International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34372-34374

Network Anomaly Detection Stochastic Model Analysis

D. Ayyamuthukumar[1], S. Karthik[2], A. Rajivkannan[3]
Department of CSE, K.S.Rangasamy College of Technology,Tiruchengode, Namakkal, Tamilnadu-637215, 94430-15341, ukdkumaarcse@gmail.com.
Professor & Dean, Department of CSE, SNS College of Technology,Coimbatore, Tamilnadu-641035, 9842720118 profkarthik@gmail.com
Professor, Department of CSE, K.S.R. College of Engineering,Tiruchengode, Namakkal, Tamilnadu-637215, 9842761811, rajiv5757@yahoo.co.in

Abstract- DDoS attacks threaten the functionality, reliability, availability, and maintainability of IP networks. Correct and early detection is vital for mitigation. In this paper, network traffic is modelled as a stochastic process Y(t) = X(t) + N(t) ,where Y ,X . N ,are observed, genuine, and flooding traffics respectively .Using the properties of stochastic processes we find SY(f) = Sx (f) + Sn (f) in the frequency domain in spectral densities under certain conditions .This enables to detect flooding and take appropriate measures for mitigation.

Keywords- network, anomaly detection, stochastic model, spectral density

I. Introduction

The modern network is expected effectively, to offer a boundless communication paradigm thereby offering *anytime, anywhere, anyhow*

Communication for all its users. Recent surveys [1] indicate that DDoS attacks pose a critical threat to the internet. Hackers motivated by Financial rewards use botnets to commit these crimes.[2] A concerted security effort which involves cooperation dissipated among all, at various levels of the architecture is therefore necessary for securing the network **early enough from external attacks.[3] Time** series methods have also been proposed for modelling and predicting network traffic.[4] In reality the network traffic is essentially a stochastic process Y = X + N where X and N are independent stochastic processes representing respectively, genuine and destructive traffic. Stochastic model analysis of anomaly detection is the goal of this paper.

2. Mathematical Basis [5 -7]

a. Stochastic processes

A stochastic process X(t) is a mapping of outcomes of an experiment to functions of time. X(t) is both the name of the process as well as the name of the random variable observed at time t. A probability model for X(t) consists of the joint PMF or joint PDF for all possible $\{t_1,t_2, ,t_k\}$ The IID random sequence X_1,X_2, . . is a discrete time stochastic process consisting of a sequence of independent identically distributed random variables.

The Poisson process is a memory less counting process in which an arrival at a particular instant is independent of an arrival at any other instant.

A stochastic process is stationary if its randomness does not vary with time. A stochastic process is wide sense stationary if its expected value is constant with time and the autocorrelation function depends only on the time difference between two random variables.

The auto covariance and autocorrelation functions indicate the rate of change of the sample functions of a stochastic process. The cross covariance and cross correlation functions represent the relationship of two wide sense stationary processes. Two random processes X(t) , Y(t) are jointly wide sense stationary if each of them are so and their cross correlation function

$$R_{XY}(t, \tau) = R_{XY}(\tau) \quad (2.1)$$

X(t) is a gaussian stochastic process if and if $X = \{X(t_1),.....X(t_k)\}^t$ is a gaussian random vector for any integer $k > 0$ and any set of time instants. A wide sense stationary gaussian process is stationary.

b. Power Spectral Density Of A Stochastic Process

The autocorrelation function of a stochastic process conveys information about the time structure of the process. If X(t) is stationary and $R_X(\tau)$ decreases with increasing τ , it is likely that the sample function of $X(t)$ will change abruptly in a short time.Fourier transforms offer another view of the variability of functions of time. A rapidly varying function of time has a fourier transform with a high magnitude at high frequencies and a slowly varying time function has a fourier transform with low magnitude at high frequencies. In the study of stochastic processes the power spectral density function $S_X(f)$ provides a frequency domain representation of the time structure of X(t) and is defined as the expected value of the squared magnitude of the fourier transform of a sample function of X(t), and is calculated as the fourier transform

(Discrete or continuous) of the autocorrelation $R_X(\tau$ [?]) of X(t).

Wiener Kintchine property states that

$$s_x(f) = \int_{-\infty}^{\infty} R_x(\tau) e^{-j2\pi f\tau} d\tau \quad (2.2)$$

$$R_x(f) = \int_{-\infty}^{\infty} S_x(f) e^{j2\pi f\tau} df \quad (2.3)$$

$S_x(f)$ has the following properties, then

i) $S_X(f) \geq 0$ for all (2.4)

ii) $\int_{-\infty}^{\infty} S_x(f)\, df = E(X^2(t)) = R_X(0)$ (2.5)

iii) $S_X(f) = S_x(-f)$ (2.6)

For jointly WSS processes X(t) and Y(t) the fourier transform of the cross correlation function $R_{xy}(\tau)$ gives the cross spectral density

$$s_{xy}(f) = \int_{-\infty}^{\infty} R_{xy}(\tau) e^{-j2\pi f\tau} d\tau \quad (2.7)$$

For jointly WSS processes X and Y , with Z= X + Y ,

$R_Z(\tau) = R_X + R_{xy} + R_{yx} + R_Y$ (2.8)

and

$S_Z(f) = S_X + S_{xy} + S_{YX} + S_y$ (2.9)

If further X and Y are independent

$R_z(\tau) = R_X + R_y$ (2.10)

and

$S_Z(f) = S_X + S_y$ (2.11)

3. DDoS Attack Detection Problem In Network Traffic

DDoS attacks in network traffic, should be detected early to mitigate their destructive potential. Researchers have designed and implemented a number of countermeasures based on traffic features. In this paper detection problem based on stochastic model power spectral density is discussed.

