Malicious Objects Propagation Dynamics in the Network

Dinesh Kumar Saini
Faculty of Computing and
Information Technology
Sohar University ,Oman

ABSTRACT

The network world is enormous, dynamic, divers and incredibly very high complex. Survival of computer network is highly depended on the capability of the network to fight with malicious objects which are abundantly available in the cyber space. Our network world is growing larger in size and ways of networking like wired and wireless with different techniques are also growing, but reliability and robustness is the issue of concern in the today's network. In this paper biologically based mathematical inspired modelling is carried out to monitor the spread of these malicious objects in the network. An attempt is made to develop a discrete-time "Susceptible -Attacked-Infectious-Non-Infectious (SAIN)" model for computer infection with the aim of estimating parameters such as time of attack, incubation time, and mean infection time by using probabilistic approach. SAIN model is basically compartment-specific approach; each compartment is having distinct boundaries. Computer nodes transfers from one compartment to other such as Susceptible to Attacked, Attacked to Infectious, and Infectious to Non-Infectious with some stochastic random variable. In the end of the paper it is described where and how to use this mathematical modelling for designing the cyber defence systems.

General Terms

Security, Mathematical Modeling and Computer Networking

Keywords

Malicious Object, propagation, Mathematical Modelling

1. INTRODUCTION

Malicious objects such as virus, worm, Trojan horse, spam etc. are the major threat to the computer networks through cyber attacks. Cyber attacks of different forms threaten an organization's computer and network systems. Such attacks are increasingly becoming more sophisticated and pose greater threats In the present era of Internet, security of information is the major concern. A large number of malicious objects are infecting the interconnected computers.[1,2,3] A lot of work has been carried out for the virtual vaccination of malicious objects infection. But to understand the propagation of malicious objects is still a challenge due to large number of constraints such as distinct nature of each malicious objects, distinct mode of propagation, less visibility of malicious objects to the user, etc.[4,5,6,7,8,13] To understand the dynamics of malicious object, we make an analogy in between the biological infection and computer infection propagation. In the biological infections, how infected and non-infected cells behave and help to propagate the infection can be more similar to computer infection propagation and malicious object behavior. In our model we fixed certain parameters by which we can predict the behavior of malicious object. In the initial phase of our modeling we consider each possible detail of every parameter.

The advent of Internet/Network technology in past three decades has led to sea change in the way data is transferred and information exchange takes place. Over the years coupled with technological development and need, Internet technology has grown, offering numerous functionalities and facilities. The growth of Internet technology has thrown severe challenges in form of requirement of a suitable cyber defense system to safeguard the valuable information stored on system. Towards this goal it is proposed to study and understand the various malicious objects and develop a mathematical model to represent their behavior. In this work it is intended to initially study self-replication and self-propagation of malicious objects such as virus, worm, Trojan horse, Bots etc. [1, 2].

The solution of different infections can be prepared in different phase's like– What are the various characteristics of propagation of infection into the connected computers? What type of models will be helpful to understand the propagation of infection by malicious objects? And what defensive measurement parameters can be decided? In cyber space a large number of malicious objects exist and they are categorized according to their characters [3]. When a new malicious object is detected, it will be characterized in one of the existed category and if any of the categories is not suited, a new category is devised but it happens very rarely.

A model can represent each category of malicious object and on this basis some defensive measures can be decided. These models can be any one of the following types like – Code Red Model, Lion Model, Stochastic Models, STERIDE Models, Packet-Level Worm Models, Self-Replicating Worm Models, Internet Relay Chat (IRC) Worm Models, Peer-to-Peer Worm Model etc. [4, 5, 6]. These measures generally help after the infection happens in the system. But there may be a possibility to detect whether the system is under threat or not before actual attack happens. But it is only probabilistic, because malicious attacks can happen at any discrete and random time and it is very difficult to predict the time of next attack. Thus the mathematical models and computer simulation can help us to save the system by malicious attacks in taking defensive actions. Further these mathematical models can be generalized to represent the behavior of numerous other technologies misused for cyber attacks like- instant messaging, P2P technology, bots, Phishing, DDoS attacks etc. Later on we omit the less important details of parameters and give simplified mathematical model. The paper is organized as under:

• Section-2: Theoretical model

• Section-3: Mathematical analysis of model

• Section-4: Numerical and experimental analysis and

• Section-5: Conclusion..

2. THEORETICAL MODELING

Malicious object dynamics model provides a good scene of the malicious object elimination, replication, and propagation during anti malicious object treatment.[10,11,12] Thus for evaluating the efficacy of anti malicious object software and understanding the dynamics of propagation, it is great interest to estimate dynamics parameters for the whole population and for individual computer [14,15,16,17]

Some Basic Terminologies

A. Attack

An attack is an external force by which the nodes existing in one category transfers into other category.

B. Vulnerable Nodes

Vulnerable nodes are the nodes those can be exploited by the malicious attacks.

