SURVEY PAPER ON CYCLIC WORM PROPAGATION MODEL AND ANALYTICAL WORM PROPAGATION MODEL

Rupinder Kaur[1], Er.Sunil Nagpal[2], Saurabh Chamotra[3]

[1] *M.Tech (CSE), Baba Farid College of Engineering and Technology, Bathinda, (India)*

[2] *Ph.D Research Scholar, Punjab Technical University, Computer Science Department, Kapurthala (India)*

[3] *Sr.Engg /Scientist C, CDAC, A-34 Phase 8 Industrial Area, Mohali, (India)*

ABSTRACT

Active worm spread automatically in a regular fashion and can be flood into the internet in a very short time. Modelling the spread of active worms can help us to understand, how active worms are spread, and how can be monitor and defend against the propagation of worm effectively. In this paper we describe the worm propagation using the analytical active worm propagation model, which characterize the propagation of worms that employ random scanning. It is optimistic in the sense that worms can still be controlled and pre-generated target list, or internally generated target lists as their target discovery technique. Furthermore, we extend our AAWP model to understand the spread of worms that employ local subnet scanning. In this paper we present the AAWP model to analyze the characteristics of the spread of active worm. In this paper we also describe the model of cycle worm propagation to defend against the future and current worm of compromised system and some prevention mechanism to monitor the spreading of active worm. This article will step through common practices to prevent worm propagation and also examines these results in the analytical worm propagation model.

Keywords: ***Network Security, Active Worm, Cyclic Worm Propagation, AAWP Modelling, Worm Traffic Monitoring, Detection Of Active Worm, Vulnerable Infections, Miscode Functions***

I. INTRODUCTION

All manuscripts must be in English. These guidelines include complete descriptions of the fonts, spacing, and related information for producing yourWorms are self propagating program that spread over network, usually the internet. Active worms have been a persistent security threat on the Internet since the Morris worm arose in 1988. The Code Red and Nimda worms infected hundreds of thousands of systems, and cost both the public and private sectors millions of dollars [21],[22],[23],[24].Worms spread by scanning the network for vulnerable machines and then infecting them. Worms can cause an enormous amount of damage Launch DDOS attacks,

Access sensitive information and Cause confusion by corrupting the sensitive information. Therefore it is important to understand how worms propagate in order to contain them. They are capable of automatically infecting thousands or even millions of hosts in a short period of time. Kienzle and Elder defined a worm as 'malicious code (standalone or file infecting) that propagates over a network, with or without human assistance' [11]. This is a broad definition of worms, since it neither differentiates standalone from file-infecting code nor distinguishes between code with and without human assistance to propagate. All malicious code that propagates over a network is covered by the above definition. In the last several years, the security threat caused by worms has continuously increased. Some active worms, like Code Red and SQL Slammer, caused in cost of millions of dollars and a denial of service effect on the internet. Because worms don't need any human intervention, worm's propagation is quickly performed and it makes human's response to be difficult. Therefore a worm detection system is demanded by the fast spreading characteristic, and it can be used to automatically respond to worm propagation. Much recent research for worm early detection was introduced. To detect worm in early stage of propagation, many worm detection architectures and systems are developed. However, most solutions need to monitor global-scale network. This paper focuses on detecting worm activities in local networks. In contrast of global network monitoring, the characteristics in monitoring local networks are analyzed and we use those for detecting worm. To quantify the performance of defense systems, we first characterize the spread of active worms. Analytical Active Worm Propagation (AAWP) model, developed by Chen et.al. [3] Can capture the propagation of active worms that employ random scanning. Using this analytical model, we identify three key parameters of worms propagation exploited by current systems: number of vulnerable machines, scanning rate, and time to complete infection. The propagation characteristics of a worm show what kind of network traffic will be generated by that worm and how fast the response time must be for countermeasures.

Our analysis shows that a significant amount of resources is required for the existing systems to fight effectively against active worm.

