PREDICTION OF MALICIOUS OBJECTS IN COMPUTER NETWORK AND DEFENSE

Hemraj Sainia[1], T. C. Panda[2], Minaketan Panda[3]

[1]Department of Computer Science & engineering,
Alwar Institute of Engineering & Technology, India
hemraj1977@yahoo.co.in

[2]Department of Applied Mathematics,
Orissa Engineering College, Bhubaneswar, Orissa, India
tc_panda@yahoo.com

[3]Engineer, Presales & Planning,
SPANCO TELE, Chandigarh, India
tominaketa@gmail.com

ABSTRACT

The paper envisages defense of critical information used in Computer Networks those are using Network Topologies such as Star Topology. The first part of the paper develops a model to predict the malicious traffic from the incoming traffic by using Black Scholes Equations. MATLAB is used to simulate the developed model for realistic values. However, the second part of the problem provides a framework for the treatment of predicted malicious traffic with detailed discussion of security measures.

KEYWORDS

Malicious Object, Black Scholes Equations, Star Topology, Anti Malicious Objects, System Hardening, Friendly-Cooperative Framework

1. INTRODUCTION

Models for malicious object propagation in the computer networks are well discussed in literature [1, 2, 3, 4, 5] but its propagation in network topology [6, 7, 8] is not adequately documented. Network topology plays an important role for various factors such as speed of propagation, server management, band width usage etc. Hence, before deciding the malicious object's dynamics, the network topology must be considered.

The paper uses star topology [9] for deciding the dynamics of malicious objects as it is widely used network topology. A star topology is depicted in figure-1 where the server is centrally located and connected with the outer world through ISP. The incoming traffic from ISP having malicious objects and may enter into the network and destroy the network or steal the information. The work presented in the paper predicts the malicious traffic by using the Black Scholes Equations [10, 11], which are the most widely used equations to predict the portfolio of financial market. Cyber Attacks are totally analogous to financial market. The uncertainty of the option price in the financial market is similar to the uncertainty of the cyber attacks. Other feature such as input to the financial market is similar to number of cyber attackers, pattern of change of option price is similar to the change in the rate of malicious objects, and the effect of strike price is compatible to the effect of Anti Malicious Software (AMS) [12, 13] i.e. number of malicious objects already restricted by the AMS. In addition, the

DOI : 10.5121/ijnsa.2011.3612

change in option price is affected by multi factors similar to the number of incoming malicious objects in the cyber world and these are uncertain for every attack.

The predicted malicious traffic is isolated and cured by security measures and then again put in to the regular traffic. In addition the information about the malicious traffic is parallelly transferred to all the connected nodes so that they can make themselves self-harden [14, 15] enough to face the attack by using the friendly-cooperative-framework.

In addition to Introduction, the paper envisages model formulation as section-II, friendly cooperative framework for processing the malicious information as section-III and finally the conclusion and future direction to the work as section-IV.

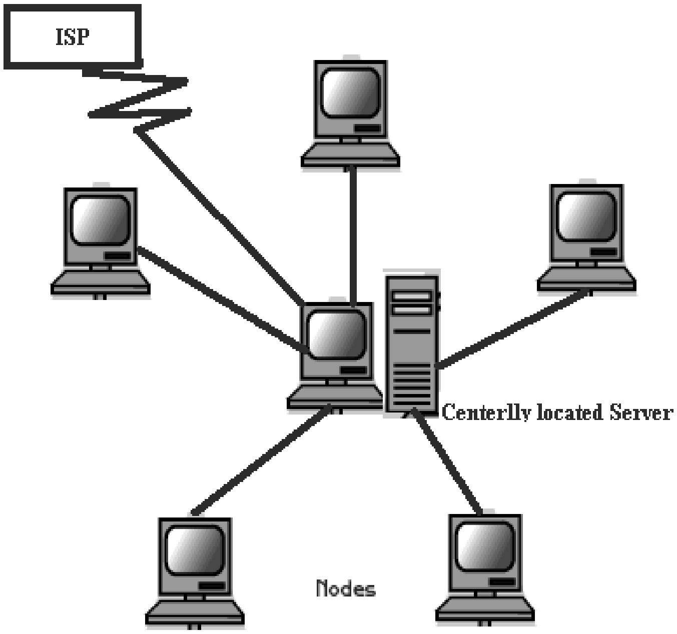

Figure-1: Star Topology

2. MODEL FORMULATION

The normal functioning of the server ensures the smoothness and malicious objects free environment of the network as far as star topology is concerned. If the server gets down then all the nodes or clients will also remain in idle condition, and as such cannot communicate each other as well as with the outer world. Hence, sever is the only gateway for the communication.

