribution.

H_1 = The two samples do not come from the same distributions

2.2 Proposed Algorithm

1. Collect training data set and treatment data set and calculate cumulative mean of each data sets separately.
2. Calculate exponential distribution, also known as cumulative density function, for each data value in each sample using the following formula

$$E(i) = (1 - e^{(1/\mu) * i}),$$

where, μ is the mean of a sample data set and i is the single data.

3. Calculate D_{max} (maximum distance between the values of cumulative density functions of the two samples) *i.e.*

$$D_{max} = Max(E1(i) - E2(i))$$

where, $E1$ and $E2$ are the cumulative density functions for each data of both sample and 1 i n if each sample contains n number of data.

4. Calculate the critical value, C_{alpha} (threshold value),

to check whether a data set is normal or anomalous. This value is calculated from the following formula:
$Calpha = c(\alpha) * \sqrt{((n1 + n2)/(n1 * n2))}$, where $n1$ and $n2$ are the sizes of the trained and treatment data set respectively and α is the significance level. The standard value of α is 0.5 and its corresponding $c(\alpha)$ value is 1.36.

5. The hypothesis $H0$, regarding the distribution form, is rejected if the test statistic, $Dmax$, is greater than the critical value, $Calpha$, *i.e.* data set is *anomalous*. Otherwise, the hypothesis $H0$ is accepted *i.e.* the data set is *normal*.
6. If the data set is normal then the training data set is updated by the treatment data set. Otherwise training data set remains same and collects new treatment data.

The algorithm is explained using a flow chart in Fig 1:

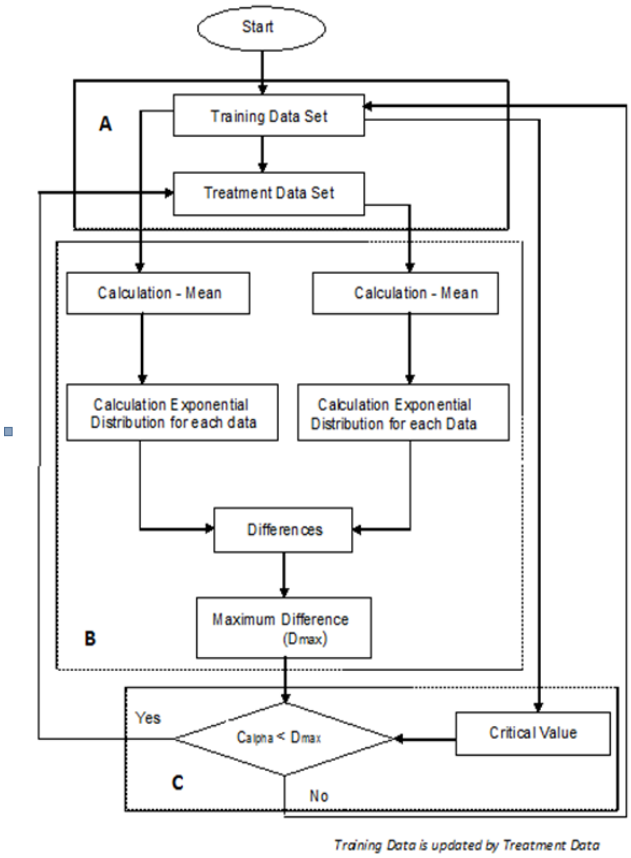

Fig 1

After plotting the cumulative density function values, we have two graphs for the training and the treatment data sets as well as their deviations from each other. If the maximum deviation is greater than a predefined *critical value* (Threshold Value) then the data set declared to be anomalous. Otherwise the data set is normal.