II. RELATED WORK

Existing malware propagation models mainly concentrate to forecasting the number of infected computers in the initial propagation phase.After an introductory terminology sections presented, worm characteristics during target finding and worm transferring phases are identified. This is followed by an overview of worm defense mechanisms: detection and containment. Self-propagation is a key characteristic of an active worm. For example, when a worm is released into the Internet, it starts out on a single host and scans randomly for other vulnerable machines. When the scan finds a host that can be compromised, the worm sends out a probe to infect the target. After a new host is compromised, the worm transfers a copy of itself to this host. This new host then begins to run the worm and infects other targets. Kienzle and Elder defined a worm as 'malicious code (standalone or file infecting) that propagates over a network, with or without human assistance' One other example is "hitlist" scanning worm investigated by Weaver [15]. Before a worm is released, the worm author gathers a "hitlist" of potentially vulnerable machines with good connections. The worm, when unleashed into the Internet, begins scanning down the list. After this list has been exhausted, the worm turns to infect other vulnerable machines. One closely related work is "Internet Quarantine" by Moore et.al. this work investigates the requirements for containing the self-propagation code. Another type of model, which is discussed in this

paper, is the Analytical Active Worm Propagation (AAWP) model, which uses a discrete time model [3]. Chen et. al [3] presented a discrete-time version worm model with considering of the patching and cleaning effect during worm's propagation. Zou et.al [18] proposed a trend based detection system using the Kalman filter. The method using the Kalman filter is suitable to detect worm in its starting stage on the network without worm infected. Our algorithm applies to the network with or without worm traffic existence. Our monitoring mechanism presents an easy method to distinguish worm traffic in the router junction of enterprise network. Our contribution in this paper is to point out the worm-infected hosts efficiently. It will be helpful for network administrators to set up their security policy. In this we describe the life cycle of worm progation model and the analytical active worm model for analyzing the internet worm traffic through the techniques and formulation of AAWP model [3]. This model applies only to active worms employing the uniform scanning approach discussed in a previous section since it was derived based on that scanning
Approach.

III. CYCLE OF WORM PROPAGATION MODEL

Existing malware propagation models mainly concentrate to forecasting the number of infectedAnalyzing most of malware or worm, there are several specific common ways of propagation. By developing the countermeasure specific mechanism used to prevent, contain and slow of propagation of current and future worm. In this cycle we can explain the cycle of worm propagation , in which infected host machine selected their target according to worms traffic category and deliver the selected malcode to compromise system , here it can transfer the data to the payload . In the payload if the malicious worm activities found then go to the executable payload if the worm file is not found then go to the initial state of infected host [2]. Figure 1 shows the generalized model of cyclic worm propagation. As the model shows, there are only three steps for a worm to infect a host. In the first stage the infected host searches for vulnerable targets. When the target is found the infected host tries to deliver malcode to the selected target. Executing the malcode, the target host would be compromised, making the target a Sinfected host and the cycle goes around. As the system compromised, some malwares execute additional tasks. Payload refers to those additional task produced by a worm. It may include leaving a backdoor, self replication or performing the Denial of Service Attacks against websites. Some malwares such as hybrid Worm/Trojan use payloads on compromised systems. To do this, malware writers exploit the propagation speed of worms to distribute their Botnets. Bot a.k.a. zombie refers to a host that receives commands from its handler [2].

3.1 How Cycle Of Propagation Work

In this section we describe how the model works by defining the actions which take place in each of the stages. These actions are common practices that top threat malwares use to complete their life cycle. Knowing these methods, one can use the knowledge to prevent malware propagation by deploying defense mechanisms for each of them. Models can use these methods for comparing their effectiveness in malware propagations modeling. Some of these methods such as scanning, in the Target Selecting phase are used in all propagation models. In the target selecting phase, the malware is trying to somehow choose a way to propagate malcode. There are three specific common ways among malwares to choose the target.1-Generating random IP addresses