The incoming traffic is in the form of packets with destination address. The server receives the packets first and diverts the packets to the nodes as shown in the figure-2.

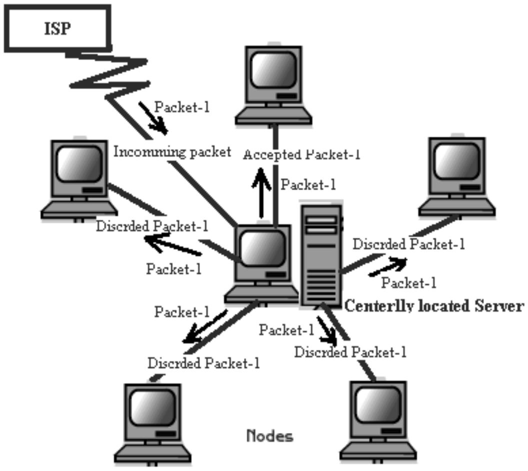

Figure-2: Packet transferring in star Topology

Packet-1 is broadcasted to all the nodes after it is received by the server. The concern node accepts it and other discard. By analyzing the traffic pattern one can separate the suspected traffic and can take security measures. Signature based methods are the most widely used methods to identify the malicious traffic. But if signature database is not having the signature of incoming traffic then it cannot be detected. In such a situation we have to use some of predictable approach, in our case we are using the Black Scholes equations to predict the malicious traffic.

Let number of incoming packets at any instance t are N, from which any random packet may be a malicious packet. The connection from star network to its ISP is continuous and so the packets are continuously transmitting to and fro.

Let the traffic is coming with $\Delta x / \Delta t$ speed. As the traffic is having two parts, one is malicious and second non-malicious, so, we assume that the probability of being malicious is p and non-malicious is q, p + q=1. For n spans of time Δt, the total time of which the malicious objects are to be find is given by-

$$t = n\Delta t \qquad \text{(a)}$$

So, the number of total malicious/non-malicious objects in time t is $x(t)$ and given by-

$$x(t) = z_1 + z_2 + z_3 + ... + z_n \qquad (1)$$

Where, z_i (I = 1, 2, …, n) is the number of malicious/non-malicious objects.

The expectation of total traffic is as under-

$$E(x(t)) = E(z_1) + E(z_2) + E(z_3) + ... + E(z_n) \qquad (2)$$

Where, $E(z_i)$ represents the ith time span expectation of being either malicious/non-malicious.

Above equation (2) can be rewritten as-

$$E(x(t)) = \sum_{i=1}^{n} p_i x_i \tag{3}$$

Now, $E(z_i)$ will be given by-

$$E(z_i) = (p\Delta x) + (-q\Delta x)$$

$$= (p-q)\Delta x \tag{4}$$

Where, i=1, 2, …, n so, equation-(3) can be expended by using equation-(4) as follows-

$$E(x(t)) - (p-q)\Delta x + (p-q)\Delta x + ... + (p-q)\Delta x$$

$$E(x(t)) = n(p-q)\Delta x \tag{5}$$

The variance of the traffic is calculated as follows, which represents the behavior of traffic of being malicious/non-malicious.