C. Attacked-Nodes

These are vulnerable nodes on which attacks are carried out but still they cannot help in propagation of infection.

D. Infectious Nodes

These are the infected nodes and help in propagation of infection.

E. Non-infectious Nodes

These are the recovered nodes from the infectious category and having no infection.

F. Transfer rate

This is the rate by which the vulnerable nodes are attacked by malicious objects.

G. Incubation time

This is the time period during which a node remains in the Attacked phase.

H. Mean infection time

This is the mean time period during which a node remains in the infectious phase

2.1 Stochastic Mathematical Modeling

The attacks on the computer are totally stochastic. We do not know the actual time of next attack on the computer. But on the basis of probability concepts in simulation we can find the probability of the attack at an instance of time.

If stochastic variable (Time of attack) can take I different values, xi (i = 1, 2, …, I), and the probability of the value xi being taken is P(xi), the set of numbers P(xi) is said to be a probability mass function. Since the variable must taken one of the values, it follows that

$$\sum_{i=1}^{I} P(X_i) = 1$$

Probability mass function can be defined as

P(xi) = ni / N

Where N= total number of attacks and ni number of attacks from a specified source.

A cumulative distributed function can also be found which gives the probability of stochastic attacks' being less than or equal to a given value. Different measures of probability functions can be used for the study of the stochastic system such as mean, mode, median, Standard deviation, etc. Models characteristic equations can be of two types – Linear and non-Linear. Non-linear system can be represented by Partial Differential Equations (PDE). Consider that malicious object has propagation property P, depends upon various other factors like- A, B, C …etc. It can be represented as

$$P=f(A, B, C...).$$

The velocity can be represented as

$$\partial P/\partial t = \partial f(A, B, C,...)/\partial t.$$

and the acceleration rate can be represented as

$$\partial 2P/\partial t2 = \partial 2f(A,B,C,\ldots)/\partial t2.$$

Once the simulated results obtained by the use of certain approximation techniques mentioned below can be used for complementing the data generated by simulation as well as validation:-

Taylor series expansion: Any function that has derivatives can be expanded by Taylor's Formula, The value of the independent variable, x, in a region near x = a, a function f(x) can be approximated by the polynomial

F(x) = f(a) + f'(a)(x-a) + (f''(a)/2!)*(x-a)2 +…..+ (f(n)(a)/a!)*(x-a)n.

Finite difference approximation methods: This method transforms a partial deferential equation over small intervals. This is of two types-

Forward difference Approximation: It calculates the function gradient at various points by the formula:

$$f'(xi) = (f(xi+1) - f(xi))/ \Delta x$$

Backward difference approximation: It also calculates the function gradient at various points by the formula:

$$f'(xi) = (f(xi) - f(xi-1))/ \Delta x$$

Higher order derivatives: These can be calculated to describe the various important points in the distribution by the following formula- f(n) = (f(n-1))'

Some regression tests such as Polynomial regression tests can also be used to validate the model. It finds that the values can be fitted into a polynomial or not.

Once the characteristic equation is derived then results can be empirically/analytically validated on the basis of available standard mathematical hypothesis. The first thing for mathematical model validation is the dimensional homogeneity, which requires that each term has the same net dimensions. Secondly, the models can be validated by checking qualitative and limit behavior. Except these some other things can also be considered, depending on how large the errors are? What is the accuracy and precision? Are the data fitted into the uniform curve? The data can be prepared by mean, mode, median or standard deviation. These data can be compared easily and help us to understand the behavior of malicious objects.

2.2 Mathematical Model

We proposed a mathematical model for mathematical dynamics by considering following computer or node and malicious object parameters:

- Uninfected target nodes (N)
- Vulnerable nodes which are actually targeted by malicious objects (NV)
- Nodes with unknown behavior (NM)
- Latently or hidden infected nodes (NL)
- Productively (Actively propagating malicious object) nodes (NP)
- Long-lived infectious nodes (NS)
- Infectious malicious object (VI)
- Non-infectious malicious object (VNI)

