ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Modelling for Propagation and Analysis of Worm

Neha Chavan [1], Dipali Chavan [2], Pratiksha Karalkar [3]

U.G. Student, Department of Computer Engineering, SSPM Engineering College, Harkul, Maharashtra, India[1,2,3]

ABSTRACT: In recent years ,the worms and their ability to infect has increased alot. In order to know them we have to look into their payload as well as propagation patterns. An accurate model with proper analysis can help us to comprehensively study how a worm propagates under various conditions. We develop a detailed analytical model that reveals the relationship between network parameters and the spreading rate of worm. Traditionally most modeling in this area concentrated on random scan method. However modeling the permutation scanning worms, a class of worms that are fast yet stealthy has been a challenge to date.

KEYWORDS: Permutation scanning; Worms

I. INTRODUCTION

Computer worm are those who replicate without any human intervention by creating an copy of itself on another computer through some network communication. To better understand the characteristics of worms and potential counter measures through both analysis and prevention. Fast Internet worms have become relatively new threat to Internet infrastructure and hosts to a faster rate. These worms can tamper or attack number of hosts in a short time to minutes now a day and these hosts can be used to perform other attacks, like massively Distributed Denial-of-Service attacks. As the fact that there is no perfect solution to this problem as each worm is unique in its own way so modelling of worms has been a challenge to date.

Worms have the ability to affect a number of hosts in a very short time span. Worms are not just a problem for those who become infected but even to those that are uninfected this increases network load. The propagation characteristics of a worm help to understand and prevent worms from infecting the network further, it is very important to characterize their overall propagation properties and have a proper analysis.

II. RELATED WORK

Linear scanning, where the worm scans a linear address range and partitions this range between itself and any newly infected machine is a strategy which is not seen in practice. It lacks the good initial scattering of random scanning

.Worms pose heavy threat to network. Worms exploit common vulnerabilities in member hosts of a network and spread topologically in the network, a potentially more effective strategy than random scanning for locating victims should be applied. Considering that the topology of networks has important effect on active worm spreading, it is very difficult to model propagation of active worms. For this reason, so far few propagation models are proposed. In this paper, we propose a propagation model of active worms in networks based on permutation method.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

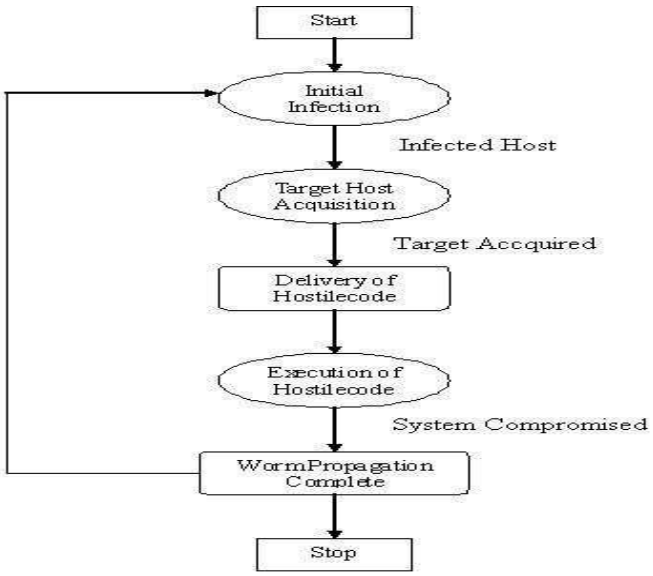
III. PROPOSED SYSTEM

Traditionally all work in this area in concentrate on the relatively simple random-scanning worms. However, modeling the permutation- scanning worms, a class of worms that are fast yet stealthy, has been a challenge to date. This paper proposes a mathematical model that precisely characterizes the propagation patterns of the general permutation-scanning worms. The analytical framework captures the interactions among all infected hosts by a series of interdependent differential equations, which are then integrated into closed-form solutions that together present the overall worm behaviour. We use the model to study how each worm/network parameter affects the worm propagation. We also investigate the impact of dynamic network conditions on the correctness of the model

IV. METHODOLOGY

PERMUTATION SCANNING METHOD:

It uses divide and conquer strategy that reduces chance of scanning the same address again and again. The divide and conquer method is then applied on permutation ring. Each initially infected host starts walking along the ad-dress ring clockwise from its own location and sequentially scans the traversed addresses. Whenever it infects a host, it continues walking and scanning the addresses after that host, while the newly infected host performs a jump.