$$Var(x) = \sigma^2 = (E(x^2)) - (E(x))^2 \tag{6}$$

Equation-(6) leads that

$$Var(z_i) = (E(z_i{}^2)) - (E(z_i))^2$$

$$= p(\Delta x)^2 + (-q(\Delta x)^2 - ((p-q)\Delta x)^2$$

$$= 4pq(\Delta x)^2$$

$$Var(\sum_{i=0}^{n} x_i) = \sum_{i=0}^{n} Var(x_i)$$

Or

$$Var(x(t)) = 4npq(\Delta x)^2 \tag{7}$$

Equation-(5) represents the instantaneous expectation. Now,

$$E_{inst} = Limit_{\Delta t \to 0} \frac{(p-q)\Delta x}{\Delta t} \tag{8}$$

Thus from equation-(a) and equation-(8) we have-

$$Limit_{\Delta t \to o} E(x(t)) = Limit_{\Delta t \to o} \frac{t(p-q)}{\Delta t} = t.\mu \tag{9}$$

as the traffic is continuous to the network.

Similarly the instantaneous variance can be given as under-

$$\sigma^2 = Limit_{\Delta t \to 0} \frac{4pq(\Delta x)^2}{\Delta t}$$ or

$$Var(x(t)) = Limit_{\Delta t \to 0} 4.\frac{t}{\Delta t}.pq(\Delta x)^2 = t\sigma^2 \tag{10}$$

Initially there are no malicious objects in the network and the possibility of malicious objects in the further independently incremented time span does not depend on each other. In addition we assuming that the value of malicious objects at time t i.e. $x(t)$ follows normal distribution [16] with mean $\mu.t$ or $\sigma^2 t$, which are derived in equation-(9) and equation –(10) separately.

In other words, the variable $x(t)$ is a stochastic process with respect to time t.

Now, the traffic is continuous and represented by Standard Normal distribution, which is given by-

$$\Phi = \frac{x(t) - \mu t}{\sigma\sqrt{t}} \tag{11}$$

Φ is a Standard Normal Distribution with mean zero and variance one i.e. $E(\Phi) = 0$ and $Var(\Phi) = 0$ So, from equation-(11)-

$$x(t) = \mu t + \sigma\sqrt{t}\Phi$$

$$\Rightarrow x(t) = \mu(t) + \sigma\omega(t) \tag{12}$$

If $\mu = 0$ and $\sigma = 1$ then

$x(t) = \omega(t)$, where, $\omega(t)$ is a wiener's process.

Now, as $x(t)$, the number of malicious objects in time t, is a stochastic process and hence $x(t)$ is said to follow a Geometric Brownian Motion (GBM) [17], which satisfies the following stochastic deferential equation-

$$dx(t) = \mu x(t)dt + \sigma(x(t))d\omega \tag{13}$$

Additionally, the stochastic process $x(t)$ is an ITO-Process and satisfies the below equation-

$$dx(t) = \mu(x(t),t)dt + \sigma(x(t),t)d\omega \tag{14}$$

Now, the evolution of malicious objects in the network traffic follows GBM in a long normal distribution form i.e. the deviation in general behavior is very less within the range say, $\pm 5\%$.

The change of the incoming malicious objects in the short period of the computation of the number of incoming malicious objects in the traffic is almost constant.

There is no extra load of malicious objects in the system as the AMS is running to overcome of it.

By above conclusions, we can say the number of malicious objects represented by $V(S,t)$ where, S is a stochastic process [18] which represents the last counted number of malicious objects.

Let present time is t and the number of malicious objects in the network is π which is given by-

$$\pi = V - \Delta s\,, \tag{15}$$

Where V is the maximum possible value of $V(S,t)$ and Δs is the small value changed in the number of malicious objects.

After time period dt the number of malicious objects will be increased by $d\pi$ and becomes $\pi + d\pi$ i.e.

$$\pi + d\pi = (V - \Delta s) + d\pi$$

$$= (V + dV) - \Delta(s + ds) \tag{16}$$

The change in the value of the number of malicious objects in time dt is $d\pi$ and given by-

$$d\pi = (\pi + d\pi) - \pi \tag{17}$$

By equation (15) to (16)-

$$d\pi = dV - \Delta ds \tag{18}$$

Since V satisfies GBM. Hence by ITO’s lemma is-

$$dV = \left(\frac{\partial V}{\partial t} + \frac{1}{2}\sigma^2 s^2 \frac{\partial^2 V}{\sigma s^2} + \mu s \frac{\partial V}{\partial s} \right) \partial t + \frac{\partial V}{\partial s} \sigma s dx \tag{19}$$

The solution of equation – (19) can be obtained by the following process:-

Let there are k time spans of duration δt in the total time T to compute the total number of malicious objects and the Malicious Object Updating (MOU) Step as δs such that

$\delta t = \frac{T}{k}$, $\delta s = \frac{S_i}{I}$, where $0 \le i \le I$.