Without the intervention of anti malicious treatment, uninfected target nodes (V_{NI}) may either decrease due to malicious object infection or be in equilibrium state due to balancing between proliferation of new users and malicious object infection. Some uninfected target nodes (N) are infected by infectious malicious objects (V_I) and may become mysterious infected nodes (N_M), latently or hidden infected nodes (N_L), long-lived infected nodes (N_S), or productively infected nodes (N_P) with proportion $\alpha_m kV_I$, $\alpha_l kV_I$, $\alpha_s kV_I$, $\alpha_p kV_I$, respectively, where $\alpha_m + \alpha_l + \alpha_s + \alpha_p = 1$.Latently infected nodes (N_L) may be stimulated to become productively infected nodes (N_P) with a rate δ_L. Infected nodes N_M , N_S , and N_P can be totally jammed (killed) by the malicious object at some rate say δ_M , δ_S , and δ_P , respectively after producing or replicating malicious object an average of Z infections per node during their life time.Infected nodes N_M , N_S , and N_P can also be totally jammed (killed) at the rates μ_M , μ_S , and μ_L respectively, without replicating or producing malicious objects.We assume that the proportion of noninfectious malicious objects propagated by infected nodes (due to user's cautiousness) is η without the intervention of AMS.The elimination rates of infectious malicious objects and noninfectious malicious object rates are same, say c.Now we assume that the anti malicious treatment is having more than one AMS. Here we model the effect of AMS by reducing the infection rate K_0 to $K_0(1- \gamma)$, where γ is AMS efficacy and $0 \leq \gamma \leq 1$. If $\gamma = 0$, then AMS is totally failed and $\gamma=1$, then AMS is perfectly effective. We assume that AMS will not block the malicious objects perfectly. So, dynamics of our model is:

The model formulation is as follow

$$\frac{dN_M}{dt} = (1-\gamma)\alpha_M k_0 N V_I - \delta_M N_M - \mu_M N_M$$

$$\frac{dN_S}{dt} = (1-\gamma)\alpha_S k_0 N V_I - \delta_S N_S - \mu_S N_S$$

$$\frac{dN_L}{dt} = (1-\gamma)\alpha_L k_0 N V_I - \delta_L N_L - \mu_L N_L$$

$$\frac{dN_P}{dt} = (1-\gamma)\alpha_P k_0 N V_I + \delta_L N_L - \delta_P N_P$$

$$\frac{dV_I}{dt} = (1-\eta)P - cV_I$$

Where, P is additional malicious object propagation rate, because AMS cannot stop the malicious object propagation completely.

$$\frac{dV_{NI}}{dt} = \eta P + Z\delta_M N_M + Z\delta_S N_S + Z\delta_P N_P - cV_{NI}$$

Where, $\alpha_M + \alpha_S + \alpha_L + \alpha_P = 1$

In our proposed model we have taken four compartments:

- Vulnerable nodes
- Attacked nodes
- Infectious nodes
- Non-Infectious nodes

An assumption is made that recovering process is having patches for the vulnerability and hence recovered nodes will not become further vulnerable. Figure-1 shows the transfer of nodes from one compartment to the other compartment. There are three type of transfer observed:

- Vulnerable to Attacked
- Attacked to Infectious and
- Infectious to non-infectious

A malicious attack can occur on vulnerable nodes and the vulnerable node converts into the attacked nodes. Here the time-dependent transfer rate is nothing but rate of malicious attack. Every time the number of malicious objects and number of vulnerable nodes change with time .i.e. attacks are discrete and stochastic.

Attacked nodes convert into the infectious nodes as soon as the process of propagation proceeds by occurrence of a specific event. The time of transmission is discrete as it depends on the specific event occurrence such as e-mail opening or clicking a download button. The time in which a node remains in the attacked compartment is known as incubation time.

Infectious nodes convert into the non-infectious nodes due to factors such as:

- Users' awareness
- Use of anti-malicious software
- Use of anomaly detection and prevention

This phase is also discrete and stochastic because the occurrence of safe factors is at distinct points of time.Attacked nodes convert into the infectious nodes as soon as the process of propagation proceeds by occurrence of a specific event. The time of transmission is discrete as it depends on the specific event occurrence such as e-mail opening or clicking a download button. The time in which a node remains in the attacked compartment is known as incubation time.[21,22] Infectious nodes convert into the non-infectious nodes due to factors such

as :Users' awareness, Use of anti-malicious software and Use of anomaly detection and prevention, This phase is also discrete and stochastic because the occurrence of safe factors is at distinct points of time.

2.2.1 Attack Time

Let the size of the jump be one unit. Now if t be an arbitrary point in time, the probability that there are no attacks in (t, t+s) is $e^{-\lambda s}$. This is independent of the history of attacks before t. If we replace t by other arbitrary time T_n then same result will come as under:

$$P\{B_{T_n+s} - B_{T_n} = 0 \mid B_u; u \le T_n\} = e^{-\lambda s}. \quad (18)$$

Also the inter-arrival times of attack T_1, T_2-T_1, T_3-T_2, … are independent and identically distributed random variables, with common distribution:

$$1 - e^{-\lambda t}, t \ge 0 \quad (19)$$

In certain situations, we are interested in the number of attacks in an interval (T, T+s], where T is a random variable instead of a fixed number. It turns out that for a certain class of random times T, the independence of B_{T+s}-B_T from the past history $\{B_u; u \le T\}$ until T is still preserved, and furthermore, the distribution of B_{T+s}-B_T is again a Poisson with parameter λs. Such "good" random times T are characterized by the property that for any number t, one can determine whether the event $\{T \le t\}$ has occurred or not by knowing the history $\{B_u; u \le t\}$ of the arrival attack until the time t.Figure-3 shows that the inter-arrival time of attacks increases and then becomes constant. In the starting the number of vulnerable nodes are more but infectious nodes are not (assume that by very few points the malicious object outbreaks) available, so inter-arrival time is more in stating phase but as infectious nodes increases the inter-arrival time decreases and at last becomes constant as almost all vulnerable nodes are exploited or patched.