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

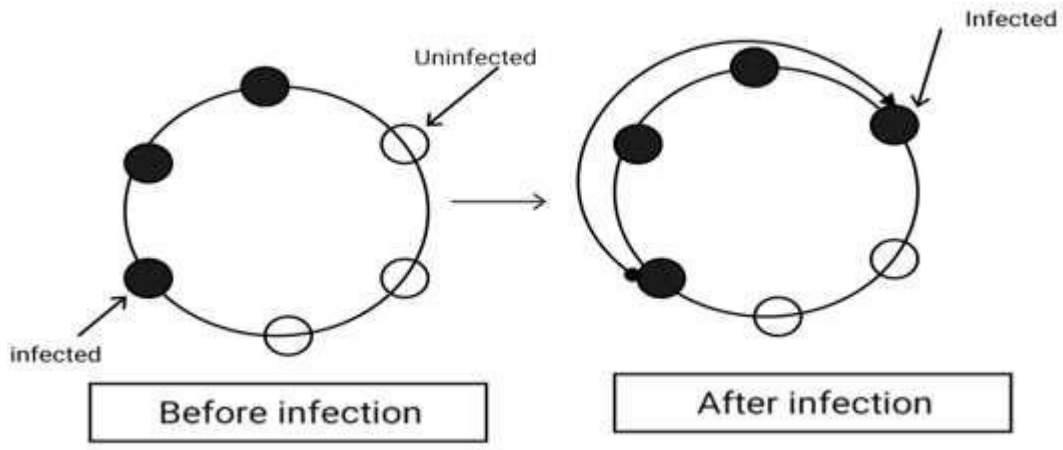
Vol. 6, Issue 3, March 2018

Description:

A data flow diagram provides no information about the timing of processes, or about whether processes will operate in sequence or in parallel. It is therefore quite different from a flowchart, it allows a reader to determine not what kinds of data will be input to and output from the system, where the data will come from and go to, where the data will be stored. Worm propagation can be broadly described by process illustrated in Fig 1.In the Initial Infection the model begins with the presumption that there exists a system that is already infected by the worm and that the worm is active on this system and in Target Acquisition, in order for the worm to propagate itself it must find additional systems to infect. The presence of hostile code on a system is not sufficient for worm propagation; execution of the code must be triggered in some fashion which is done in Execution Step. This process is repeated in a loop till required numbers of hosts are compromised

Multiple method:

In permutation scanning method worm are scanned by using multiple method. In this method if there is a infected host in the permutation ring it then finds the next uninfected host for infection. So according to this method the multiple of the current position of the infected host is taken into consideration and as per the position the host at that position is infected so due to this the drawback of random scan method is effectively solved as the same host will not be infected twice .Due to this method the worms can be scanned in a effective manner



CLASSIFICATION OF VULNERABLE HOST

In our model, we define classes for vulnerable hosts that are uninfected, infected, active, retired, effective, in-effective, and nascent, respectively, and we deliberately make the class notations the same as the corresponding variables in our later propagation model for the sizes of these classes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Terminology:

We classify infected hosts into two categories:

1. active infected hosts, which are actively scanning for vulnerable hosts; and
2. retired infected hosts, which have stopped scanning. When the context makes it clear, we omit infected from the above terms.

Other terms are defined as follows:

1. Jump: When an infected host chooses a random location on the permutation ring to perform its sequentially scan along the ring, we say that the host jumps (to that location).
2. Old Infection: When an active host hits a vulnerable host that was infected previously, we denote the event (as well as host) as an old infection.
3. New Infection: When an active host hits a vulnerable host that was not previously infected we denote the event as a new infection.

We observe that every infected host in the address space belongs to the scanzone of a non-nascent effective host. This is true at the beginning as each of the initially infected hosts belongs to its own scanzone. When a non- effective host infects another host , the address becomes part of scanzone. When retires by hitting (tail of a non-effective host scanzone and the infections made in scanzone now become part of scanzone. Continuing this way, every infected host remains part of the scanzone of a non-nascent effective host until the last active host retires. It should be noted that the scanzones of nascent or ineffective hosts do not contain any infected hosts.