3. EXPERIMENT

The above KS Test can be represented graphically as shown in Fig 1.1 below. The X axis represents the sample sizes and the Y axis represents the cumulative density function values for all the sample values. The cumulative density function values always lie in between 0 and 1. We have two sample data sets, the training dataset and the treatment data set:

Trained Data Set = 0.08, 0.10, 0.15, 0.17, 0.24,0.34, 0.38, 0.42, 0.49, 0.50, 0.70, 0.94, 0.95, 1.26,1.37, 1.55, 1.75, 3.20, 6.98, 50.57

Treatment Data Set = 0.001, 0.008, 0.019, 0.019,0.029, 0.079, 0.068, 0.502, 0.115, 0.136, 0.107,0.151, 0.205, 0.201, 0.166, 0.288, 0.492, 27.44,30.41, 10.04

The graphical representation of the dataset is shown in Fig 2:

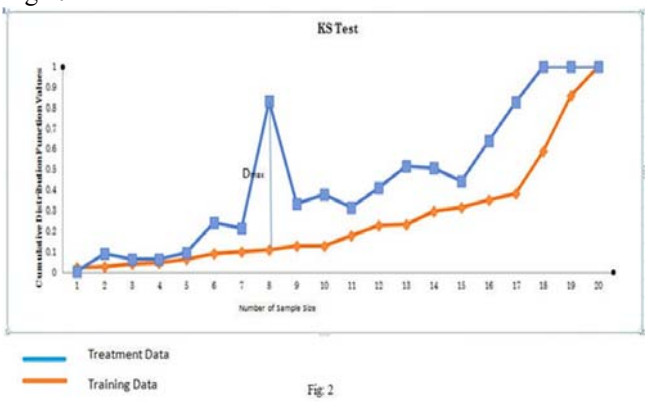

Fig 2

To perform experiment with our algorithm we choose a small local area network (LAN) of C-DAC (Centre of Development of Advance Computing) which contains 11 switches and 264 machines connected to those switches, out of which we targeted only one switch. The IP address of which is 172.16.16.247 and is having 24 interfaces.

We have considered 22 OIDs for polling data using SNMP which includes 8 OIDs from *interface* group, 4 OIDs from *icmp* group, 4 OIDs from *tcp* group, 2 OIDs from *udp* group and 4 OIDs from *ip* group. The details of the OIDs are listed below in Fig 3.

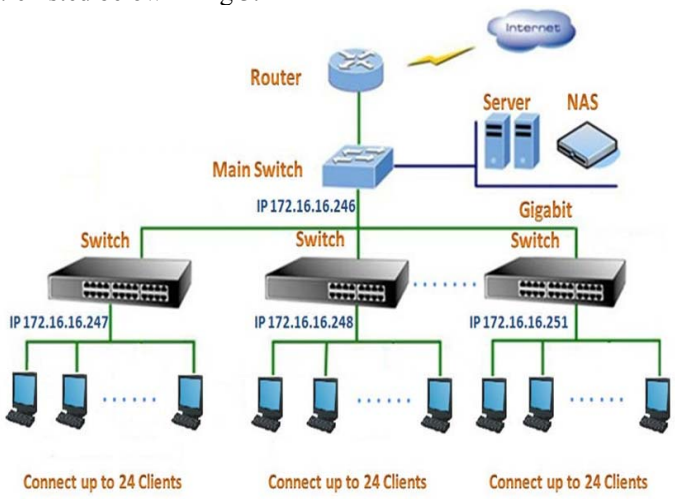

Fig 3

interface	tcp	ip	icmp	udp
ifInOctets	tcpPassiveOpens	ipInReceives	icmpInEchos	udpInDatagrams
ifOutOctets	tcpAttemptFails	ipInDelivers	icmpOutEchos	udpOutDatagrams
ifInUcastPkts	tcpInSegs	ipInDiscards	icmpInMsgs	
ifOutUcastPkts	tcpOutSegs	ipOutDiscards	icmpOutMsgs	
ifInNUcastPkts				
ifOutNUcastPkts				
ifInDiscards				
ifOutDiscards				

Fig 4

3.1 Preparing of Training and Treatment Data Sets

The proposed model is a statistical model. It needs training and treatment data sets. The training data set is used to train the system and the system takes the data set as a profile or reference data set.

In order to test the algorithm, a system has been set up. The set up includes a switch having 24 interfaces. Data is collected directly from the switch. Data has to be collected for all OIDs of interface group, separately for each of the 24 interfaces. E.g. if we consider the OID ifInOctets from interface group, then we have to poll the ifInOctets value for all the 24 interfaces. For tcp, ip, udp and icmp, every OID value obtained from SNMP MIB are accumulated value for all interfaces, so interfaces need not be considered separately. In total, we monitored 206 OIDs for our experiment, polling each value for 2 seconds. Collecting data for 4 days we had our training data set.

