Intelligent Failure Connection Algorithm for Detecting Internet Worms

Mohammad M. Rasheed, Norita Md Norwawi, Osman Ghazali, and Mohammed M. Kadhum

Graduate Department of Computer Science, College of Arts and Sciences,
Universiti Utara Malaysia
06010 UUM Sintok, MALAYSIA

Summary
Morris worm showed the Internet community for the first time in 1988 that a worm could bring the Internet down in hours. Worm requires host computer with an address on the Internet and any of several vulnerabilities to create a big threat environment. We propose intelligent early system detection mechanism for detecting internet worm. The mechanism of our technique is concerned with detecting the internet worm and stealthy internet worm. The average of failure connections by using Artificial Immune System (AIS) is the main factor that our technique depends on in detecting the worm. In this paper, we show that our algorithm can detect new types of worms. This paper shows that intelligent Failure Connection Algorithm (IFCA) operation is faster than traditional algorithm in detecting worms.

Key words:
Internet worm Detection, Firewall, Router.

1. Introduction

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other 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 in order to have any chance of success because worms spread too fast [8]. 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 a virus, 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 [1].
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.
An ICMP "Destination Unreachable" returned only when the IP addresses is unused. When a SYN packet is sent to a used IP address with destination port closed, TCP RESET packet is returned [2].
Anti-virus can't detect the worm due to its spreading speed. Also, anti-virus can't detect unknown internet worm automatically because it doesn't depend on the worm behavior but depend on signature to detect it. Therefore, the anti virus can't detect most of unknown internet worm automatically.
There are a few of the solutions to solve the worm attack. One of solutions is updating anti-virus to detect the worms, but cannot detect unknown worms. Antivirus can not detect unknown Internet worms automatically because it does not depend on the behavior of the worms, but depends on the signature to detect the worm. Firewalls and routers can be used to block the worm traffic signature, but this occurs after the worm spread.
The remainder of this paper is organized as follows. Section 2 describes related work. Section 3 shows the design of the anti-internet worm through three steps. Section 4 discusses the result. Section 5 concludes the proposed mechanism.

2. Related Work

Schechter et al. [3] introduced worm detection method based on the failed connection. This algorithm can detect the internet worm but doesn't work well on detecting stealthy worm. The threshold can't detect stealthy worm.
Chen & Tang [4] analyzed the essential character of TCP based worm's propagation that sending out a large number of TCP connection requests. They proposed an effective approach to detect and contain network worms based on the number of failure connection received by the network routers. The approach can be divided into two defense phrases: short term and longer term. This strategy may works well on detecting uniform scanning worm and

Manuscript received May 5, 2009
Manuscript revised May 20, 2009

"stealthy" worm, however the impact of normal network activities has not been considered. Then, the rate of false alarms could be large and take long time to detect the worm.

Yang et al. [5] built an algorithm for detecting the worm which has two sub algorithms. The first algorithm that is "short term algorithm" runs well to detect worm while the second algorithm that is "longer term algorithm" cannot detect all types of the stealthy worm. In addition, Yang's algorithm cannot hold any equation 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.

In this paper we propose a new equation that depends on the AIS to compute the threshold. Also, we propose an intelligent way to compute the threshold range for detecting new types of worm. IFCA can detect the worm earlier than the traditional algorithms (see table 1).

Table 1: Mechanisms Analysis

Algorithm Name	*Worm Detection*	*Stealthy worm Detection*	*Speed*
Schechter [3]	(√)	-	Slow
Chen [4]	(√)	-	Slow
Yang [5]	(√)	(√) but some worm cannot detect it	fast
Our proposed algorithm	(√)	(√)	Faster than Yang's algorithm

3. Design of IFCA

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. Therefore, there will be a large number of failures connections if the computer has worm.

Biological immune system is a typical distributed parallel system for processing biological information to defense the body against viruses and diseases [6]. 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 [7].

If normal connection is received, i.e. TCP SYN/ACK, "counter" will be decreased. Only the first failed connection sent from the forged source IP address to different destination IP address is recorded. Normal network activities are considered to decrease the counter's value. IFCA will remove the "counter" every three days. The packet should be ignored when the destination IP is recorded into the counter table.

