Research Journal of Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 2 (4): 228-234, 2010
ISSN 1815-7432

Server Scanning Worm Detection by using Intelligent Failure Connection Algorithm

[1]M.M. Rasheed, [1]O. Ghazali and [2]N.M. Norwawi
[1]Graduate Department of Computer Science, College of Arts and Sciences,
Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia
[2]Faculty of Science and Technology, Universiti 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 spreads 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. The aim of this study is to propose Server Worm Register (SWD) to register the number of computers that are infected by the worm. Our proposal decreases the false alarm in Intelligent Failure Connection Algorithm (IFCA). Our proposal also works when the computer is infected by the worm and IFCDA detected the worm, many computers that are connected through the internet will receive the warning by using our proposal. We have found IFCA is more reliable by using SWD because it reduced the false alarm.

Key words: Internet worm detection, firewall, router

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 (Debany, 2008). The 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 spreads in an automated style and can flood the internet in a very short time.

Anti-virus is signature-based technology (Alagna *et al.*, 2005) which compares the file structure to the signatures stored in its database. If the file contains the 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.

Corresponding Author: Mohammad M. Rasheed, Graduate Department of Computer Science,
College of Arts and Sciences, Universiti Utara Malaysia,
06010 UUM Sintok, Kedah, Malaysia

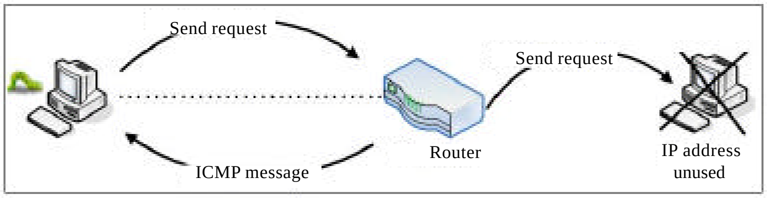

Fig. 1: ICMP unreachable message

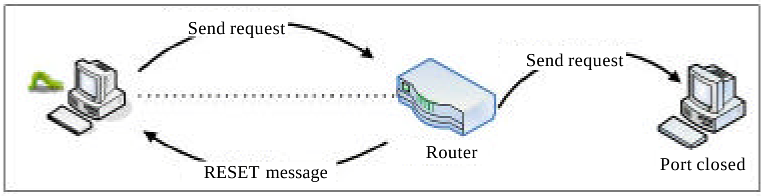

Fig. 2: RESET message

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 (Costa *et al.*, 2005). The internet is an influential function in the economy and is considered mainstay to life. Once the internet breaks 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.

There are few solutions to solve the worm attack. One of the solutions is to update the anti-virus to detect 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 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 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.

Usually, the worm keep IP address in list or generates IP address resulting in several failure connection messages received when the computer is infected by the worm, when the IP address is unused in the destination IP address as shown in the Fig. 1, the router returned an Internet Control Message Protocol (ICMP) destination unreachable to source IP (infector computer) (Ellis *et al.*, 2004).

When the worm send a SYN packet from the source IP address to a distention IP that is being used as shown in the Fig. 2 but if the destination port is closed then the router will return the TCP RESET message (Ellis *et al.*, 2004).

Zou *et al.* (2003) 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.* (2003) proposed a monitoring system by collecting ICMP, Berk used a potentially unlimited number of collectors and analyzers.

Schechter *et al.* (2004) proposed worm detection method based on the failed connection. This algorithm can detect internet worm but doesn't work well on detecting stealthy worm. The threshold for the algorithm cannot detect stealthy worm.

Yang *et al.* (2006) 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.* (2009) proposed IFCA that contained 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 is on the different IP address. But this algorithm works in the local network.

IFCA

IFCA distinguishes the difference between regular connection and worm connection (Rasheed *et al.*, 2009). 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 a large number of failure 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 is one of the most recent approaches in computational intelligence. It provides effective information processing capabilities (Schaust and Drozda, 2008).