The procedure for collecting treatment dataset is the same as that of training data set. Next, we compare both the training and the treatment data sets using the proposed algorithm and find out the maximum deviation between them, if the maximum deviation is greater than or equal to the critical value (explained in Algorithm section), the dataset can be considered to be anomalous; otherwise the data set is normal. In the experiment, the proposed algorithm detects the appropriate OIDs which behave anomalous along with the IP addresses connected to those interfaces with minimum detection time.

Attacks: The proposed algorithm was tested using hping tool to launch various types of flooding attacks including tcp SYN flood, icmp ping flood, udp flooding, ip flooding etc. Since we are polling data from a switch having 24 interfaces, connected by different hosts, so we target some of the hosts as target hosts for launching attacks. In our experiment we performed attacks from different hosts to the victim hosts and examined the results.

4. RESULTS:

We performed a number of attacks for 24 hours to the victim hosts and the results are shown in Fig 5

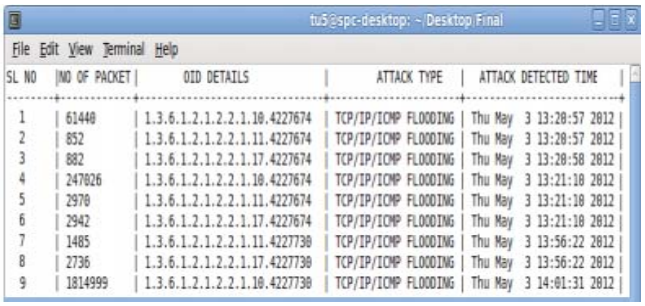

Fig 5

The table shows the minimum number of packets or bytes for which the OID behaves anomalous, the name of the OID, the IP address of the hosts which was targeted, the types of the attacks and the attack detection time. The efficiency of an intrusion detection algorithm depends upon the accuracy rate in terms of the false positive and false negative rate. In our laboratory, this algorithm works fine and detects all attacks. It shows less false positive as well as less false negative.

5. CONCLUSION

In the survey carried out by us, in many of the journals such as [4, 5, 7], researchers have carried out a large number of DOS attacks in their test-bed during which many MIB parameters are examined and monitored. In these experiments, they evaluated the performances of five prominent and promising similarity metrics namely Chi Square, Kolmogorov Smirnov Test, Fractional Among them Kolmogorov Smirnov Test shows the best overall performance and thus the proposed model implements this algorithm. The proposed model takes 2 seconds as polling time, and so the detection time lies in between 2 to 8 seconds, which is more acceptable than the earlier methods. An important feature of the proposed algorithm is that it has the privilege to detect the exact OIDs for which the system behavior is anomalous, the exact number of the packets or bytes for which it deviates from the normal data set, exact attack detection time, the type of attacks as well as the IP address of the victim hosts. The algorithm shows low false positive and the false negative rates. The false positive rate is 0.78124. A striking feature of the proposed model is that although it is a statistical model (because of the fact that anomalies are detected based on statistical data), it behaves as a machine learning model. This is evident because if an anomaly is not detected for a treatment data set, then the normal dataset is updated by the treatment data set, otherwise it remains the same i.e. the machine learns dynamically. Lastly, the proposed algorithm is that it detects anomalies for network based as well as host based systems i.e. if run for a single machine it is capable of detecting for that machine only. On the other hand if the algorithm is run for a network device e.g. switch, it is capable of detecting attacks for the interfaces connected to the switch as well.

The only restriction of the proposed algorithm is that it is capable of detecting DDOS attacks only of the type flooding. It could be further modified to detect scan attacks using FDM (Fractional Deviation from the Mean).

REFERENCES

[1] A.T.Mizrak, S.Savage, K.Marzullo, Detecting Compromised Routers via Packet Forwarding Behaviour ,IEEE Transaction on Networking. Volume: 22,Issue: 2,Publication Year: 2008 , Page(s): 34-39 IEEE Journals.

