ISSN 1512-1232

# Server Worm Detection by Using Intelligent Failure Connection Algorithm

Mohammad M. Rasheed[1], Osman Ghazali[2] and Norita Md Norwawi[3]

[1,2]Graduate Department of Computer Science, College of Arts and Sciences,
University Utara Malaysia, 06010 UUM Sintok, Kedah, MALAYSIA, E-mail : [1] mohmadmhr@yahoo.com

[3]Faculty of Science and Technology, University Sains Islam Malaysia, 71800 Nilai, N.Sembilan, MALAYSIA

***Abstract***

*On July 19th 2001 "Code-Red" was released to the internet after fourteen hours the worm infected 36,000 hosts. Internet worm procedure that spread autonomously from one host to another, worm requires host computer with an address on the Internet and any of several vulnerabilities to create a big threat environment. To decrease the false alarm in IFCA (Intelligent Failure Connection Algorithm) we proposed server worm register to register the number of the computer that infected by the worm. We are finding SWD (Server Worm Detection) by using IFCA is more reliable because it reduced the false alarm. Also, when the computer infected by the worm many computers that connected throw internet will be received the warning by using our proposed.*

***Keywords:*** *worm detection, algorithm security detection, intelligent detection.*

## I. INTRODUCTION

The "Morris Worm" of 1988, which required no human mutual action but only a host computer with an address on the Internet and any of several vulnerabilities, created a completely new threat environment [1], that a worm could bring the Internet down in hours. New worm outbreaks have occurred periodically even though their mechanism of spreading was long well understood

Passive worms are different from viruses in that they are completely autonomous entities. Virus is dependent upon a host file or boot sector, and the transfer of files between machines to spread, while a worm can run independently and spread through network connections. Active worm spread in an automated style and can flood the internet in a very short time.

Anti-virus is signature-based technology [2] which compares the file structure to the signatures stored in its database. If the file contain same signature, so it is infected by the worm. The anti-virus database must be updated continuously to detect new worms.

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention.

Currently, worms are serious security threat that may cause congestion in the network which leads to large queuing delays, and high packet loss. Since Code Red and Nimda worms were spread in 2001, Epidemic-style attacks have caused huge damages. The Worm handling must be automatic to have any chance of success because worms spread too fast [3]. The internet is an influential function in the economy and reckon mainstay to the life. Once the internet is broken down, it will cause a huge economic loss.

Unlike viruses, worms do not need to attach themselves to an existing program. Passive worms can run completely independently and through a network of connections, while virus needs a host file, boot sector or file transfer between machines to propagate [4].

There are few solutions to solve the worm attack. One of the solutions to update the anti-virus for detects the worms. Anti-virus cannot detect the worm due to its spreading speed. Also, anti-virus cannot detect unknown internet worms automatically because it does not depend on the worm

ISSN 1512-1232

behavior but depends on signature to detect the worm. Routers and firewalls can block packets using traffic signatures, but this happens after the worm has already spread.

Automatic detection is particularly challenging because it is difficult to predict what form that the next worm will take. However, automatic detection and response is fast becoming an imperative because a recently released (flash or topological) worm can infect millions of hosts in a matter of seconds.

The technology directed to scrutinize the way of the error message, such as RESET in TCP and ICMP (internet controller message protocol) destination unreachable message.

In remainder of this paper is organized as follows. Section II describes related work. Section III describes IFCA. Section IV describes SWD by using IFCA. Section V compares between IFCA and SWD by using IFCA. Finally section VI is the conclusion.

## II. RELATED WORK

Zou et al. [5] introduced the architecture of a worm monitoring system. The monitoring system aims to provide comprehensive observation data on a worm's activities for the early detection of the worm. Zou focused just on the ICMP message.

Berk et al. [6] proposed a monitoring system by collecting ICMP; the Internet Control Message Protocol (ICMP) provides such error notification. Berk used a potentially unlimited number of collectors and analyzers.

Schechter et al. [7] proposed worm detection method based on the failed connection. This algorithm can detect internets worm but doesn't work well on detecting stealthy worm. The threshold for the algorithm cannot detect stealthy worm.