V. WORM DETECTION

The main focus of this section is to detect worms using various scan techniques and we use permutation scan method . Worm scan detection is raising an alarm upon sensing anomalies that are most likely caused by large scale worm spreads. Our goal is to quickly detect unknown worms on large enter- prise networks or the Internet while making the false alarm probability as low as possible.

VI. SUMMARY AND CONCLUSIONS

We studied difference between worms ,virus and trojan horse .In this paper we study the worms. In this project we studied how worm propagate on this network so for this we use permutation scanning method. We first studied precise propagation model for 0-jump.It is concluded that permutation scanning does give a worm an overall advantages relative to random probing. through this output we analyze that permutation scanning worms can infect the host in the network very fast and effectively compared to simple random scanning worms.

VII. RESULTS

So here finally we have successfully modelled the propagation characteristics of permutation scanning worm we have successfully put forth the method of multiple scanning due to which it becomes easier to detect the worms buy avoiding repeated scanning of the host again and again which was seen in previous method . So here in our model we have shown a scenario of four host which are scanned successfully and the worms are detected using the pattern matching technique we can find out whether in the file worm is present or not if yes then it gets detected and is deleted successfully.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

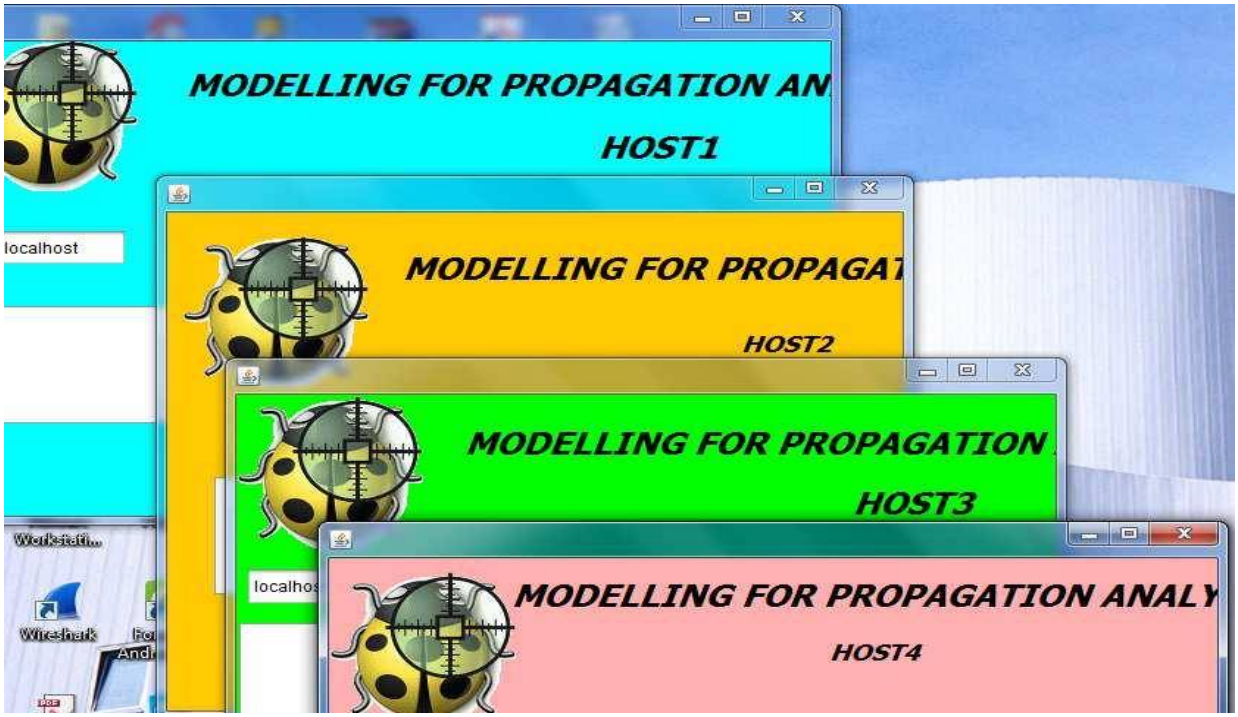


Fig. Network of different host.

In above fig there are four host connecting to each other in ring fashion. That means host1 is connected to host2 and host2 connected with host3 and similarly host3 connected to host4 and host4 to host1.