if the vulnerability for exploiting, is in an active service on machines. 2-HarvestingEmail addresses via online profiles or on the local machine. 3-Through file sharing systems. When the target is selected, the delivery phase begins. The aim of this phase is to deliver the malicious code to the target. This could be done via the following methods: 1-As a payload associated with buffer overflows, e.g. Blaster, Sasser, Slammer [12]. 2-Using mail or IM services to send special crafted message to anonymous users, e.g. MyDoom, NetSky, Sohanad [12]. 3-Specially crafted HTML page hosted on a web server,e.g. Nimda [22]. Compromising the system requires the malcode to be executed. The latter method happens when the malcode delivery is the result of buffer overrun vulnerability, as the system compromised the malware may execute some payloads. Payloads effects are viable if the malware itself is removed. For instance, if the malware left a backdoor on the system, this backdoor may live forever even if the malware is removed. Installing kernel level root kits in some cases requires the operating system to be reinstalled again. In self-carried worms, propagation is straightforward; the worm payload is transferred in a packet by itself. Other worms are delivered through a second channel; that is, after finding the target, the worm first goes into the target, and then downloads the worm's payload from the Internet or a previously infected machine through a backdoor, which has been installed using RPC or other applications. A more deceitful worm may append the payload after, or replace, legitimate traffic to hide itself.

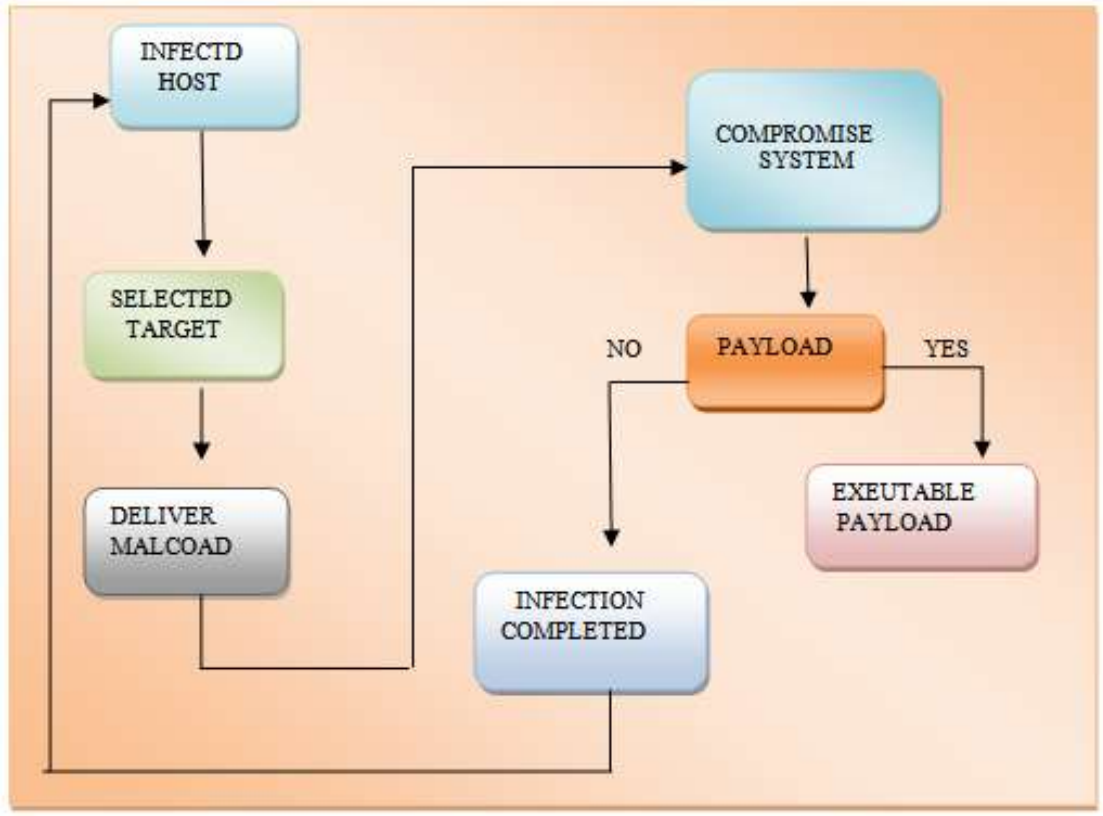

FIG 1.GERNALIZED CYCLE OF WORM PROPAGATION MODEL

IV. PREVENTION MECHANISM FOR CYCLIC WORM PROPAGATION MODEL

4.1 Topology Based Solution

In Target Selection phase we saw that there are three common ways that malwares use to propagate. To prevent connection setup between infected host and randomly generated IP Addresses, one can use client side software

firewall or Host IPS. For an enterprise network, this solution may not be cost effective, so using Network IPS or hardware firewall is a better solution. For an enterprise network, this solution may not be cost effective, so using Network IPS or hardware firewall is a better solution. Lots of efforts have been done to Elevate IPS capabilities such as detection of self decrypting malwares [1] that allows polymorphic worms to be detected within network. These new techniques can help slowing down worm propagation.

