

Learning-based System for Detecting Abnormal Traffic and Host Control

Changwoo Nam¹, Chanyeol Park², Huhnkuk Lim², Seongjin Ahn^{3*}, Jinwook Chung¹

¹ Dept. of Electrical and Computer Engineering, Sungkyunkwan Univ., Suwon Kyonggi-do, Korea

² Korea Institute of Science and Technology Information, Daejeon, Korea

³ Dept. of Computer Education, Sungkyunkwan Univ., Seoul, Korea

Summary

Worm viruses nowadays tend not only to simply attack a host and destroy it but generate high volumes of traffic and cause network failure. This paper proposes a learning-based system for detecting abnormal traffic with a control function for individual hosts included in it for efficient protection against worm viruses and network security on a network level. The system searches, detects and learns abnormal traffic on a network level to prevent factors causing network bottleneck from affecting in advance. This paper also presents a network security management system using the ARP Spoofing attack method to efficiently control the hosts within the network.

Key words:

Network Management, Network Security, ARP spoofing, Abnormal Traffic, Worm Virus, Worm Detection

Introduction

Network losses due to worm attacks exploiting vulnerability in TCP/IP protocols or operating systems are increasing. In particular, worm viruses, which spread rapidly and broadly, are quite an important issue in network security[7][8].

Technology detecting worm viruses using scanning strategy common in all worm viruses is actively in research to prevent damage from worm viruses in a network. Major characteristics in scanning strategy used by worms include the following. In order to find a target to attack, it generates addresses randomly in a short time and attempts connection to them. In its attempts to connect to the many generated addresses, it tries to connect to addresses which are not in actual use, increasing the connection failure rate. Due to these two processes, much traffic is generated in the network by the worm[1][3].

Worm attacks are becoming more sophisticated and intelligent and tend to attack an entire network, clogging it, rather than attacking and destroying a singular host[10]. As host-level security measures are not strong enough to prepare for such attacks, security management at a network level is required[3][9].

This paper presents a method examining network connection for each host to analyze worm viruses and unknown traffic attack patterns in order to efficiently prevent worm attacks and secure the network at a network level. This method uses the IP and MAC addresses and examines the number of connected IP addresses at a unit time. If it exceeds the connection critical value, it is judged as a worm virus. By isolating the source of the worm virus, that is, the worm-infected host, the network can be protected from abnormal traffic such as the worm virus.

Isolating worm-infected hosts are done using the ARP Spoofing attack and network devices such as a switch. ARP Spoofing attacks a host by forging the IP and MAC addresses of a specific host so that it cannot make normal connections with other hosts[4]. However, the ARP Spoofing attack in this paper is used for the host security management in the network[2].

This paper proposes a learning-based system for detecting abnormal traffic in which the two functions mentioned above are modularized and a control function for each host to efficiently secure and manage the network is included.

2. Worm Virus Detection

In this paper, common characteristics of the scanning strategy in worm viruses are used to detect various worms. The scanning strategy was chosen because the attack methods of worm viruses may vary widely but most of the

* Dr. S. Ahn. is the Corresponding Author.

features in the scanning strategy are similar[8]. In order to find an IP address to attack, IP addresses are generated randomly in the scanning strategy, and this causes frequent attempts to connect to IP addresses which are not in actual use[3][8]. Another characteristic is that a large number of IP addresses are searched in a very short time for the worm to quickly spread[1][8]. Using these two characteristics, worm viruses can be detected based on the number of IP addresses that a host communicates with within a time unit.

A network traffic learning method to be utilized during normal times can be considered for a more accurate detection of worm viruses. This method periodically analyzes normal network traffic patterns, creates a database on it and learns the normal usage patterns. Such feature makes it possible for agent systems to learn in different network environments. Based on the database records, if the number of hosts trying to connect increase suddenly, it can be judged that there is a worm virus infection.

The selection of items to be analyzed is important in efficiently detecting worm viruses as the number of items is inversely proportional to the system performance but proportional to the detection success rate. This paper examines whether vulnerable ports are open or not and uses the worm's characteristic of attempting connection to many hosts in a short time. Packet analysis items are set as the destination port number and the IP addresses of the source and destination.

The worm virus count procedure is performed periodically. It analyzes every IP information stored in the database and takes a count on the same source IP address. If the number of attempted connections by the source IP address for a certain period of time exceeds the connection critical value α , the system detects that the specific host of the source IP address is infected by a worm virus.

To increase the system efficiency, an increased critical value β is applied so that if attempts to connect to the network increase suddenly, it can be detected that the host of the source IP address is infected by a worm virus. This is based on the count value of the specific source IP in the database, and even if the number of attempted connections does not exceed the connection critical value α , if the number is detected to have increased by increased critical value β times, than it is detected as a worm virus.