So, we can get the solution to obtain the number of malicious objects, $V(S_i, t_k) \equiv V_i^k$ for the already identified malicious objects by AMS, S_i and for kth time span of the total time, where $0 \le i \le I$ & $0 \le k \le K$, which can be obtained by the following equation-(20).

$$\frac{V_i^k - V_i^{k+1}}{\delta t} + \frac{1}{2}\sigma^2 S_i^2 \left[\frac{V_{i+1}{}^k - 2V_i^k + V_{i-1}{}^k}{(\delta s)^2} \right] + \mu S_i \left(\frac{V_{i+1}{}^k - V_{i-1}{}^k}{2\delta s} \right) - \mu V_i^k = 0 \tag{20}$$

Where i=1, 2, …, I-1 and k=0, 1, 2, …., K-1

$$V_i^{k+1} = A_i V_{i-1}{}^k + B_i V_i^k + C_i V_{i+1}{}^k \tag{21}$$

Where A_i, B_i and C_i are constants given by following equation-(22).

$$A_i = \frac{T}{K}\left[\sigma^2 I^2 - \mu I\right]; \quad B_i = \left[\frac{K - T\sigma^2 I^2 - \mu T}{K}\right]; \quad C_i = \frac{T}{2K}\left[\sigma^2 I^2 + \mu I\right] \tag{22}$$

3. Defending Mechanism

Figure-3 shows the MATLAB simulation of the equation-(20) for the number of malicious objects already identified by AMS as 10.

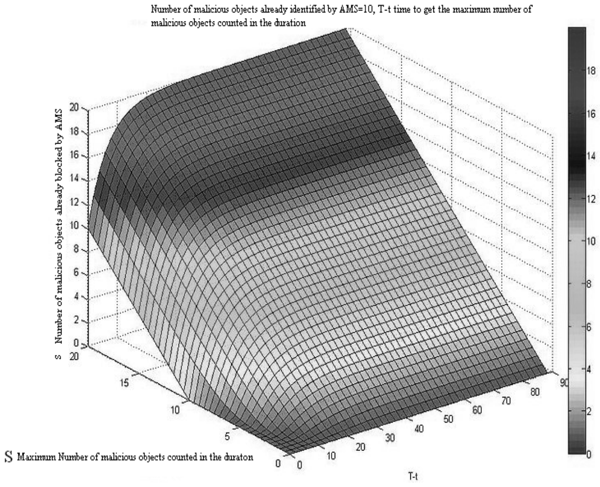

Figure-3: Relation among s, S and t

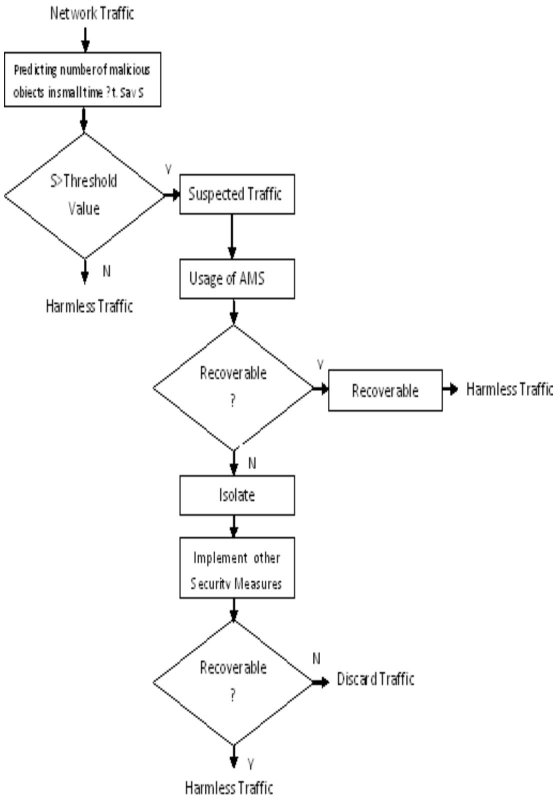

Figure-4: Traffic analysis algorithm

As soon as the prediction of the number of malicious objects increases by a threshold value, the traffic becomes the suspected one and may be isolated either to ignore or to deploy the security measures over it as shown in the figure-4.