4.2 Client Related Solution

Deploying client side solution is more effective because propagation starts from infectious hosts. targets of attacks are gathered from infected host, e.g. email harvested on local machine are used to send social engineered mail to victims, all top threat worms such as NetSky use their own SMTP Engine, to prevent this function, basically one need to write a custom signature on IDS to pick up any SMTP traffic not coming from specified mail servers, another option is using firewall to alert for uncommon SMTP traffic.

4.3 Worm Traffic Detection in Local Network

In this section, we propose a method to detect worm activities in local network. Most worms have some common characteristics such as autonomous propagation, targeting vulnerable hosts and generation of scanning traffic. Using these characteristics, we can identify problematic hosts and detect worm activities. In our study, we focus on the following objectives. Identifying hosts with scanning activity in local network Detecting worm propagation activities with a low false positive error. It means that the detection system must be able to provide network administrators. Worms spread many connection requests to propagate itself and infect vulnerable hosts on the Internet. When selecting target hosts, worms use a kind of scanning strategies.

V. ANALYTICAL ACTIVE WORM PROPAGATION MODEL (AAWP)

To understand the characteristics of the spread of active worms that employ random scanning, we develop the AAWP model, which uses the discrete time and continuous state deterministic approximation model. Discrete time deterministic models of active worms in a homogeneous system. It is called the Analytical Active Worm Propagation (AAWP) model. This model applies only to active worms employing the uniform scanning approach. The AAWP model is based on discrete time and thus more accurate if macro-scope modeling is needed. In this model, a host cannot infect other hosts before it is infected completely. But in models based on continuous time, a host begins devoting itself to infecting other hosts even though only a ‘small part’ of it is infected. The time to infect a host is an important factor for the spread of active worms [25]. Beside, in the AAWP model, the case that worms infect the same destination at the same time is considered, AAWP model is based on a discrete time model. We believe that the AAWP model is more accurate. Because in the AAWP model, a computer cannot infect other machines before it is infected completely. AAWP model is considered the patching rate or the time that it takes the worm to infect the machine. During the worm propagation, it is possible now days to promptly patch the vulnerability on the computers and assuming a reasonable patching rate and different worm have different infection abilities which are reflected by the scanning rate and time taken to infect the machine. Time required to infect a machine also depend upon the size of the worm and degree of network congestion, distance between source and destination. In the AAWP model, we consider the case that the worm can infect the same destination at the same time. Models, however, try to get the expected number of

infected machines, given the size of the hitlist, total number of vulnerable machines, scanning rate/birth rate and death rate. Applications of Analytical Active Worm Propagation (AAWP) Model A good model can reflect the spread of real worms and at the same time resolve many practical tasks. In this section, we apply the AAWP model to monitoring, detecting and defending against the spread of active worms. To quantify the performance of defense systems, we first characterize the spread of active worms. Analytical Active Worm Propagation (AAWP) model, developed by Chen et.al. [3] Can capture the propagation of active worms that employ random scanning. Using this analytical model, we identify three key parameters of worms propagation exploited by current systems: number of vulnerable machines, scanning rate, and time to complete infection. The severity of worm propagation can be mitigated greatly, if a defense system can reduce the number of vulnerable machines significantly, decrease the scanning rate dramatically, and prolong the time that worms need to infect a machine.