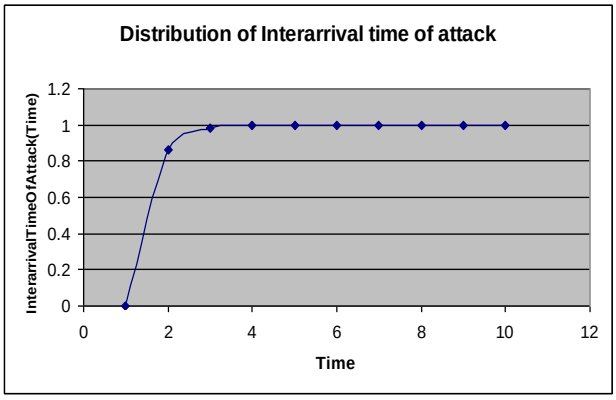

Fig. 1: Inter-arrival time of attack distribution with transfer rate λ=2.

2.2.2. Incubation Time

Let a malicious object attack through e-mail. Now the e-mail is in the account of the user but still it is not opened. So, the machine is under attacked phase but not infectious. The time in which the e-mail is opened by the user will be equal to the incubation time here. As soon as the e-mail is opened the malicious object becomes active and node converts its category to infectious node. This incubation time is random and its distribution is equivalent to Poisson process.

As discussed in the case of time of attack, times in between two consecutive conversions from attacked phase to infectious phase is independent and identically distributed random variables, with common distribution:

$$1 - e^{-t/\rho}, t \ge 0$$

Where, ρ is the incubation period.

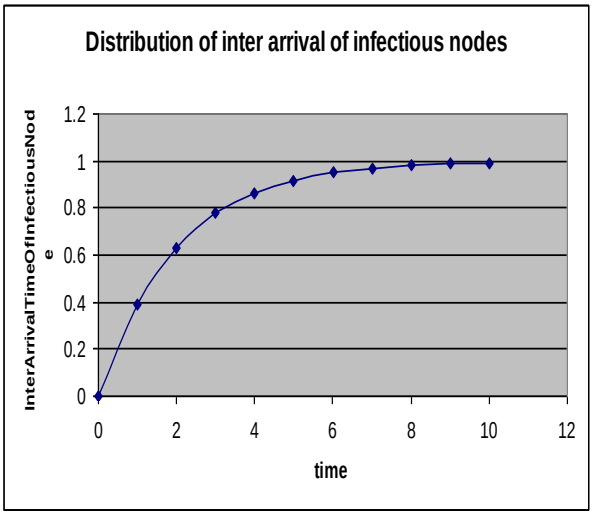

Fig.2: Inter Arrival Time of Infectious Nodes for ρ=2.0

At the starting of the process the numbers of malicious breakout points are less and so are the attacked nodes. So the mean incubation time remains more but as the attacked nodes increase with time it starts decreasing and become constant because the number of attacked nodes approach the number of vulnerable nodes at that instance. This is well explained by the figure-4.

2.2.3. Mean Infectious Time

As soon as the e-mail is opened to be read, the node becomes infectious. Here we are assuming that user is not aware of malicious code existing in his mail when he is reading the mail. Again we don't know that up to how much time the node remains in the infectious phase. It depends in how much time the symptoms will be detected by the user and having the proper anti malicious software to quarantine it. So we can say that it is independent and identically distributed random variables, with common distribution:

$$1 - e^{-t/\mu}, t \ge 0$$

Where, μ is the mean infection period.

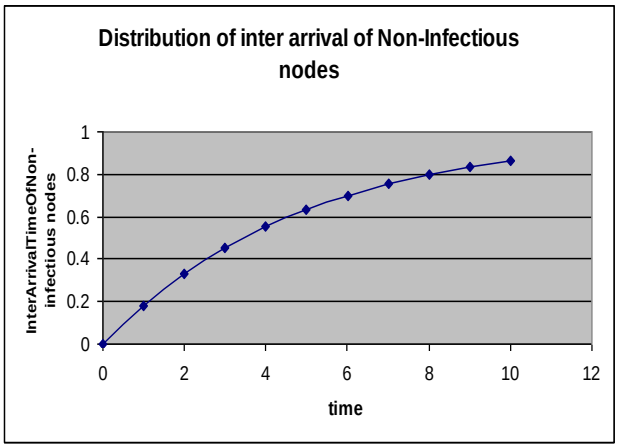

Fig.-3: Inter Arrival Time of Non-Infectious Nodes for μ=5.0

At the starting of the process the numbers of malicious breakout points are lesser and no specific diagnostic process is activated so, the mean infection time is more. As soon as the specific diagnostic process is come into the picture it starts decreasing. Once almost all the infectious nodes convert into the non-infectious nodes it becomes constant. Refer figure-5 to understand the above explanation.