Yang et al. [8] built algorithm for detecting the worm which has two sub algorithms: the first algorithm "short term algorithm" runs well to detect worm while the second algorithm "longer term algorithm" cannot detect all types of the stealthy worm. In addition, Yang's algorithm cannot hold any equations to determine specification when the equation runs in the algorithm to detect early worm if it has higher rate for value in average of failure connection. Yang's algorithm focuses on detecting the computer that contains the worm only.

Rasheed et al. [9] proposed IFCA that contented intelligent early system detection mechanism for detecting internet worm. The mechanism of this technique is concerned with detecting the internet worm and stealthy internet worm. In order to reduce the number of false alarm, the impact of normal network activities is involved but TCP failure and ICMP unreachable connection on same IP address are not calculated because the internet worm strategic attack on the different IP address. But this algorithm works in the local network.

## III. IFCA

IFCA [9] appoints the difference between regular connection and worm connection. The worm scans different IP addresses every second. IFCA depends on the TCP failure and ICMP unreachable connection on different random addresses. There will be in a large number of failures connections if the computer has worm.

IFCA is based on Artificial Immune System; the Artificial Immune System distinguishes between self and non-self. An Artificial Immune System (AIS) is a bio-inspired classification system which is derived from the Human Immune System (HIS). AIS are one of the most recent approaches in computational intelligence. They provide effective information processing capabilities [10].

IFCA mechanism records the number of first failed connection packets such as ICMP and TCP RESET packets that returned from the external destination address to the internal forged and monitored source IP address based in the router. Once detecting the first failed connection packets, the algorithm then extracts (the source address, source port, destination address, destination port) from the packet and creates the record. The IFCA works on the local network see figure1.