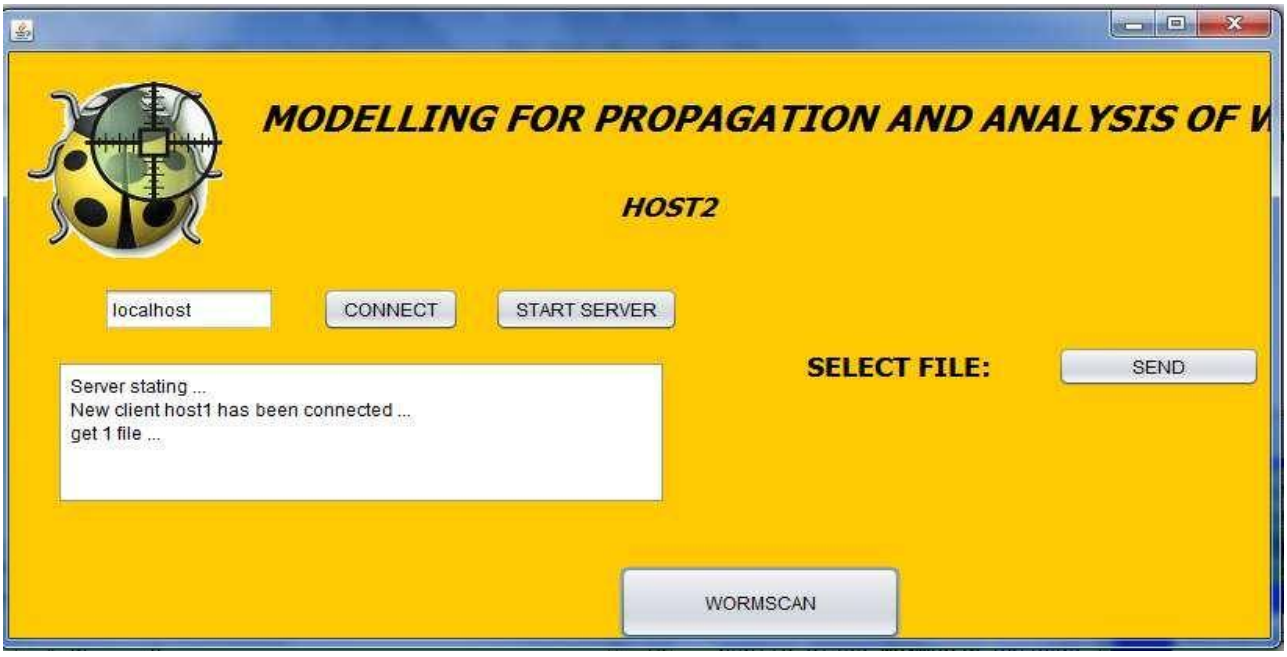


Fig. File sharing to host2.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Fig. Function for worm scanner

REFERENCES

1. SAI DIVYA KALAGATLA,RAMANA REDDY B.,MOHANA ROOPAY " PROPAGATION MODEL FOR PERMUTATION SCANNING WORMS BASED ON DISCRETE TIME SYSTEM". SOME FINE JOURNAL, VOL. 17, PP. 1-100, 1987.
2. Parbati Kumar Manna, Member, IEEE, Shigang Chen, and Sanjay Ranka, Fellow, IEEE. "Inside the Permutati on-Scanning Worms Propagation Modeling and Analysis".
3. Z. Chen, C. Chen, and C. Ji, Understanding localized-scanningworms: Proceeding of the 26th IEEE International Performance Computing and Communication Conference (IPCC07), pp. 186-193, New Orleans, LA, 2008..
4. J. Ma, G. M. Voelker, and S. Savage, Self-stopping worms, in Proc. ACM Workshop Rapid Malcode (WORM), 2005, pp. 1221.
5. G. Gu, M. Sharif, X. Qin, D. Dagon, W. Lee, and G. Riley, Worm detection, early warning and response based on local victim information, in Proc. 20th ACSAC, 2004, pp. 136145.
6. N. Weaver, I. Hamadeh, G. Kesidis, and V. Paxson, Preliminary results using scale-down to explore worm dynamics, in Proc. ACM Workshop Rapid Malcode (WORM), Mar. 2004, pp. 6572