Our 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 monitored source IP address based in the router (see figure 1). 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.

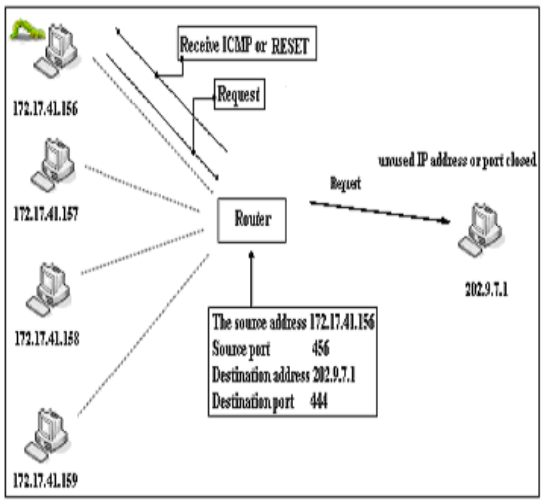

Fig. 1: Error message returned to router

We suppose β =100. Then X= (1 to n) average of failure connection in one minute. Threshold can be processed by the following equation:-

***Summation of threshold*= 2^ (6.65 + 0.050054 (β -X)).**

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

The Yang's algorithm [5] detects the internet worm if the failure connection is equal or greater than 100/minute failure connections by using "long term" algorithm. When the failure connection is equal or greater 3000/day failure connection the Yang algorithm detects this type of stealthy internet worm by using "shorter term" algorithm. Our algorithm can detect the worm by calculating different time on different failure connections .We use Yang's algorithm to calculate the warning.

T1= (summation of Threshold / average of failure connection)
T2= (time now – time start of the algorithm)

Unlike Yang's algorithm, IFCA is more dynamic in detecting the worm because it calculates the threshold every time. IFCA detects the worm by compare 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) the worm is detected. Else check T1, T2. If (T2 is greater than T1), then go to feed back and decrease the average with new calculate to give other chance to detect the worm. If T1 small than T2, then forward the traffic because it is a normal connection. Whenever the counter value does not exceed the threshold during time cumulative computation phrase, the traffic sent from the corresponding IP address would be forwarded as normal activity (see figure 2).

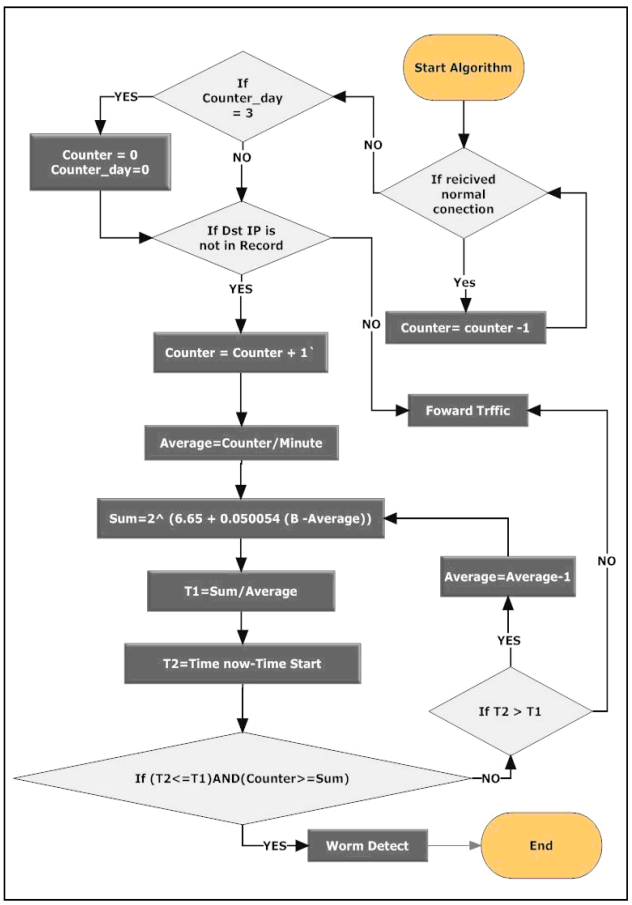

Fig. 2: The flow chart of the IFCA

4. Results

This section discusses the result of the study Section 4.1 shows results of faster work detection and section 4.2 shows the detection of new types of worms. The result in this section is obtained by using the same types of worms that are tested on the two different algorithms namely Yang algorithm Yang et al. [5] and IFCA.