[2] A.T.Mizrak, S.Savage, K.Marzullo, Detect- ing Malicious Packet Losses ,Parallel and Dis- tributed System .Volume: 20, Issue: 2,Publi- cation Year: 2009 , Page(s): 191 - 206 IEEE Journals.

[3] A.T.Mizrak, Yu-Chung Cheng, K.Marzullo, S.Savage, Detecting and Isolating Malicious Routers ,IEEE Transaction on Dependable and Secure Network.Volume: 3 , Issue: 3,Pub- lication Year: 2006 , Page(s): 230 - 244 .IEEE Journals

[4] Marina.Thottan and Chuanji Ji, Anomaly De- tection in IP Networks , IEEE Journals on Sig- nal Processing, Volume: 51, Issue: 8, Publica- tion Year: 2003.Pages: 2191-2204.

[5] C.Manikopoulos, S.Papavassiliou, Network Intrusion and Fault Detection:A Statistical Anomaly Approach , IEEE Transaction on Telecommunication Network Security. Vol- ume: 40.Issue: 10. Published Year-2002 , Page(s): 76 82.

[6] B.Dong, X.L. Liu, An Improved Intrusion De- tection System Based on Agent , IEEE Con- ference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.page(s): 3164 3167

[7] J.Li, C.Manikopoulos, Early Statistical Anomaly Intrusion Detection of DOS Attacks Using MIB Traffic Parameters , Information Assuarance Workshop, 2003.IEEE systems, Man and cybernetics Society.IEEE conference, Issue Date: 18-20 June 2003 page(s): 53 59.

[8] Gaspary.L.P., Sanchez.R.N., Antunes.D.W., M.E., A SNMPBased Platform for Dis- tributed Stateful Intrusion Detection in Enter- prise Networks IEEE Journal on Selected area in communication .Volume:23, Issue: 10. Pub- lication Year: 2005 , Page(s): 1973 1982.

[9] Bau Cui-Mei, Intrusion detection Based on one-class SVM and SNMP MIB data , IEEE conference on Information Assurance and Se- curity. Volume:2, Publication Year: 2009, Page(s):346-349.

[10] Xinyou Zhang, Chengzhong Li, Wenbin Zheng, Intrusion Prevention System Design , IEEE conference on Computer and Information Technology, Publication Year-2004, Page(s): 386-390

[11] Zarpelao.B.B, Mendes L.S, Proenca M.L, Ro- drigues J, Three Level Network analysis for Anomaly Detection IEEE conference on Soft- ware Telecommunication and Networks, Pub- lication Year: 2009 , Page(s): 281 285.

[12] Zarpelao. B.B., Mendes. L.S., Proenca, M.L., Rodrigues, J.J.P.C, Parameterised Anomaly Detection System with Automatic configura- tion , IEEE conference on Global Telecommu- nication.Publication Year: 2009,Page(s): 1-6.

[13] Cabrera.J.B.D., Lewis. L., Qin. X., Gutier- rez C., Lee, W., Mehra, R.K., Proactive Intrusion Detection And SNMP Based Man- agement: Experiment and Validation , IEEE conference on Integrated Network Manage- ment.Publication Year-2003.Page(s):93-96.

[14] Thottan.M,Chuanyi Ji, Proactive Anomaly Detection Using Distributed Intelligent Agents ., IEEE Transaction on Network.Volume: 12, Issue: 5, Publication Year: 1998, Page(s): 21-27.

[15] Jakobson. G, Weissman. M, Alarm correlation , IEEE Transaction on Network,Volume: 7,Is- sue: 6,Publication Year:1993, Page(s): 52-59.

[16] V.Chandola, A. Banerjee,V.Kumar, Anomaly Detection: A Survey , ACM Computing Sur- veys, Vol. 41, No. 3, Article 15, Publication date: July 2009.

[17] F.Sabahi,A.Movaghar, Intrusion Detection: A Survey , IEEE conference on System and Net- work Communications.Publication Year: 2008 , Page(s): 23 26.

[18] Thottan M,Chuanyi Ji, A Survey of Anomaly Detection Methods in Networks , IEEE journal on Signal Processing.Volume:51,Issue:8, Pub- lication Year:2003,Page(s) 2191-2204.