5.1 Monitoring the Active Worms

Monitoring the active worm in an analytical active worm model is an interesting task to perform their action of worm reflection from the system. It is vital to detect active worms effectively. In the near future active worms may spread across the whole Internet in a very short period of time. The most effective and also feasible way to increase a worm's propagation speed is to increase the worm's hitting probability. Localized scanning increases hitting probability in situations where vulnerable hosts are close to each other. Sequential scanning increases hitting probability in situations where IP addresses of vulnerable hosts form a consecutive sequence. Routable scanning reduces scanning space and thus increases hitting probability. This model shows that the speed of worms spreading is determined by such parameters as the size of a hitlist [3], the total number of vulnerable machines, the size of Entry addresses that worms scan, the scanning rate, the death rate, the patching rate, and the time to complete infection. The model assumes that worms can simultaneously scan many machines and do not re-infect an infected machine. The model assumes that worms can simultaneously scan many machines and do not re-infect an infected machine. The model also assumes that the machines on the hitlist are already infected at the start of the worm propagation. The model is derived as follows. Suppose that a worm scans N entry addresses and needs one time tick to infect a machine. For random scanning, the probability that a machine is hit by one scan is $^1/_N$ specially, when the worm scans 2^{32} entry addresses, this probability becomes $^1/_{2^{32}}$. Assume that currently there are η_i infected machine host and m_i vulnerable machines, where i is the index of time tick. Then the infected machines send out $\eta_i s$ scans to find the vulnerable machines, where s is the scanning rate [4]. On the average, there are $(m_i-\eta_i)$ $[1-(1-^1/_N)^{\eta_i s}]$ on the next time tick. Newly-infected machines on the next time tick. Meanwhile, given death rate d and patching rate p, at the next time tick, pm_i vulnerable machines are patched, and $d\eta_i+p\eta_i$, infected machines change to either vulnerable machines without being patched ($d\eta i$) or invulnerable machines ($p\eta_i$), Therefore, the number of infected machines is $\eta_{i+1} = \eta_i + (m_i-\eta_i)[1-(1-^1/_N)^{s\eta i}] - (d-p)\eta_i$ on the next time tick. In addition, $m_{i+1} = (1-p)\, m_i$, giving $m_i = (1-p)^i\, m_o = (1-p)^i M$, where M is the total number of vulnerable machines. Putting the above equations together, and letting k_i and e_i be the machine at a time tick i ($i \geq 1$) respectively, the AAWP model can be derived as [4]:

$$m_{i+1} = (1-p)^{i+1} M \quad (1)$$

$$k_{i+1} = \eta_i s \quad (2)$$

$$e_{i+1} = (m_i-\eta_i)[1-(1-^1/_N)^{k_{i+1}} \quad (3)$$

$$\eta_{i+1} = (1-d-p)\eta_i + e_{i+1} \quad (4)$$

where $i \geq 0$, $\eta_0 = h$ = size of hitlist, and $m_0 = M$. The recursion stops when there are no more vulnerable machines left or when the worm can not increase the total number of infected machines. AAWP model thus characterizes the active worms spreading newly-infected machines on the next time tick. Table I summarizes all the notations. Important Parameters AAWP model reveals the key parameters that constrain the speed of worms spreading and an ultimate prevalence of the worms in general. These parameters include the total number of vulnerable machines, the scanning rate, and the time to complete infection.

5.2Total Number of Vulnerable Machines

To understand the impact of this parameter, as the size of vulnerable machines decreases, it takes the worm a longer time to spread. This is because that the scans from the worm are less likely to hit the vulnerable machines. Therefore, reducing the number of vulnerable machines can be used by defense systems against worms spreading in the network.

Table1 Notation of AAWP Model

NOTATION	EXPLANATION
M	total number of vulnerable machine
N	size of entry addresses that worms scan
H	size of hitlist (the number of infected machines at the beginning of the spread of active worms)
S	scanning rate (the average number of machines scanned by an infected machine per unit time)
D	death rate (the rate at which an infection is detected on a machine and eliminated without patching)
P	patching rate (the rate at which an infected or vulnerable machine becomes invulnerable)
η_i	number of infected machines at time tick i
m_i	number of vulnerable machines at time tick i
k_i	number of scans at time tick i
e_i	number of newly infected machines at time tick i

5.3 Scanning Rate

The effect of the scanning rate on worm propagation in which worm spreads slowly when the scanning rate decreases [4]. When a worm's signature has been identified, packets containing this signature are dropped when received by the routers with this defense system. In this way, the system can block the scans or the worm copy transmissions from the infected machines, and therefore the scanning rate is reduced.