ISSN 1512-1232

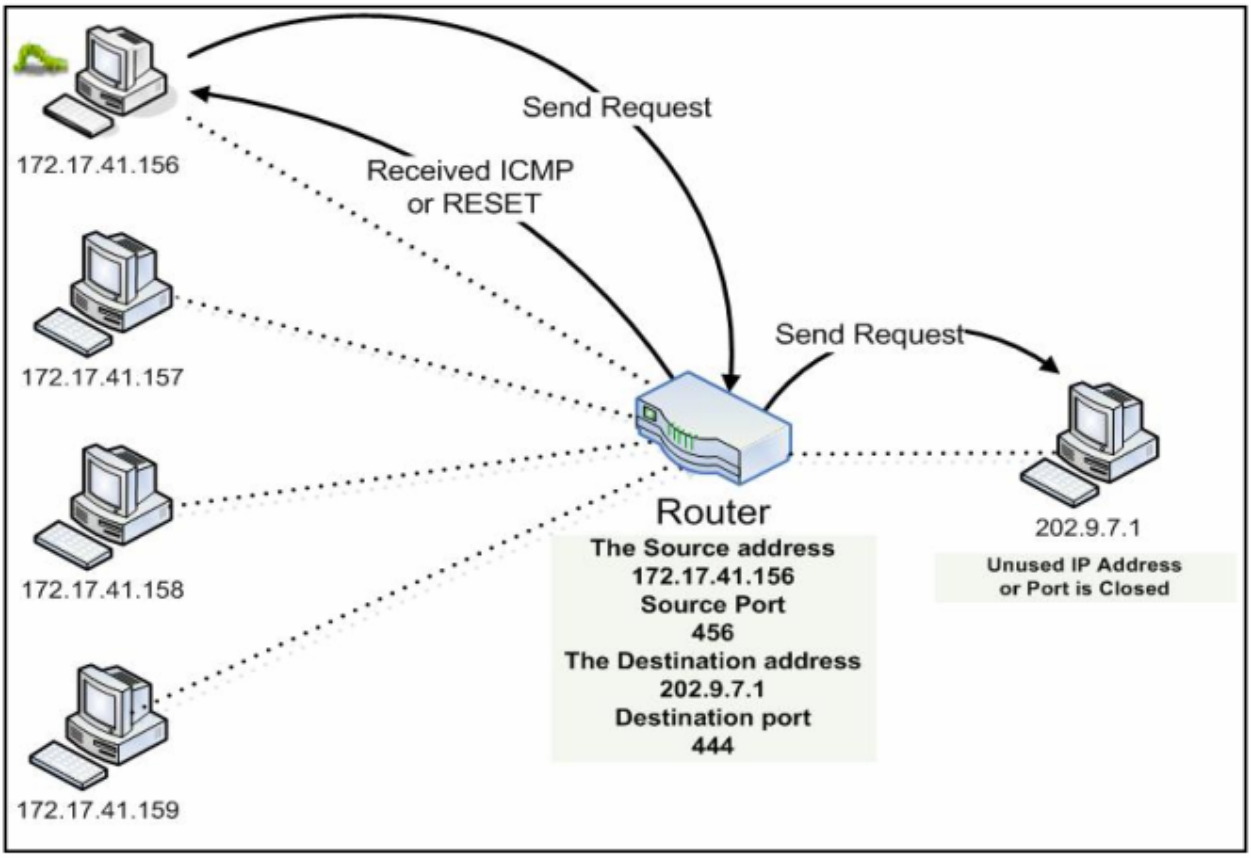


Figure1. Intelligent Failure Connection Algorithm

## IV. SWD BY USING IFCA

Our proposed works when three deferent computers sending the warning to the server throw the internet.

IFCA detects the worm and send the warning to the server but sever does not send the warning to all clients because it least the server must be three warning after that sending the warning to all clients that share this service, so that our proposed is reduced the false alarm.

Antibody works when the viruses or germs infected the body the Human Immune System detect this viruses or germs and send warning to all parts of the body about this warning.

Our proposed it is same Human Immune System for protect the internet from the internet worms.

