ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Forecasting Network Flow in IDS

Dr. Dhanakoti, V.

Department of Computer Science and Engineering, VSA Group of Institutions, Salem, India.

ARTICLE INFO

Article history:
Received 12 November 2014
Received in revised form 26 December 2014
Accepted 29 January 2015
Available online 10 February 2015

Keywords:
Congestion Analysis, Network Measurement, Sachet Predictor, Denial of Service and DDoS.

ABSTRACT

Network security mechanisms for congestion processing such as intrusion detection system (IDS) is the need of the hour today to keep up in pace with the high frequency networks. Security solutions in use today are insufficiently reliable as the congestion is quite high of network frequency. For combating the present insufficiency Sachet testing schemes are suggested to be used in the beginning of network screening systems. Presently used testing methods are unreliable because the current scenario in network trafficking is not able to get used to new situations. To meet this immediate requirement with minimum overheads Adaptive testing methods are being proposed on Predicted Sachet testing. The proposed testing method increases the ability of finding denial of Service attacks in Network IDS. This typical method does not reduce the size of the information that is to be scrutinized by an IDS and further more it also retains the essential similar attributes of the network congestion. IDS can use this method to detect DOS attacks if there is a small variation in the congestion similarity.

To Cite This Article: Dr. Dhanakoti, V., Forecasting Network Flow in IDS. ***Aust. J. Basic & Appl. Sci.,*** *9(6): 20-23, 2015*

INTRODUCTION

Internet is growing at a tremendous rapid pace. Hence to provide a reliable mechanism for measuring congestion flow in the networks is required. Security systems in the network (IDS) have not adapted to the current trends in network pace such as gigabytes in Ethernet. Hence there are large scale attacks which utilize the frequency and network bandwidth is a point to be kept in mind. The reason for inability of present results to spot intrusions in huge pace network as it is very expensive using customary network screening plans such as host based and router based screening results. The above plans evaluate network limits of all sachets that pass through the network gadget. The above is also a disadvantage that is tremendously complicated to screen the working patterns of huge number of sachets in huge pace networks (Aitha, N., R. Srinadas, 2011).

Netflow is widely deployed for all principle capacity characteristics of Juniper and Cisco Routers (NetFlow, C., 2012). In the process the quantity of information gathered by the Network flow is problematic, hence to prevail over this size and congestion variety of huge pace networks, the Netflow checks for 1 in M sachet testing. The Sachet testing velocity and parameters are defined physically and are rarely changed. Defining low parameters may result in inaccurate measurement; setting high parameters may end up using more power and large amount of memory particularly on volume of congestion to high and unusual congestion patterns. During idle or small network execution long testing periods provide perfect accuracy with negligible rate but when there is high activity, it requires smaller testing time to precisely calculate the congestion position at the cost of large testing projection. To sort out the above problem adaptive testing have been put forward to automatically regulate the testing time, accuracy and to make best use of it. This adaptive testing method utilize preceding sachet to guess or predict further dimension that is accurate. The adaptive testing is compared to simple cyclic testing and the result thus obtained is used to gauge the performances.

This paper is organized as follows. Reviews of Sachet testing are done in section 2. Section 3 presents Predicted Sachet testing and the projected adaptive weighted testing method. The simulation results and performance analysis with simple cyclic testing are dealt with in section 4. Section 5 concludes and suggests possible areas of application.

Related Work:

The major test in the network is to deploy a testing method and measure its scalability. The ever rising deployment of huge pace networks, large

Corresponding Author: Dr. Dhanakoti, V., Department of Computer Science and Engineering, VSA Group of Institutions, Salem, India.