5.4 Time To Complete Infection

In this we describe the effect of time to complete infection on worm propagation. In the future, worms can become more virulent by utilizing any of the following such methods: scanning the vulnerable machines only, increasing the scanning rate, and exploiting the vulnerability that many computers may have [4]

5.5 Patching

A patch repairs a security hole of a host, which equivalently reduces the total number of vulnerable machines. Statistics show that few worms exploit vulnerabilities that are new and unknown [4]. Popular worms, such as Code Red and Sapphire, attack well-known vulnerabilities.

VI. COMPARISON BETWEEN CYCLIC WORM PROPAGATION MODEL AND ANALYTICAL ACTIVE WORM PROPAGATION (AAWP)

In the cyclic worm propagation model here it can be Describing the worm propagation cycle in real world and identifying the ways that worms exploit to spread themselves, it can be describes prevention mechanisms from two point of views, one is network topological solutions and the other is client side solutions. Models can use these methods for comparing their effectiveness in malware propagations modeling. Some of these methods such as scanning, in the Target Selecting phase are used in all propagation models [1], [8], [9], [10], [11]. In this article we have used the worm propagation model [10]. In the first stage the infected host searches for vulnerable targets. When the target is found the infected host tries to deliver malcode to the selected target.Executing the malcode, the target host would be compromised, making the target an infected host and the cycle goes around. It can most effective to reduce or detect the worm in compromised system. But in an AAWP is a mathematical model to detect the worm from the compromised target system. . It is optimistic in the sense that worms can still be controlled and pre-generated target list, or internally generated target lists as their target discovery technique. Furthermore, we extend our AAWP model to understand the spread of worms that employ local subnet scanning. In this paper we present the AAWP model to analyze the characteristics of the spread of active worm.but the time deterministic model in several specific times their infection is complete but the cyclic worm propagation is not time deterministic. In this model cyclic stages are used for detect worm in their life cycle. Its deployment is difficult than AAWP model. In the AAWP model, the case that worms infect the same destination at the same time is considered, but in cyclic model it is not possible. We believe that the AAWP model is more accurate. Because in the AAWP model, a computer cannot infect other machines before it is infected completely. In a AAWP model considers the patching rate or the time that it takes the worm to infect a machine, but cyclic model not considered these patching rate or time takes a worm to infect the machine.Cyclic model examine their result for the AAWP model. Bothe is correlated to each other.

VII. CONCLUSION AND FUTURE WORK

In this paper some worm propagation methods were described using strategies that fast spreading worms used to propagate themselves through the cyclic worm propagation model. But results of cyclic model are examined in the AAWP model. By defining these methods one can countermeasure them to prevent worm propagation. In order to identify how prevention methods affect on propagation of the worms, we used the two-factor model. In a patch management has a salient effect on decreasing the total number of infected hosts. In this paper we present the AAWP model to analyze then Characteristics of the spread of active worms. Even though the AAWP model also used deterministic approximation, it gives more realistic results when compared to the cyclic worm propagation model and result of cyclic model are examine in the analytical worm propagation model . In particular, a worm using an evenly distributed hitlist spreads at the fastest rate. When the hitlist is concentrated

in some subnet, the spread of active worms is slowed down. We plan to study the effect of the distribution of vulnerable machines in order to get more accurate results.

As part of our ongoing work, we will further study the optimal combination of different defense systems. In addition, we will study the effectiveness of defense systems on a worm that employs other scanning methods, such as localized scanning. If we want to imrove detection accuracy, however, we can add some other rule sets in the worm modeling and more accurately defend the system against real word active worm.

REFERENCES

[1] Michele Garetto, Weibo Gong, and Don Towsley, "Modeling Malware Spreading Dynamics," *IEEE INFOCOM*, 2003.

[2] Mohammad R. Faghani, Hossein Saidi, Mohammad R. Ataei, "Effects of Security Solutions on Worm Propagation", Isfahan University of Technology.