Figure 1 shows the worm virus detection procedure.

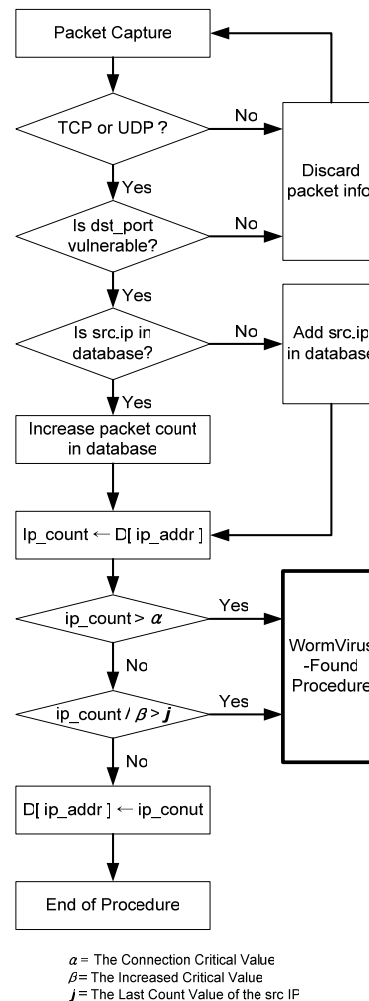


Fig. 1 Worm Virus Detection Procedure

3. Blocking Individual Hosts

The worm virus must be prevented from spreading once founded in order to minimize the damage. The administrator can consider shutting down network devices and block all traffic, but to provide the most convenience possible to general users, a method blocking only the infected hosts is applied in this paper.

In order to block individual hosts, methods applying the ARP Spoofing attack and using the access control list of a switch were researched. These two methods do not require program installment on each host, as installing an agent system on the network makes it possible to control all hosts subjected to management. However, both methods have advantages and disadvantages in their efficiency or installment environment and more research to produce a practical measure is required.

3.1 Blocking Method Using ARP Spoofing

ARP Spoofing is an attack method which sends packets containing false IP and MAC addresses to trick the target host to be attacked, and snatches the packets intended to be sent to another host. This method uses the vulnerability that ARP cache tables update without an authentication process[2][6]. When the attacker sends the host's IP address to capture and its own MAC address, the host which received the packet updates its ARP cache table. The attacked host then sends packets to the attacker according to its ARP cache table, making normal transmission and reception impossible[2][4].

Applying the ARP Spoofing attack method mentioned above, a specific user connected to the network can be blocked more efficiently. There is a difference in the purpose, as ARP Spoofing is used to snatch packets for a different host while the proposed method is for the administrator to control the network of a managed host[2]. The basic mechanism uses the same method as ARP Spoofing in sending the wrong MAC address to the IP address to be blocked.

Figure 2 shows host blocking, maintaining blocking, and releasing using ARP.

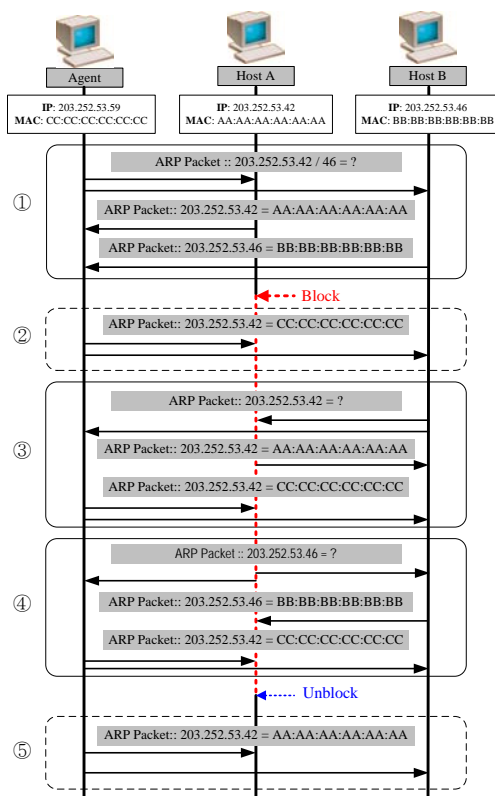


Fig. 2 Host Blocking, Maintaining Blocking, Releasing Using ARP Spoofing

- ① The agent broadcasts ARP request packets and acquires network information.
- ② The agent blocks Host A using ARP Spoofing.
- ③ The blocking may be released if unblocked Host B requests information of blocked Host A, but the agent sends ARP packets and maintains the blocking.
- ④ The blocking may be released if blocked Host A requests information of Host B, but the agent sends ARP packets and maintains the blocking.
- ⑤ When releasing the blocking of Host A, the agent broadcasts ARP packets with the correct information and releases Host A.