3. SIMULATION OF RESULTS

3.1. Probability Distribution for Random Variable B(t) with Mean =2

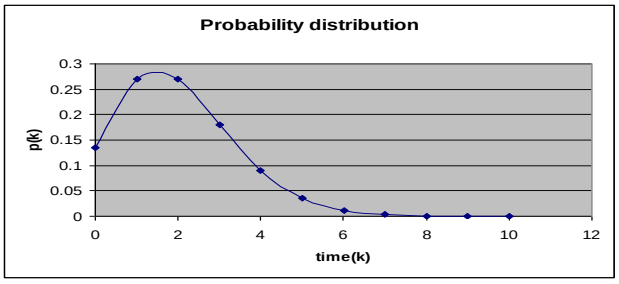

Figure-4: Probability distribution for random variable B(t) with k=1, 2, 3, …, 10 and mean(λt) = 2.

From the probability distribution, as shown in figure-6, it is clear that the probability of a random number increases up to the mean value and then decreases with time. So, till the mean value the chance of attack increases and after it the chance of attack decreases. This is understood that in the starting, the numbers of vulnerable nodes are more but malicious object outbreak from less number of points. With the time, the infectious nodes increases and hence the chance of attack but after some time the number of infectious nodes start converting into the non-infectious nodes due to patching or other preventive factors, so, the chance of attack decreases and becomes constant at its lowest level.

3.1 Cumulative Probability Distribution with Mean =2

Form the cumulative probability distribution, as shown in figure-7, it is clear that the number of attacked nodes increases as the cumulative probability increases and after some time it became almost constant. The number of attacks becomes constant after a time t because the number of vulnerable nodes becomes lesser with time and finally almost constant.

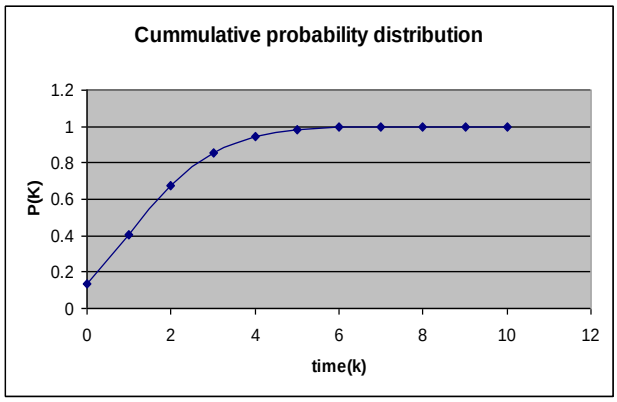

Fig. 5 : Cumulative probability distribution for random variable B(t) with k=1, 2, 3, …, 10 and mean(λt) = 2.

4. HOW THIS MODEL CAN BE USED IN CYBER DEFENSE

To understand the use of this model in the cyber defense we take following two examples: Suppose that there are a thousand computers in an intranet which are vulnerable to malicious attack and suppose that the probability, that in any given week any given vulnerable computer will be attacked by a malicious object is 1/500. Now, what is the probability that in the coming week 3 or more vulnerable computers will be attacked by the malicious objects?

Here λ=1000 and t=1/500. So λt=2.

$$p(x \geq 3) = 1 - p(x \leq 2) \cong 1 - \sum_{x=0}^{2} \frac{e^{-\lambda t}(\lambda t)^{x}}{x!} =$$

$$1 - \sum_{x=0}^{2} \frac{e^{2} 2^{x}}{x!} = 0.3232$$

During the busiest period of intranet, a malicious attack is initiated randomly at an average of 30% per minute. The intranet overloads if 3 or more attacks are initiated within 1-second interval. What is the probability that the intranet will be overload by attacks initiated during a particular 1-second interval within the busiest period?

$$mean = \frac{1-\sec ond}{1-\min ute} * 30 = 0.5$$

$$p(overload) = p(x \geq 3) = 1 - p(x \leq 2) =$$

$$-\frac{1}{\sqrt{e}}(\sum_{i=0}^{2}\frac{(0.5)^i}{i!} = 0.0146$$

As the above two examples shows that the possibility of attack on vulnerable nodes and possibility of overloading of intranet respectively can be found out by using the prior or posterior analysis of the existing information or by making some expert analogy.

From our discussion, three important parameters are evolved i.e. time of attack, incubation period, and mean infection time. If time of attack is known to us we can take the proactive measures to make our information safe. Prediction of incubation time helps to quarantine the infected machines and hence restrict the further propagation of malicious objects. Finally, the prediction of mean infection time helps to predict the direction of the propagation of the malicious object.