ISSN 1512-1232

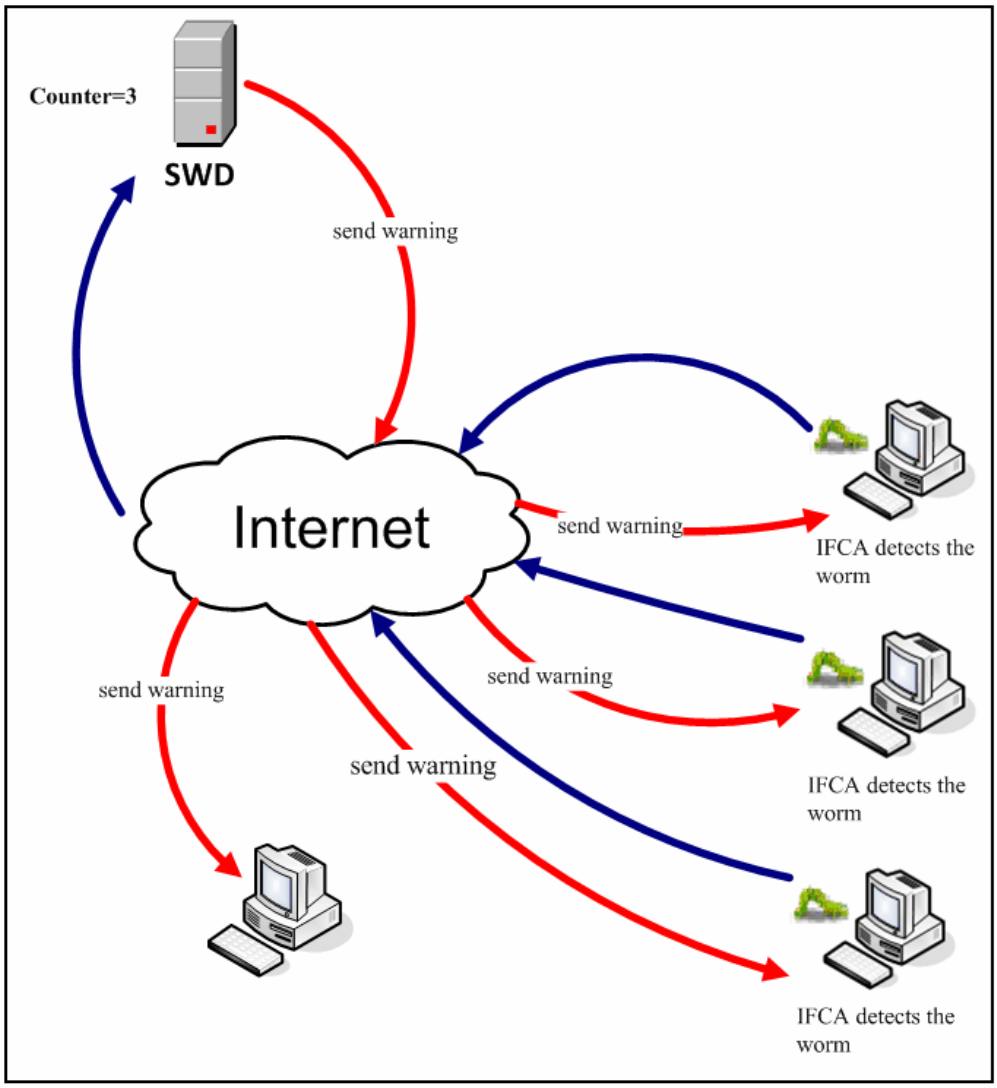


Figure 2. SWD by using IFCA

## V. COMPARE BETWEEN IFCA AND SWD BY USING IFCA

In this section we compare between IFCA and SWD by Using IFCA as shown in the table 1.

TABLE I

COMPARE BETWEEN IFCA AND SWD BY USING IFCA

| **IFCA** | **SWD by Using IFCA** |
|---|---|
| Detect the worm in local network | Detect the worm in internet |
| Reduce false alarm | Reduce false alarm more than IFCA |
| Send the alarm to all clients on the network | Send the alarm to all clients on the internet |

We are finding the Server Worm Detection by using IFCA is more reliable because it reduced the false alarm in IFCA. Also, when the computer infected by the worm many computers that connected throw internet will be received the warning by using our proposed. But IFCA the computers received the waning on the local network.

ISSN 1512-1232

## VI. CONCLUSION

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention.

IFCA appoints the difference between regular connection and worm connection. The worm scans different IP addresses every second. IFCA depends on the TCP failure and ICMP unreachable connection on different random addresses. There will be in a large number of failures connections if the computer has worm. But IFCA works on the local network.

Our proposed works when three deferent computers sending the warning to the server throw the internet. After that our proposed send the waning to all clients on the internet.

We finding our proposed can detect the worm in internet with reduced false alarm more than IFCA. Our proposed send the alarm to all clients on the internet.

## REFERENCES

[1] W. Debany. "Modeling the Spread of Internet Worms via Persistently Unpatched Hosts". IEEE Journal, Volume 22, Issue 2, Mar 2008, pages 26 – 32.

[2] T. Alagna, E. Chen, C. Elliott, R. Elron, S. W. Foster, J. Kennedy, M. Mahdavi, G. G. McBride, R. Moritz, J. Nisbet, J. Porell, H. Schmidt, J. C. Seanor, S. Singh, S. Stolfo and M. Xie, Defending the Digital You: How to Fight Online Identity Theft, Washington: Larstan Publishing Inc., 2005.

[3] M. Costa, J. Crowcroft, M. Castro, A. Rowstron, L. Zhou, L. Zhang, and P. Barham, "Vigilante: End-to-end containment of Internet worms", In Proc. of the 20th ACM Symp. on Operating Systems Principles (SOSP), Brighton, UK, Oct. 2005.

[4] Worms, Computer worms information, Retrieved January 2, 2009, from http://virusall.com/worms.shtml

[5] C.C. Zou, L. Gao, W. Gong, and D. Towsley, " Monitoring and Early Warning for Internet Worms," In 10th ACM Symposium on Computer and Communication Security, Washington, 2003.

[6] V. H. Berk, R.S. Gray, and G. Bakos, "Using Sensor Networks and Data Fusion for Early Detection of Active Worms,"Proceedings of the SPIE AeroSense, pp. 92–104, 2003.

[7] S. Schechter, J. Jung, & A. Berger. "Fast Detection of Scanning Worm Infections", Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID), Sophia Antipolois, France, Sep 2004.

[8] X. Yang, J. Lu, Y. Zhu & P. Wang. "Simulation and Evaluation of a New Algorithm of Worm Detection and Containment", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), Taiwan, Dec 2006, pp. 448-453.

[9] M. M. Rasheed, N. M. Norwawi, O. Ghazali, and M. M. Kadhum, "Intelligent Failure Connection Algorithm for Detecting Internet Worms," International Journal of Computer Science and Network Security, May 2009, Vol. 9, No.5, pp. 280-285.

[10] S. Schaust & M. Drozda . "Influence of Network Payload and Traffic Modelson the Detection Performance of AIS", IEEE International Conference, 2008, pp. 44-51.

Article received: 2010-05-12