Internet congestion, the needs for storing a huge size of tested sachets have an important effect on measuring the ability of a testing method. Testing network congestion was commenced in 1994. Claffy et al evaluated three testing approaches to reduce the burden of the network feature to measure communications on the NSFNET backbone (Claffy, K.C., 1993). A testing rate for the adaptive testing method is to make best use of the resources in routers was proposed by Drobisz and Christensen (Drobisz, J. and K.J. Christensen, 2001). The author proposed using sachet based time period and CPU utilization for the above two methods to organize resource utilization and vary the testing rate. The results were able to prove that adaptive method generated better results than static testing method. Fried *et al* concentrated in decreasing the frequency for broadcasting congestion measurement to an isolated server for latter's detailed examination and came up with a volume dependant flow testing method (Friedl, A., 2009).

Proposed Testing Methods:

IP network measuring and screening congestion are the important features of network executions for instance load balancing, weight configuration, etc. In current scenario it is not possible to measure and screen the huge frequency in today's world. Hence Sachet testing has been suggested to handle this problem in this chapter. Traditionally Sachet testing method value was found to be different when measured, which pointed out that there was sudden burst of data in the network over a period of time such as periodic cycle or trends. Section 3.1 describes the Predicted Sachet testing which is used for forecasting the next testing gap. Section 3.2 explains the testing method.

Predicted Sachet Testing:

The array Y clutches the values of the prior M trials, where Y_M is the most current trial, Y_{M-1} prior trial and Y_1 be the oldest trial. In a permanent pane size of M, while the new testing occurs Y_M replaces Y_{M-1} and Y_1 is removed. Predicted Sachet testing replica as a result predicts the value of Y_P prearranged as $Y_1,\ldots..,Y_{M-2},Y_{M-1},Y_M$. Therefore to predict the worth as a task of the past M trials i.e.,

$$\hat{Y}_P = \beta^R \hat{Y} \quad (1)$$

The value $\hat{Y}_P$ characterizes the value predicted used for the subsequent trial. The array $\hat{Y}$ is the array of past M trials and β^R is an array of concurrent predictors which has a great influence on the predicted value $\hat{Y}_P$. Another array r, reports the time of every trial and is replaced in the similar approach as Y. The aim of the predicted sachet testing method is to locate a suitable concurrent array β^R, as a result the subsequent aggregate is reduced.

$$S = \sum_{j=1}^{M} \omega_j \left(Y_j - \hat{Y}_j\right)^2 \quad (2)$$

In Equation (2), ω_j, indicates the weight, Y_j is the actual trialed value and $\hat{Y}_j$ indicate the value predicted in the j^{th} period, correspondingly. The array concurrent is denoted as:

$$\beta^R = (\hat{Y}^R Z \hat{Y})^{-1} \quad \hat{Y}^R Z \quad (3)$$

In Equation (3), $Z = z^R z$ be a $(M-1) \times (M-1)$ diagonal weight matrix and z be $M \times 1$ weight array among weighted coefficient's ω_j that are calculated based on two conditions: 1.The latest of the past M trials. More recent ones have a greater weight, 2. Starting of the time period the value predicted is compared with the prior value. The similar results are calculated by the distance among them. The lesser the distance the more similar it is. Based on the above two condition, weight coefficient is defined as

$$\omega_j = \frac{r_M - r_{M-1}}{M-1} \sum_{j=1}^{M} \left(\frac{Y_{j+1} - Y_j}{(r_{j+1} - r_j) + \Theta} \right), 1 \leq j \leq M \quad (4)$$

Where Θ be a value to evade division with zero.

Adaptive Predicted Testing Method:

Adaptive testing method alters the testing speed depending on the previous tested data. The main feature within the adaptive testing is upcoming performance which is predicted depends on the experimental results of the trials. Adaptive predicted testing method explained in this section uses the Predicted Sachet testing method as shown in section 3.1 to pick the next testing period. In Predicted Sachet testing if there is an inaccurate prediction, then there is a need to alter the testing speed.

Adaptive Predicted Testing Method has the subsequent features:

i. Pick the first M testing periods equal to σ. (Where σ = 120 seconds and M = 20)
ii. Assign Predicted Sachet testing to forecast the predictable value, $\hat{Y}_P$, belonging to the network.
iii. When the testing time period comes to a finish, the network factor value is measured.
iv. The predicted value is evaluated with the actual value.
v. The predefined rule is used to adjust the testing rate in case the forecasted value differs from that of the genuine value.