4.1. Results for Faster Detection

Figures 3, 4, 5 and 6, show four types of worms are detected Yang et al. [5] algorithm. Figure 3 shows the average of failure connection is 88/minute, and the time process to detect a worm is 34min 5sec Figure 4 shows the average of failure connection is 93/minute, and the time process to detect the worm is 32min 15sec. In figure 5, the average of failure connection is 76/minute, and the time process to detect the worm is 39min 28sec. In figure 6, the average of failure connection is 97/minute, and the time process to detect the worm is 30min 55sec.

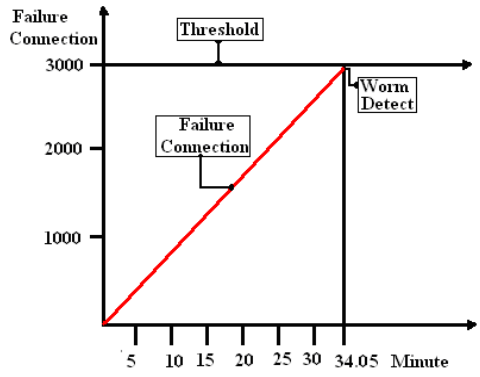

Fig. 3: Yang algorithm detected the worm after 34min 5 sec

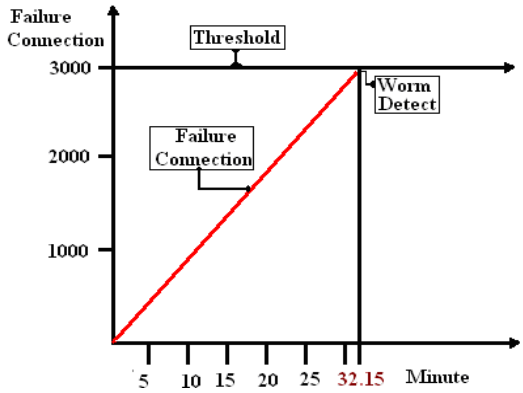

Fig. 4: Yang algorithm detected the worm after 32 min 15 sec

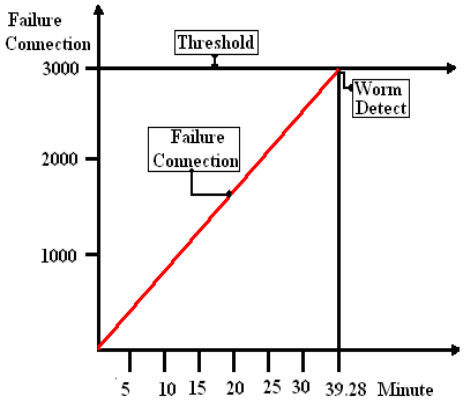

Fig. 5: Yang algorithm detected the worm after 39 min 28 sec

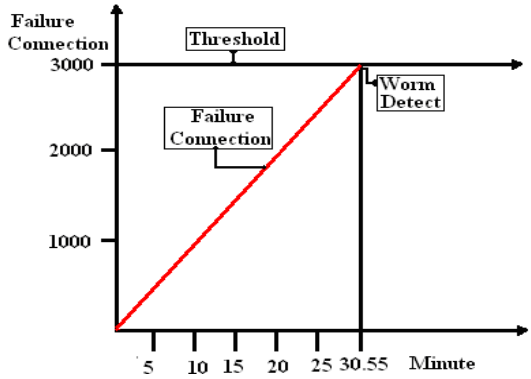

Fig. 6: Yang algorithm detected the worm after 30 min 55 sec

Figures 7, 8, 9 and 10, show four types of worm are detected by IFCA. Figure 7 shows the average of failure connection which is 88/minute, and the time process to detect the worm is 103 sec. In figure 8, the average failure connection is 93/minute, and the time process to detect the worm is 82sec. In figure 9, the average of failure connection is 76/minute, and the time process to detect the worm is 3min 1sec. In figure 10, the average of failure connection is 97/minute, and the time process to detect worm is 68sec.