5. USE OF MODELING

For modeling a cyber defense system one should know about the different components needed. Here is a good division of cyber defense components are given in figure-6
These are sensors and exploitation, situation awareness, defensive mechanism, command and control, strategies and tactics, and science and Engineering [28]. He also tried to set an analogy in between an "art of war" to technology and he got a success in doing such thing at some extent .Some learning attack strategies by intrusion alert are also provided to predict the future attacks on the basis of analysis of sad mind, representing it in the form of graphs and finding the possible flow of sad mind ideas in advance [29, 30,31]. Detecting these sad-mind ideas, precautions can be taken in advance.
An attempt is made to explore the fast Internet worm (Slammer) in the context of both simulation and analysis, using as a calibration touchstone an attempt to reproduce the empirically observed behavior of the Slammer worm, which exhibited a peculiar decline in average per-worm scanning rate not seen in other worms (except for the later Witty worm, which exhibited similar propagation dynamics). The efforts are made to study two complementary worm quarantine defense strategies and combine their strengths to devise hybrid quarantine worm defense strategy and simulate the results. Gupta, A. et al [19] proposed a number of extensions to the original predator model, including immunizing predators, persistent predators, and seeking predators to deal with the bottleneck problem of the traffic. They also report on a set of simulations which explore the effects of predators on small-scale (800 to 1600 node) networks. It showed that an intelligent worm can exploit the directory and naming services necessary for the functioning of any network, and they modeled the behavior of such a worm in this paper.

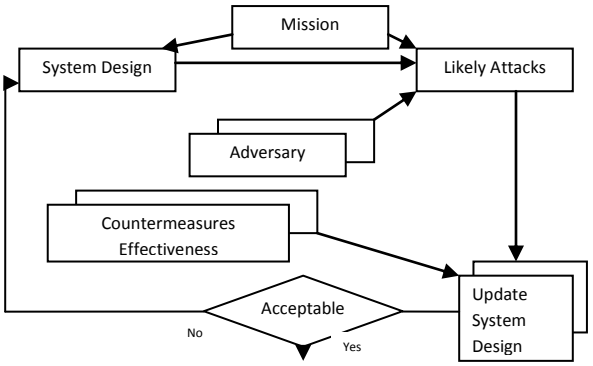

Fig. 6: Cyber Defense System Design model

They also explored via analysis and simulation the spread of such worms in an IPv6 Internet. As a result, additional work is suggested in developing detection and defense mechanisms against future worms, and their work identifies directory and naming services as the natural place to do it. It described a worm simulation model. They worked to accurately model the large scale spread dynamics of a worm and many aspects of its detailed effects on the network. They modeled slow or fast worms with realistic scan rates on realistic IP address spaces and selectively model local detailed network behavior. They showed how it could be used to generate realistic input track for a working prototype worm detection and tracking system, the Dartmouth ICMP BCC: System/Tracking and Fusion Engine (DIB: S/TRAFEN), allowing performance evaluation of the system under realistic conditions. Thus, they could answer important design questions relating to necessary detector coverage and noise filtering without deploying and operating a full system. Their experiments indicate that the tracking algorithms currently implemented in the DIB: S/TRAFEN system could detect attacks such as Code Red v2 and Sapphire/Slammer very early, even when monitoring a quite limited portion of the address space. Also they indicate some improvement to make more sophisticated algorithms to reduce the risk of false positives in the presence of significant \background noise" scanning, to simulate worm spread and other Internet-wide events such as DDoS, flash crowds and spam we need a detailed Internet model, a packet-level simulation of relevant event features, and a realistic model of background traffic on the whole Internet. They also proposed a design and present implementation of a distributed worm simulator, called PAWS. It is explored the use of selective abstraction through epidemiological models in conjunction with detailed protocol models as a means to scale up simulations to a point where they could ask meaningful questions regarding a hypothesized link between worms and inter-domain routing instability. They also described some approaches to collect the underlying data for their models. It is proposed a novel worm-curtailing scheme, i.e., beehive, which is able to fight-back worm propagation by actively immunizing any encountered worm-infected node. More specifically, by owning a portion of the unused but routable IP space that is open to infection attempts of different worms, a beehive not only attracts and traps these attempts, but also defensively gives a security shot to each attempting worm-infected node. They did both analysis and simulation results of beehive evaluation. They showed in their results that their system is able to reduce the maximum worm infection coverage

to as low as 13%, it described a model of worm propagation and its affect on routers and application traffic. They also gave a simulation Framework (SSF) API, they modeled worm propagation, its affect on the routing infrastructure and its affect on application traffic using multi-scale traffic models. The paper introduced a novel worm containment strategy that integrates two complementary worm quarantine techniques. They presented an SSFnet-based microscopic simulation of the containment strategy against random scan worms, and explored various performance characteristics of the group defense mechanism. It is discussed the issues of the atypical and aggressive behavior of worms could easily consume excessive resources, both processing time and storage, within a typical simulator. They discussed the design of their Internet worm models in the Georgia Tech Network Simulator, and showed how they addressed these issues. They presented some results from their Internet worm simulations that showed the rate of infection spread for a typical worm under a variety of conditions. The series of simulations run to estimate various worm growth patterns and their corresponding propagation algorithms. It also tested the impact of various improvements, starting from a trivial simulation of worm propagation and the underlying network infrastructure to more reined models, it attempted to determine the theoretical maximum propagation speed of worms and how it could be achieved.