The forecasted result, $\hat{Y}_P$, obtained from the prior M trials, is being evaluated among the trial's original value, Y_{ACT}. Predefined group of laws are used for regulating the present testing period, $\Delta U_{Curr} = r_M - r_{M-1}$, for obtaining a latest value, ΔU_{New}, the obtained value is utilized to program the management questions. Predefined group of laws is put into use by regulating the testing period and evaluating pace of alteration within the forecasted value, $\hat{Y}_P - Y_M$, to the original speed of adjustment, $Y_{ACT} - Y_M$. P, the proportion among both the speeds is described below:

$$P = \left|\frac{\hat{Y}_P - Y_M}{Y_{ACT} - Y_M}\right| \quad (5)$$

The limit of P value is defined as $P_{MIN} < 1 < P_{MAX}$ and the subsequently testing period ΔU_{New} is revealed in the Equation (6). The Equation (6), $\gamma 1$ and $\gamma 2$ are adjustable limits and to set standards for $\gamma 1$ and $\gamma 2$ altering the speed of network features is a point to be remembered. As in Hernandez *et al*, (2001) the values $\gamma 1 = 2$ and $\gamma 2 = 2$ are used in the proposed simulations.

$$\Delta U_{New} = \begin{cases} (1 + P) \times \Delta U_{Curr} & \text{if } P > P_{MAX} \\ \gamma 1 \times \Delta U_{Curr} & \text{if } P_{MIN} < P < P_{MAX} \\ P \times \Delta U_{Curr} & \text{if } P < P_{MIN} \\ \gamma 2 \times \Delta U_{Curr} & \text{if P is Undefined} \end{cases} \quad (6)$$

P is equivalent to 1 while the forecasted value is similar to the monitored value. In case P is below P_{MIN}, then it signifies with the intention that the value calculated is altered quicker than that of the forecasted value which shows the symptom that the testing period should be decreased. In case P is above P_{MAX}, then it signifies with the intention that the value calculated is altered slower than that of the forecasted value which shows the symptom that the testing period should be increased. Alternatively P has a value which is possibly not known. It happens while the denominator and numerator are equal to nil in equation 5. The present situation shows that the network is in an inactive state or in a firmly fixed position. So in a current situation the testing period is improved with a element ($\gamma 2 > 1$). During the experiment session the P_{MIN} and P_{MAX} are assigned with 0.87 and 1.16 correspondingly. The above standards are chosen because of excellent results in a large area of congestion types.

Performance Evaluations:

Genetic evaluate the proposed adaptive testing method simulations were used by the information received through ICE Pvt Ltd, where the above project network contains connectivity from speed 2 mbps till 1000 mbps. The database is evaluated for 24 hours sample. The criteria used in evaluating the simple cyclic testing with adaptive testing method were the Mean Square Error (MSE) of the population that is being estimated. The mean square error of estimator Z is defined as an inconsolable limit λ where $Z = Eq (Z - \lambda)^2$. Root Mean Square Error (RMSE) be defined as square root of mean square error and the RMSE be reduced while $\lambda = Eq(Z)$ and hence Standard Deviation(SD) of Z is the smallest element.

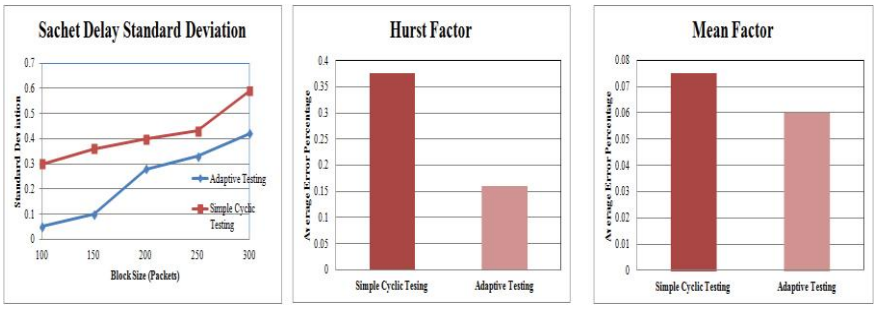

Fig. 2: Sachet Delay. **Fig. 3, Fig. 4:** Error Percentage using Hurst Factor and Mean Factor.