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 as shown in the Fig. 3.

SWD BY USING IFCA

Our algorithm detects the worm and sends the warning to the server but sever does not send the warning to all clients. This because it must send a minimum three warning to send the warning to all clients that share this service, so that false alarm can be reduced as shown in the Fig. 4.

Antibody works when the viruses or germs infected the body. The Human Immune System detects this viruses or germs and sends warning to all parts of the body about this warning. Our proposal is the same as Human Immune System to protect the internet from the internet worms.

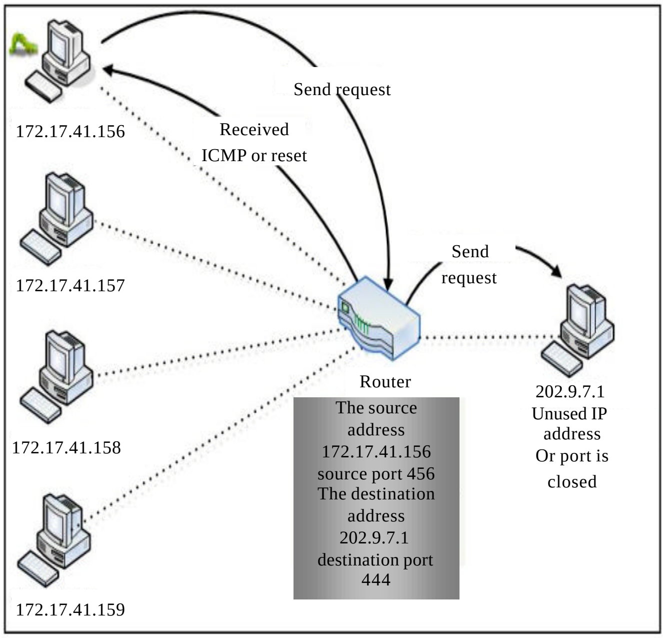

Fig. 3: Intelligent failure connection algorithm

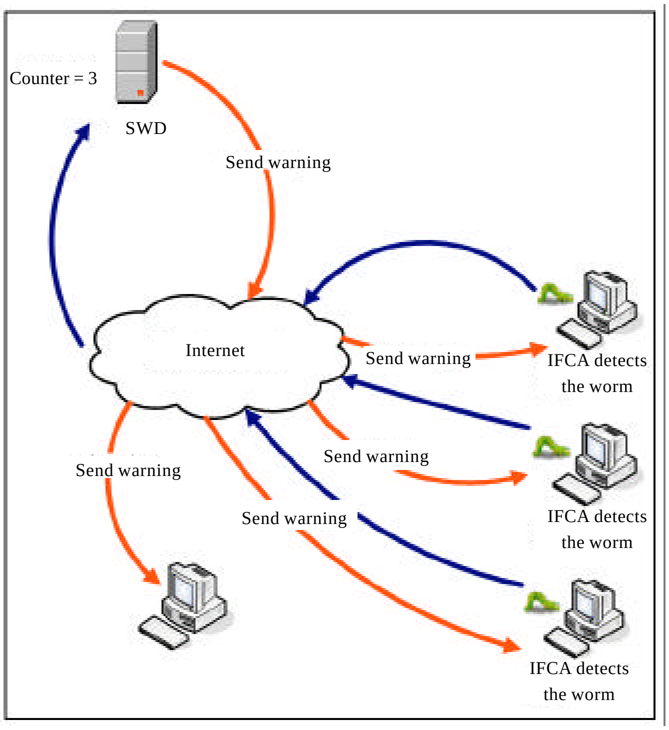

Fig. 4: SWD by using IFCA

Our proposal mechanism records the number of failed connection packets such as ICMP and TCP RESET packets that are returned from the external destination address to the internal forged. It monitors the source IP address placed in the router. Once the first failed connection packets are detected, the algorithm then extracts the source address, source port, destination address and destination port from the packet and creates the record. The false positive rate is largely reduced when our proposal receives normal connection, i.e., TCP SYN/ACK; counter is decreased. Also, our proposal ignores the packet when the destination IP is recorded into the counter table because the internet worm attack strategy is attacking different IP address.