Network Address Space Randomization (NASR) is one proactive system against hit-list worms. The concept behind it is that hit-list information could be rendered stale if the nodes are forced to frequently change their IP addresses [28]. But some constraints like- exploding routing tables, generating tremendous overhead, and requirement of global coordination restricts its usage. One way can be software diversity, by which both existing/actual and synthetically generated network topologies compared in the form of metrics & try to detect possible flaws in advance [18]. However, there have been no quantitative studies that examine the effectiveness of software diversity on viral propagation that software diversity requires. Another method can be based up on temporal consistency (low temporal variance) that shows correlation among otherwise independent peers' behavior as anomalous behavior, indication of a fast-spreading worm in the systems like- Windows XP an judging the probability of non-worm and worm program.
Fast-replicating worms like- Red-Code worm (affected more than 359,000 Web servers in 14 hours), Slammer (Achieved its maximum Internet –wide scanning rate 55 million scan per second in a few minutes) a defensive mechanism is given by Min Kai and his team that is based on scalable security overlay networks based on distributed hash tables (DHTs) to facilitate high-speed intrusion detection and alert-information exchange [27]. This paper gives its stress on fast automatic signature estimation, accurate traffic monitoring, and provides some algorithms.
The Sybil attack is related to the node replication attack, wherein a malicious node gains an unfair advantage by claiming multiple identities When the base station detects a misbehaving node, it broadcasts a message to revoke that node, a localized mechanism for sensor network node revocation. In the approach, nodes can revoke their neighbors , in the paper it is detected two shortcomings - single point of failure, and on neighborhood voting protocols that fail to detect distributed replications and proposed two algorithms based on the properties that arise through the collective actions of multiple nodes, Randomized multicast, and line-selected multicast. Both algorithms were globally recognized for their strong performance characteristic points.

6. CONCLUSION

The stochastic modeling is having its importance over continuous modeling or differential modeling in the malicious object attacks as it is discrete and stochastic in nature. The compartment-specific random dynamics is predicted by using the probability density functions. The mean of these probability distribution functions gives the best suited value of the random variables and the variance gives the most common dispersion of random values. The random values are purified by using sampling and maximum likelihood criterion. The prediction of parameters like transfer rate (λ), incubation time (ρ), and mean infection time (μ) are used in cyber defense to understand the nature of the malicious object propagations and prevention.

7. LIMITATIONS

The model needs to be tested in the real time environment. Availability of real world data about whole network is difficult to get and analyze. Our model doesn't talk about speed of malicious object spread. Better sensitivity analysis can be developed which our model does not address.

8. REFERENCES:

[1]. Housholder et al. (2002). Computer Attack Trends Challenge Internet Security, Security and Privacy (supplement to Computer), Vol. 35, No. 4, 5-7.

[2]. Chi, S.D., Park, J.S., Jung, K.C., Lee J.S. (2001). Network Security Modeling and Cyber Attack Simulation Methodology, LNCS, Vol. 2119.

[3]. Bimal Kumar Mishra and Dinesh Kumar Saini "Mathematical Models on Computer viruses" Journal of Applied Mathematics and Computation, Volume 187, Issue 2, 15 April 2007, Pages 929-936.

[4]. Bimal Kumar Mishra and Dinesh Kumar Saini "SEIRS epidemic model of transmission of malicious objects in computer network" Elsevier International Journal of Applied Mathematics and Computation, Volume 188, Issue 2, 15 May 2007, Pages 1476-1482.

[5]. Dinesh Kumar Saini and Hemraj Saini "VAIN: A Stochastic Model for Dynamics of Malicious Objects", the ICFAI Journal of Systems Management, Vol.6, No1, pp. 14- 28, February 2008.

[6]. Hemraj Saini and Dinesh Kumar Saini "Malicious Object dynamics in the presence of Anti Malicious Software" European Journal of Scientific Research ISSN 1450-216X Vol.18 No.3 (2007), pp.491-499 © Euro Journals Publishing, Inc. 2007 http://www.eurojournals.com/ejsr.htm

[7]. Dinesh Kumar Saini and Hemraj Saini "Proactive Cyber Defense and Reconfigurable Framework for Cyber

Security" International Review on computer and Software (IRCOS) Vol.2. No.2. March 2007, pages 89-98.

[8]. Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., Weaver, N. (2003). Inside the Slammer Worm, IEEE Security and Privacy, Vol. 01, No. 4, 33-39.