In the Figure 2 the adaptive testing method which is proposed is compared to simple cyclic testing method with means of SD for sachet interruption as similarity criteria. The worms and attacks that concentrate on lowering the quality of Internet Protocol networks uses sachet delay as a major criterion (Patcha, A. and J. Park, 2006). The results indicate that the simple cyclic testing method has a higher SD than adaptive plan. RMSE is straightforwardly proportional to SD. The projected method forecasts that the sachet means interruption better while reducing the congestion volume when compared to the simple cyclic testing method.

The newly proposed testing plan when experimented with the second data set shows that it posses self similarity features. For these two different parameters were used: (1) the mean of the sachet count (2) Hurst Factor. The Peak to Mean Ratio (PMR) is used to calculate the similarity by evaluating highest value of the element calculated among the mean value of the residents and used as an indicator of high congestion. But this has drawbacks also, that is it is more reliable on the size of the periods so it might or might not indicate the genuine congestion characteristics. Hurst Factor produced more reliable and precise gauge for huge congestion. In the Figures 3 and 4 Hurst factor clarifies the mean testing error and trial average correspondingly. Figure 3 show the simple cyclic testing method has larger average error percentage (0.37%) for the Hurst Factor while evaluated with adaptive testing method (0.16%). The failure of data might be due to number of testing periods. Figure 4 depicts the adaptive testing method has smaller average error percentage (0.06%) for the Mean Factor while evaluated with simple cyclic testing method (0.075%). However,

differences were very minimal. Hence it can be considered significant. This small difference is because of the inbuilt adaptive quality in the testing method. Testing method projected has a possibility to let pass small burst of actions in the network during the period of classically having low network congestion. Moreover, the cyclic testing plan is a possibility to contain such drawbacks as well.

Conclusion:

The adaptive testing method has been presented in which the Predicted Sachet testing is used to vigorously change the testing speed which depends on precision of the predicted value. Results thus obtained shows when data is cyclic or large adaptive testing method executes superior than simple cyclic testing. From the result the simulation outcomes have proved that planned testing method has been more efficient in decreasing the information quantity and more over maintaining the basic characteristics of the network. Hence, it could be employed in a vast range of purposes in screening and protections of networks.

REFERENCES

Aitha, N., R. Srinadas, 2011. A Strategy to Reduce the Control Packet Load of AODV Using Weighted Rough Set Model for MANET. *The International Arab Journal of Information Technology*, 8(1): 108-116.

Claffy, K.C., G.C. Polyzos, H.W. Braun, 1993. Application of sampling methodologies to network traffic characterization. *In ACM SIGCOMM '93: Proceedings of the Conference on Communications architectures, protocols and applications, (San Francisco, USA), ACM Press*, pp: 194-203.

Drobisz, J. and K.J. Christensen, 2001. Adaptive Sampling Methods for High Speed Networks to Determine Traffic Statistics including the Hurst Parameter. *Master's Thesis, University of South Florida*.

Friedl, A., S. Ubik, A. Kapravelos, 2009. Realistic Passive Packet Loss Measurement for High-Speed Networks. *Traffic Monitoring and Analysis, Lecture Notes in Computer Science*, 5537: 1-7.

Hernandez, E.A., M.C. Chidester, A.D. George, 2001. Adaptive sampling for network management. *Journal of Network and Systems Management*, 9: 409-434.

NetFlow, C., 2012. CISCO NetFlow. http://www.cisco.com.

Patcha, A. and J. Park, 2006. An Adaptive Sampling Algorithm with Applications to Denial-of-Service Attack Detection. *Computer Communications and Networks*, pp: 11-16.