Our proposal will remove the counter every three days. β = 100/min failed rate of threshold. Then Average of Failure Connection (AFC) in 1 min = (1 to n).

$$\text{AFC} = \text{Counter/Minute} \tag{1}$$

Threshold can be processed by the following equation of Summation of threshold (ST):

$$\text{ST} = 2\text{^}\,(6.65 + 0.050054\,(\beta\ \text{-AFC})) \tag{2}$$

Our proposal equation depends on the average of failure connection to compute the threshold. Our proposal can detect the worm early in usual time. But if the worm cannot be detected in the early stage, the algorithm provides more time and new threshold to detect the worm.

Our proposal can detect the worm by calculating different time on different number of failure connections.

The algorithm calculates ST, if ST reaches greater than fifteen failure connections the algorithm goes to next stage. Otherwise the traffic will be forwarded.

$$\text{T1} = (\text{ST/AFC}) \tag{3}$$

$$\text{T2} = (\text{Time now-Time start of the algorithm}) \tag{4}$$

Our proposal calculates the threshold every time. Our algorithm detects the worm by comparing T1 to T2 as follows: If (T2 is small or equal to T1) and (the counter is greater than or equal to the summation of Threshold) send warning to Server Worm Detection (SWD), when the SWD detects three computers or more have worm failure connection warning and send warning to all clients. Else check T1, T2. If (T2 is greater than T1), then go to feed back and decrease the average with new calculation to give another chance to detect the worm. If T1 small than T2, then the traffic will be forwarded because it is a normal connection. Whenever the counter value does not exceed the threshold during time cumulative computation phase, the traffic sent from the corresponding IP address would be forwarded as normal activity as shown in the Fig. 5.

COMPARISON BETWEEN IFCA AND SWD BY USING IFCA

Here, we compare IFCA and SWD by using IFCA as shown in the Table 1. We find the Server Worm Detection by using IFCA is more reliable because it reduces the false alarm in IFCA. Also, when the computer is infected by the worm many computers that are connected through internet will receive the warning by using our proposal. However, IFCA the computers receive the waning on the local network.