[3] Zesheng Chen, Lixin Gao, Kevin Kwiat, **"**Modeling the Spread of Active Worms", in *Proc. IEEE INFOCOM*, 2003, pp. 1890–1900.

[4] Zesheng Chen, Lixin Gao, and Chuanyi Ji, "On Effectiveness of Defense Systems against Active Worms", proceed in 2003.

[5] Pele Li, Mehdi Salour, and Xiao su, San Jose State university, " a survey of internet worm detection and containment", proceeding in IEEE communication surveys and tutorials, 1553-877X , 1st Quarter 2008.

[6] Masato Uchida, "Discrete modeling of worm spread with random scanning", proceeding in IEICE TRANS.COMMUN.VOL.E95-B No.5 May 2012.

[7] George, R., S. Monirul, and L.Wenke, "Simulating Internet active Worms". Proceeding in IEEE computer society, 2004.

[8] Shigang Chen and Yong Tang, "Slowing Down Internet Worms," 24th International Conference on Distributed Computing Systems (ICDCS'04) Hachioji, Tokyo, Japan, March 24 - 26, 2004, pp. 312-319.

[9] V. Yegneswaran, P. Barford, and J. Ullrich. Internet Intrusions: Global Characteristics and Prevalence. In *ACM SIGMETRICS*, June, 2003.

[10] D. M. Kienzle and M. C. Elder, "Recent Worms: A Survey and Trends, "presented at WORM '03, Washington D.C., USA, 2003.

[11] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time," presented at Security '02, San Francisco, CA, USA, 2002.

[12] M. Bailey, E. Cooke, F. Jahanian, D. Watson, and J. Nazario, "The Blaster Worm: Then and Now," in *IEEE Security & Privacy*, vol. 3, 2005, pp. 26-31.

[13] S. Sellke, N. B. Shroff, and S. Bagchi, "Modeling and Automated Containment of Worms," presented at DSN '05, 2005.

[14] H. Berghel, "The Code Red Worm: Malicious Software Knows No Bounds.," in *Communications of the ACM*, vol. 44, 2001, pp. 15-19.

[15] N. Weaver, "Warhol Worms: The Potential for Very Fast Internet Plagues," http://www.cs.berkeley.edu/©nweaver/warhol.html.

[16] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer Worm," in *IEEE Security & Privacy*, vol. 1, 2003, pp. 33-39.

[17] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A Taxonomy of Computer Worms," presented at WORM '03, Washington D.C., USA, 2003.

[18] C. C. Zou, W. Gong, and D. Towsley, "Code Red Worm Propagation Modeling and Analysis", *9th ACM Conference on Computer and Communication Security (CCS'02)*, Nov. 18-22, Washington DC, USA, 2002.

[19] S. Staniford, V. Paxson, and N. Weaver, "How to own the Internet in your spare time," in *Proc. USENIX Security Symposium*, 2002, pp. 149–167.

[20] Zhang *et. al.* "Analyzing Network Traffic To Detect Self-Decrypting"*ASIACCS'07*, March 20-22, 2007, Singapore.

[21] R. Russell and A. Machie, "Code Red II Worm," Incident Analysis, Security Focus, Tech. Rep., Aug. 2001.

[22] A. Machie, J. Roculan, R. Russell, and M. V. Velzen, "Nimda Worm Analysis," Incident Analysis, SecurityFocus, Tech. Rep., Sept. 2001.

[23] CERT/CC, "CERT Advisory CA-2001-26 Nimda Worm,"http://www.cert.org/advisories/CA-2001-26.html, Sept. 2001.

[24] D. Song, R. Malan, and R. Stone, "A Snapshot of Global Internet Worm Activity," http://research.arbornetworks.com/up media/up files/snapshot worm activity.pdf,Arbor Networks, Tech. Rep., Nov. 2001.

[25] Y. Wang and C. Wang, "Modeling the Effects of Timing Parameters on Virus Propagation," presented at WORM '03, Washington D.C., USA, 2003.

[26] M.Nandhini, "A Survey on modeling and detection of camouflaging worm", proceeding in International Journal OF Multidisciplinary Education Research ISSN: 2277-7881 volume 1, ISSUE 4, SEPT 2012.