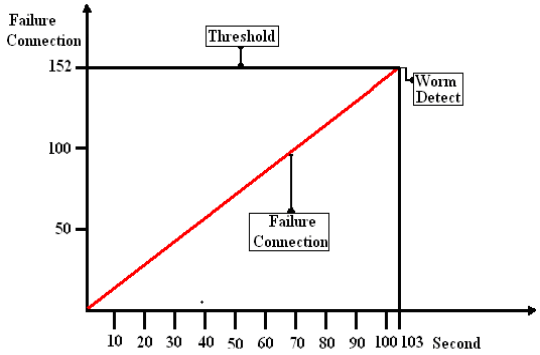

Fig. 7: IFCA detected the worm after 103 sec

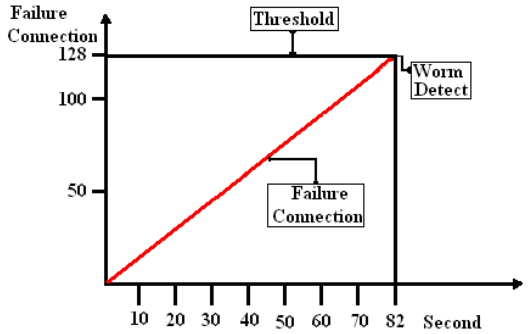

Fig. 8: IFCA detected the worm after 82 sec

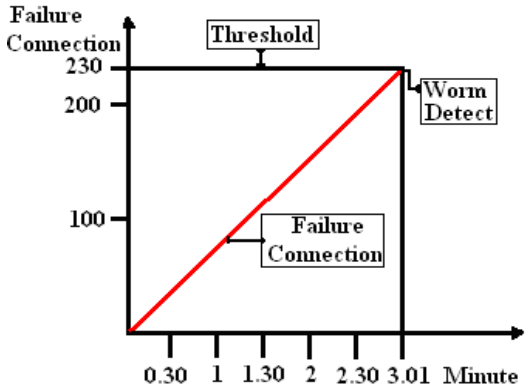

Fig. 9: IFCA detected the worm after 3 min 1 sec

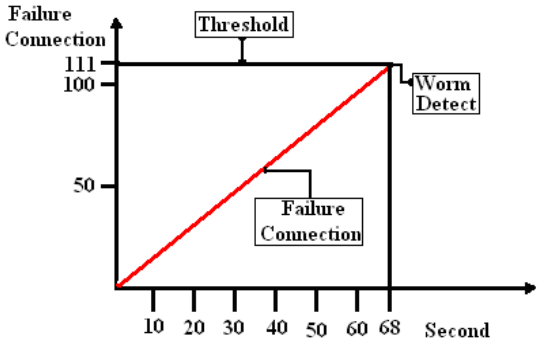

Fig. 10: IFCA detected the worm after 68 sec

IFCA operation is faster than Yang et al. [7] algorithm.

4.2. Result of Detecting Other Worm Types

In first experiment, we used Yang algorithm to detect a worm. The worm has failure connection 2360/day and the result after 30 hours is that the algorithm cannot detect this worm as shown in figure 11. Yang algorithm‘s [5] has to check again the system after 24 hours. Yang algorithms cannot detect this type of worm. This worm has properties less than 3000/day failure connection.

In the second experiment, we used the IFCA to detect the worm. The worm has failure connection 2360/day, and after 30 hours IFCA can detect this worm as shown figure 12.