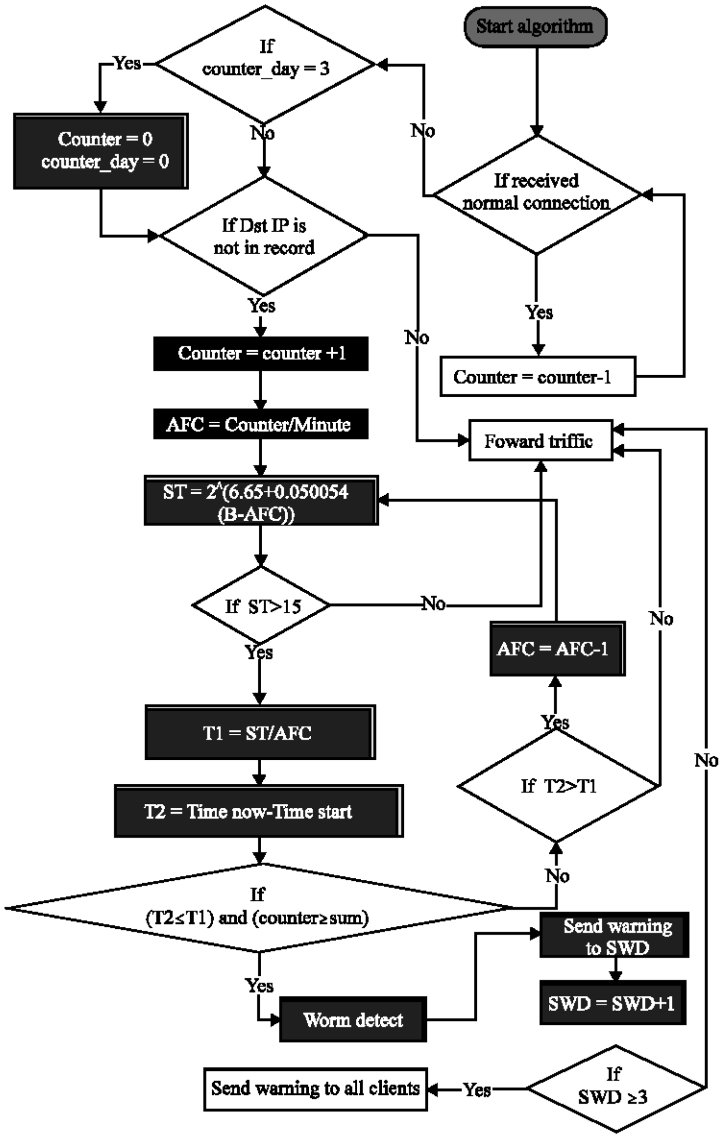

Fig. 5: The flow chart of the SWD

Table 1: Comparison 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

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 distinguishes 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 a large number of failure connections if the computer has worm. But IFCA works on the local network. Our proposal works when three different computers send warning to the server through the internet. After that our proposal send the waning to all clients on the internet. We found our proposal can detect the worm in the internet with reduced false alarm much more than IFCA.

REFERENCES

Alagna, T., E. Chen, C. Elliott, R. Elron and S.W. Foster *et al*., 2005. Defending the Digital You: How to Fight Online Identity Theft. Larstan Publishing Inc., Washington.

Berk, V.H., R.S. Gray and G. Bakos, 2003. Using sensor networks and data fusion for early detection of active worms. Proc. SPIE, 5071: 92-92.

Costa, M., J. Crowcroft, M. Castro, A. Rowstron, L. Zhou, L. Zhang and P. Barham, 2005. Vigilante: End-to-end containment of internet worms. Proceedings of the 20th ACM Symposia on Operating Systems Principles, Oct. 23-26, Brighton, UK., pp: 1-15.

Debany, W., 2008. Modeling the spread of internet worms via persistently unpatched hosts. IEEE Network, 22: 26-32.

Ellis, D.R., J.G. Aiken, K.S. Attwood and S.D. Tenaglia, 2004. A behavioral approach to worm detection. Proceedings of the 2nd ACM Workshop on Rapid Malcode, Washington DC, USA., Oct. 29, ACM, New York, USA., pp: 43-53.

Rasheed, M.M., N.M. Norwawi, O. Ghazali and M.M. Kadhum, 2009. Intelligent failure connection algorithm for detecting internet worms. Int. J. Comput. Sci. Network Security, 9: 280-285.

Schaust, S. and M. Drozda, 2008. Influence of network payload and traffic modelson the detection performance of AIS. Proceedings of the IEEE International Conference, June 16-18, Edinburgh, pp: 44-51.

Schechter, S., J. Jung and A.W. Berger, 2004. Fast Detection of Scanning Worm Infections. In: Lecture Notes in Computer Science, Jonsson, E., A. Valdes and M. Almgren (Eds.). Springer, Berlin, Heidelberg, 978-3-540-23123-3, pp: 59-81.

Yang, X., J. Lu, Y. Zhu and P. Wang, 2006. Simulation and evaluation of a new algorithm of worm detection and containment. Proceedings of the 7th International Conference on Parallel and Distributed Computing: Applications and Technologies, Dec. 4-7, Hang Zhou, China, pp: 448-453.

Zou, C.C., L. Gao, W. Gong and D. Towsley, 2003. Monitoring and early warning for internet worms. Proceedings of the 10th ACM Symposium on Computer and Communication Security, Oct. 27-30, ACM, New York, USA., pp: 190-199.