The threshold value used in figure-4 can be easily computed from the figure-3. It represents the maximum number of malicious objects counted at any moment where it goes up from the maximum number of malicious objects already blocked by AMS.

4. FRIENDLY COOPERATIVE FRAMEWORK FOR PROCESSING THE MALICIOUS INFORMATION

As the suspected traffic is isolated for its diagnostic purpose and once it got a confirmation to be the malicious then its signature and source has to be spread to all the connected nodes. This information is communicated by using friendly cooperative framework as shown in figure-5.

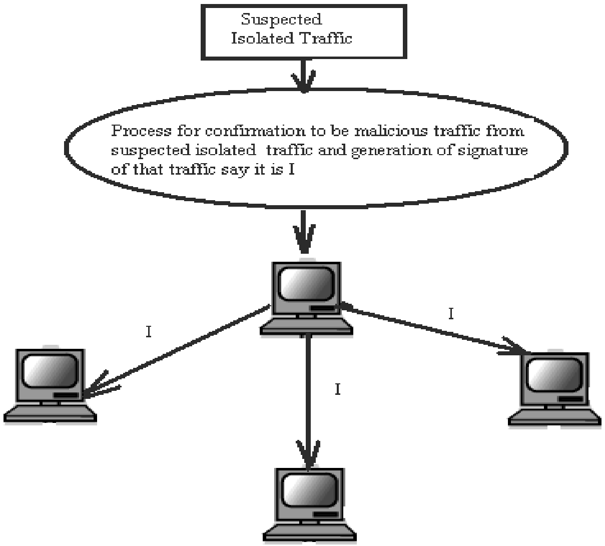
Suspected
Isolated Traffic
Process for confirmation to be malicious traffic from suspected isolated traffic and generation of signature of that traffic say it is I
I
I
I

Figure-5: Friendly cooperative framework for information transfer to all directly connected nodes.

5. CONCLUSION AND FUTURE DIRECTION TO THE WORK

The Black Scholes equations are used to predict the behavior of network traffic and the simulation for already identified malicious objects by AMS at a specific time interval is made, which is more realistic in the real time scenario. On the basis of simulated results a proposal is provided to identify the traffic in which the possibility of the number of malicious objects is beyond a threshold value and will be thus termed as suspected traffic. This suspected traffic is then treated through security measures to make it a regular traffic. In addition, a framework is also provided to propagate the generated malicious information to all the directly connected nodes or friendly nodes.

References

[1] Ossama A. Toutonji, Seong-Moo Yoo, and Moongyu Park (2010), "*Propagation modeling and analysis of network worm attack",* In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10), ACM, New York, NY, USA, , Article 48, 4 pages. DOI=10.1145/1852666.1852719 http://doi.acm.org/10.1145/18526661852719

[2] T. R. Tidwell, K. Fitch Larson, J. Hale (2001), "*Modeling Internet Attacks",* Proceedings of the IEEE Workshop on Information Assurance and Security, Unites States Military Academy, West Point, NY.

[3] Hemraj Saini, Dinesh Saini (2007), "*Malicious Object dynamics in the presence of Anti Malicious Software",* European Journal of Scientific Research, volume-18, Issue-3, pp.-491-499

[4] Hemraj Saini (2009), "*Queuing Model for Malicious Attack Detection"*, The Icfai University Journal of Information Technology, 5(2) 16-28

[5] Hemraj Saini, Dinesh Saini (2008), "*VAIN: A Stochastic Model for Dynamics of Malicious Objects",* ICFAI journal of Systems Management, Vol. 6, No. 1, pp. 14-28

[6] Jean Wairand (1998), "*Communication Networks (A first Course")*, Second Edition, WCB/McGraw Hill.