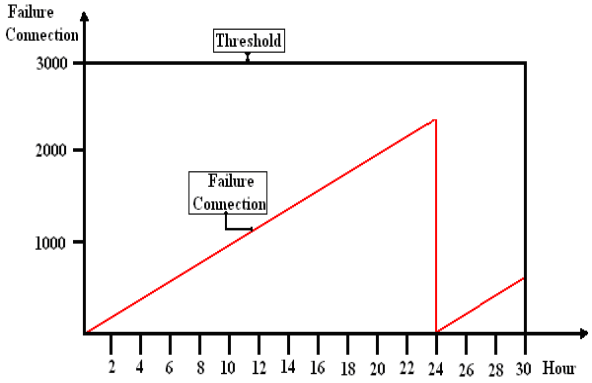

Fig. 11: Yang algorithm can't detected the worm after 30 hours

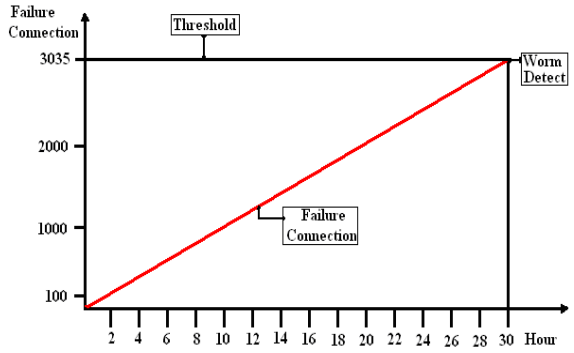

Fig. 12: IFCA detected the worm after 30 hours

The results show that IFCA detects other types of worms, while Yang algorithm failed to detect these types of worms.

5. Conclusion

In this work, we examined only one worm and test it on different spreading speed because all internet worms have same properties of failure connection [2].
The results show that the IFCA detects the worm faster than traditional Failure Connection algorithm. Also, the algorithm can detect different types of worms.

References

[1] Computer worms information, http://virusall.com/ worms.shtml Accessed Jan. 2nd, 2008.
[2] D. Ellis, J. Aiken, K. Attwood, and S. Tenaglia. "A Behavioral Approach to Worm Detection". Proceedings of the Second ACM Workshop on Rapid Malcode (WORM), Oct 2004, pages 43 – 53.
[3] 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.
[4] S. Chen & Y. Tang. "DAW: A Distributed Antiworm System". IEEE Journal, Volume 18, Issue 7, Jan 2007, Pages 893 – 906.
[5] 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, pages 448-453.
[6] T. Gong, "Unknown Non-self Detection & Robustness of Distributed Artificial Immune System with Normal Model", Proceedings of the 7th World Congress on Intelligent Control and Automation, Chongqing, China, Jun 2008, pages 1444-1448.
[7] S. Schaust & M. Drozda . "Influence of Network Payload and Traffic Modelson the Detection Performance of AIS". IEEE International Conference, 2008, pages 44-51.
[8] 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.

Mohammad M. Rasheed received his B.Sc. in Computer Science from University of Baghdad, Iraq in 2002. During 2003-2007, he worked as a researcher at Ministry of Science and Technology. He received his Masters degree in Information Technology from Northern University of Malaysia (Universiti Utara Malaysia) in 2009. Currently he is doing his PhD at Northern University of Malaysia. His current research interest is on Internet Worm Detection, he published a number of papers in national and international conferences.

Dr. Norita Md Norwawi is an Associate Professor at Northern University of Malaysia (Universiti Utara Malaysia). She obtained her Bachelor in Computer Science in 1987 from the University of New South Wales, Australia. She received her Masters degree in Computer Science from National University of Malaysia in 1994. In 2004 she obtained her PhD specializing in Temporal Data Mining from Northern University of Malaysia. As an academician, her research interests include artificial intelligence, multi-agent system, temporal data mining, text mining and knowledge mining. Her works have been published in international conferences, journals and won awards on research and innovation competition in national and international level.

Dr. Osman Ghazali is a Senior Lecturer in the Department of Computer Science for Postgraduate Studies, Northern University of Malaysia (Universiti Utara Malaysia). He received his BIT, Master and PhD in Information Technology from Northern University of Malaysia in 1994, 1996, and 2008. He published a number of papers in international conferences.

Mohammed M. Kadhum is a Lecturer in the Department of Computer Science for Postgraduate Studies, Northern University of Malaysia (Universiti Utara Malaysia). He is currently pursuing his PhD in computer networking. His current research interest is on Internet Congestion. He has been awarded with several medals for his outstanding projects. His professional activity includes being positioned as Technical Program Chair for International Conference on Network Applications, Protocols and Services 2008 (NetApps2008), which has been held successfully in the Northern University of Malaysia. So far he has published various papers including on well-known and influential international journal.

.