4. Assumptions

a) The regular traffic and the flooding traffic are wide sense stationary discrete random processes X(t) ,N(t) respectively.

b) X and N are independent and hence are jointly WSS and we can show that Y = X + N the observed traffic is a WSS stochastic process.

c) Because of irregularity E(N(t)) = $\mu_N = 0$.

5. The Detection Procedure

The observed traffic Y(t) = X(t) + N(t) is sampled periodically, the period and the sample size determined from past performance of the process and the power spectral density is computed using MATLAB or appropriate software.{As the expected value of the squared magnitude of Fourier transform of the sample values}

The obtained power spectral density function values are critically examined. If these values are HIGH then (since a rapidly varying function of time has a Fourier transform with high magnitudes) flooding / DDoS attacks are present and appropriate measures can be taken.

6. Theorem

When The values of $S_y(f)$ where Y = X + N (X , N are the regular and flooding traffic stochastic processes and Y is the observed traffic) are high then a DDoS attack is taking place.

Proof : When WSS processes X ,N which are independent are the components of Y , then we can show spectral densities S_Y , S_x ., S_N satisfy $S_Y = S_x + S_N$

For a regular traffic process X , S_x will not be high/ vary much with frequency f since the traffic X is steady and nearly time invariant. Hence the huge variations/values observed in S_Y can only be due to high values/variations in S_N. Hence huge values of S_N only contribute to huge values of S_Y. Again huge variations in N(t) are mainly due to flooding/DDoS attacks and THESE make the value of S_N large. and those of S_Y in turn.

Huge values of S_Y indicate therefore DDoS attacks.

7. Conclusion

Network traffic can be bifurcated into two parts: regular part X and a non-regular attack part N. The observed traffic Y = X + N , is the sum of two independent WSS stochastic processes and hence is itself a WSS stochastic process. The autocorrelation function of a stochastic process is a measure of its time variance. Fourier transforms offer another view of the variability of functions of time whose ensemble a stochastic process is.

A rapidly varying function of time (DDoS) has a fourier transform with high magnitudes. Thus the power spectral density $S_Y(f)$ provides a frequency domain representation of the time structure of process Y(t)

Under certain broad conditions we can show $S_Y = S_X + S_N$ and large values of S_N contribute to large values S_Y and hence DDoS/flooding is indicated when S_Y is large.

This is the result of the stochastic model analysis. This is easy to implement for detection of network attacks.

Reference

[1] Arbor," IP flow-based technology", 2011, http://www.arbornetworks.com.

[2] B.Stone-Gross, M. Cova, l. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel and G. Vigna, "Your Botnet is My Botnet : Analysis of a Botnet takeover", 2009, Proc., ACM Conference on Computer comm. Security.

[3] H. Moiin, Dec. 2006, "Next generation mobile networks beyond HSPA & EVDO," white paper, NGMN Alliance ., pp 1- 72,

[4] G. Carl, G. Kesidis, R. Brooks, and S. Rai, Jan./Feb. 2006, " Denial-of- Service Attack detection techniques "IEEE internet computing ., vol 10 ., No 1 pp. 82-89

[5] E. Parzen .,"Probability theory and its applications".,wiley .,New york [6] V .G. Kulkarni , 2009, " Modeling and analysis of stochastic systems"., Chapman and hall book.

[7] J Payser, 2013, "Stochastic analysis , estimation and control", Eastern economy edition .,

AUTHOR PROFILE

Mr. D. Ayyamuthukumar received his Bachelor degree in Electrical and Electronics Engineering from Bharathiyar University in the year 1997 and Masters degree in Computer Science and Engineering from Anna University, Chennai in the year 2004. He has published 1 paper in International Journal. He has also attended 8 National Conferences and 4 International Conferences. He is life member of ISTE.

Dr. S. Karthik received his Masters degree in Computer Science and Engineering from Anna University, Chennai in the year 2004. He has published 15 paper in International Journal. He has also attended 20 National Conferences and 34 International Conferences. He is life member of ISTE.

Dr. A. Rajivkannan received his Bachelors degree in Information Technology in the year 2002 and Masters degree in Computer Science and Engineering from Anna University, Chennai in the year 2004. He has published 20 paper in International Journal. He has also attended 5 National Conferences and 5 International Conferences. He is life member of ISTE.