[9]. Chen, Z., Gao, L., Kevin, Kwiat (2003). Modeling the Spread of Active Worms, In Proceedings of IEEE INFOCOMM, Vol. 3, 1890-1900.

[10]. Shannon, C., Moore, D. (2004). The Spread of the Witty Worm, IEEE Security and Privacy Magazine, Vol. 2, No. 4, 46-50.

[11]. Zou, C., Gong, W., Towsley, D. (2002). Code Red Worm Propagation Modeling and Analysis, In Proceedings of ACM Conference on Computer and Communication Security (CCS), 138-147.

[12]. Dym C.L. Principles of mathematical modeling. 2nd Ed., Elsevier-Academic press: California; 2004.

[13]. Sayadjari O.S. Cyber Defense: art to science. Communication of the ACM. 2004, Volume-47, Issue-3, ACM Press New York, NY, USA, pp. 52-57.

[14]. Ning P., Xu D. Learning attack strategies from intrusion alerts. Proceedings of the 10th ACM conference on computer and communications security. ACM Press New York NY, USA. pp. 200-209; 2003.

[15]. Ning P., Cui Y., Reeves D. S. Constructing attack scenarios through correlation of intrusion alerts. Proceedings of the 9th ACM Conf. on Computer and Communications Security. ACM Press New York NY, USA. pp. 245-254; 2002.

[16]. Ning P., Cui Y., Reeves D. S, Xu D. Techniques and tools for analyzing instruction alerts. ACM Transactions on Information and System Security (TISSEC). 2004, Volume-7, Issue-2, ACM Press New York NY, USA, pp. 274-318.

[17]. Weaver N., Kesidis G., Paxson V. Preliminary Results Using Scale down to Explore Worm Dynamics. Proceedings of the 2004 ACM workshop on Rapid malcode table of contents. ACM Press New York NY, USA. pp. 65-72; 2004.

[18]. Porras P., Briesemeister L., Skinner K., Levitt K., Rowe J., Ting Y. A. A Hybrid Quarantine Defense. Proceedings of the 2004 ACM workshop on Rapid malcode table of contents. ACM Press New York NY, USA. pp. 73-82; 2004.

[19]. Gupta A., DuVarney D. C. Using Predators to Combat Worms and Viruses: A Simulation-Based Study. 20th Annual Computer Security Applications Conference. IEEE Computer Society Washington, DC, USA. pp. 116-125; 2004.

[20]. Liljenstam M., Nicol D. M., Berk V. H., Gray R. S. Simulating Realistic Network Worm Traffic for Worm Warning System Design and Testing. Proceedings of the 2003 ACM workshop on Rapid malcode table of contents. ACM Press New York NY, USA. pp. 24-33; 2003.

[21]. Jiang X., Xu D., Lei S., Ruth P., Sun J. Worm Meets Beehive. Technical Report CSD TR 04-027, Purdue University, Department of Computer Sciences, May 2004.

[22]. Nicol D. M., Liljenstam M., Liu J. Multiscale Modeling and Simulation of Worm Effects on the Internet Routing Infrastructure. Proceedings of 13th International Conference on Modeling Techniques and Tools for Computer Performance Evaluation (Performance TOOLS 2003), Urbana, IL, Sept 2003.

[23]. Briesemeister L., Porras P. Microscopic Simulation of a Group Defense Strategy. Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation table of contents. ACM Press New York NY, USA. pp. 254-261; 2005.

[24]. Cai M., Hwang K., Kwok Y.K., Song S., Chen Y. Collaborative Internet Worm Containment. IEEE ecurity and Privacy. 2005, Volume-03, Issue-3, IEEE Computer Society Washington, DC, USA, pp. 25-33.

[25]. Douceur J.R. The Sybil attack. In Proceedings of Workshop on Peer-to-Peer Systems (IPTPS). Editors: P. Druschel, F. Kaashoek, A. Rowstron (Eds.). Springer-Verlag GmbH. 2002, Volume 2429 / 2002, pp. 251 - 260.

[26]. Eschenauer, Gligor V. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS). ACM Press New York, NY, USA. pp. 41-47; 2002.

[27]. Dinesh Kumar Saini "A Mathematical Model for the Effect of Malicious Object on Computer Network Immune System" Applied Mathematical Modeling, 35(2011) Page No. 3777-3787 USA, doi:10.1016/.2011.02.025.

[28]. Dinesh Kumar Saini, Jabar H. Yousif, and Wail M. Omar "Enhanced Inquiry Method for Malicious Object Identification" ACM SIGSOFT Volume 34 Number 3 May 2009, ISSN: 0163-5948, USA

[29]. Dinesh Kumar Saini, Imran Azad, Nitin B Raut, and Lingaraj A. Hadimani, "Utility Implementation for Cyber Risk Insurance Modeling" The 2011 International Conference of Information Engineering, (ICFE-2011) World Congress in Engineering, July 6-9th London UK