[7] Behrouz, Forouzan (2001), "*Introduction to Data Communication and Networking"*, 2nd Edition, TMH.

[8] Andrew S Tanenbaum, *Computer Networks*, 4th, (2002), Prentice Hall PTR.

[9] FitzGerald, Jerry, Alan Dennis (1999), "*Business Data Communications and Networking"*, 6th ed., New York: John Wiley & Sons.

[10] R. Company, E. Navarro, J. Ramón Pintos, E. Ponsoda (2008), "*Numerical solution of linear and nonlinear Black-Scholes option pricing equations*" Comput. Math. Appl., 56, 3 813-821. DOI= http://dx.doi.org/10.1016/j.camwa.2008. 02.010

[11] G. Barles, H. M. Soner (1998), "*Option pricing with transaction costs and a nonlinear Black-Scholes equation"*. Finance Stochast., v2. 369-397.

[12] K. Lakkaraju, and A. Slagell (2008), "*Evaluating the utility of anonymized network traces for intrusion detection"*, In Proceedings of the 4th international Conference on Security and Privacy in Communication Netowrks (Istanbul, Turkey, September 22 - 25. SecureComm '08. ACM, New York, NY, 1-8. DOI= http://doi.acm.org /10.1145/1460877.1460899

[13] Nick Clemente (2007), "System Hardening The Process of Defending and Securing Today's Information Systems", Journal of Security Education, 2(4) 89 – 118

[14] Hemraj Saini, Dinesh Kumar Saini (2007), "*Proactive cyber Defense and Reconfigurable Framework of Cyber Security",* International journal named International Review on Computer and Software, 2(2) 89-97

[15] H. Saini, D. K. Saini (2006), "*Cyber Defense Architecture in Campus Wide Network",* 3rd International Conference on Quality, Reliability and INFOCOM Technology (Trends and Future), Indian National Science Academy, New Delhi (INDIA), 2-4 December, Souvenir pp. 62

[16] M. G. Kendall, A. Stuart (1977), "*The advanced theory of statistics"*, Griffin.

[17] A. Borodin, P. Salminen (2002), *Handbook of Brownian Motion - Facts and Formulae*, 2nd Edn., Birkhauser Verlag.

[18] L. Arnold (1974), "*Stochastic differential equations"*, Wiley (Translated from Russian).

Hemraj Saini is a faculty member in the Department of Computer Science & Engineering, Alwar Institute of Engineering & Technology, Alwar, India – 752050. He received his B.Tech. in CS&E from NIT Hamirpur (H.P.) and M.Tech. degree in Information Technology from the Punjabi University Patiala, Punjab in 1999 and 2005 respectively. He has submitted his Ph.D. in Utkal University, Vani Vihar, Bhubaneswar. His main professional interests are in Mathematical Modeling, Simulation, Cyber Defense, Network Security and Intelligent Techniques

T. C. Panda is a Retd. Professor of Mathematics (Berhampur University, India), Founder Professor of Mathematics & Computer Sc. (Mizoram Central University, India) and currently associated as Principal with Orissa Engineering College, Bhubaneswar, Orissa, India-752050. He received his Masters from Banaras Hindu University in 1968 and Ph. D. from Berhampur University in 1975. His main interests are Fluid Dynamics, Air Pollution Modeling, Monsoon Dynamics, Numerical Weather Prediction, Meso-Scale Modeling, Remote Sensing Techniques, Numerical Solution of Partial Differential Equations and Cyber Defense.

Minaketan Panda is an Engineer SPANCO-TELE, a multinational company. He received his B.Tech. in E&TCE from ABIT, Cuttack (Orissa.) and M.Tech. degree in Computer Science & Engineering from the IIIT, Bhubaneswar, Orissa in 2005 and 2009 respectively. His main professional interests are in Networking, Enterprise Resource Planning, mobile Computing, Cyber Defense, Network Security and Intelligent Techniques.