3.2 Blocking Using a Switch's Access Control List

The ARP Spoofing attack method can be applied to any network environment, but has the disadvantage that it cannot prevent the performance degradation of other network communications even if excessive traffic is generated during an abnormal operation of a specific host. Another method that can be considered is to interrupt traffic transmission within the network device itself. If a switch or router interrupts the traffic transmission of a specific IP or MAC address, damage to other hosts can be minimized while blocking the worm-infected host.

The system in this paper uses a method controlling the access control list of a switch to block worm viruses. The administrator does not propose the switch device but enters the command list to the system in advance, and when a worm virus is detected, the command is executed automatically. In order to implement such function, the agent system is connected to port 23 of the switch device and the manager sends packets as if entering a command through telnet. The command entered beforehand is sent to the switch when releasing the blocking of an infected host, automatically controlling the switch's access control list.

```

Quarantine command using ACL
conf t
mac access-list extended FILTER
deny host "quarantine MAC address" any
permit any any
exit
interface f0/24
mac access-group FILTER in

Un-quarantine command using ACL
conf t
no mac access-list extended FILTER
exit
    
```

Fig. 3 Telnet Command

Telnet commands used in this paper are shown as the above. Using Cisco Catalyst 2950 was considered in this research, but even when using a different system, if entering commands manually in the manager GUI, they can be modified according to the managing network[11].

4. System Implementation

4.1 System Structure

The system consists of an agent system to be installed in each broadcast domain and a manager system. The agent system captures packets, generates ARP packets, and performs worm virus detection in a Linux environment. The system is separated into agent and manager to efficiently manage the network and detect abnormal traffic, and such formation distributes the system load, enhancing efficiency. The overall system operates with the manager administrating the agent in each network. The manager instructs the management policies to the agent, and the agent performs them. One agent can exist in each network's ARP broadcasting domain, and manages the specific broadcasting domain.

The first agent to be created in the network is registered in the manager system by the administrator, and at the same time, the agent collects its network information. Network information collecting is done for a certain period of time, and this is to minimize packets to be generated due to the information collection in the network. The agent sends the information collected through network monitoring to the manager and waits for the manager to instruct a policy. The manager can monitor the information in its managed network at real-time, and these information are recorded in the database and are used to instruct a command to the agent or record network details.

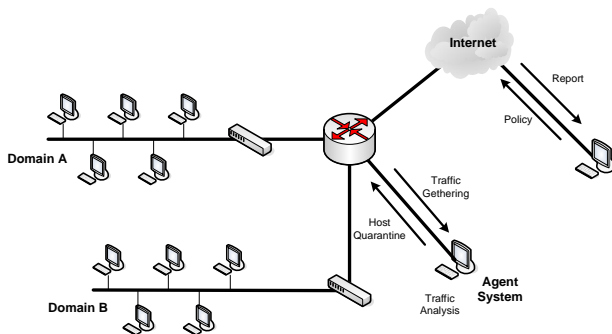


Fig. 4 System Configuration Environment

4.2 Manager System

The system consists of an agent system to be installed in each broadcast domain and a manager system. The agent system captures packets, generates ARP packets, and performs worm virus detection in a Linux environment.

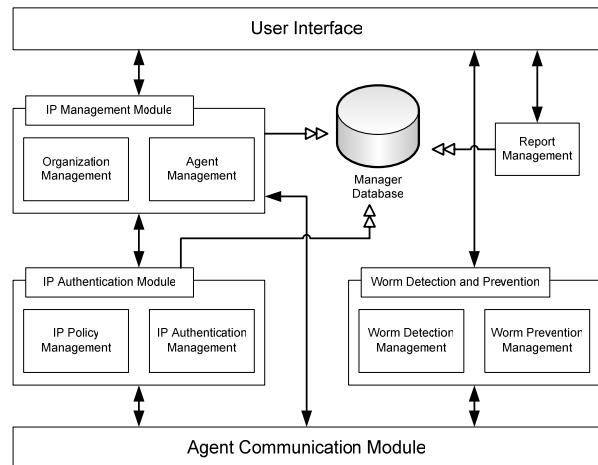


Fig. 5 Manager System Module Diagram

The manager system receives the network information collected by distributed agent systems and IP address, and has a centralized IP address managing function. Major features include management of in-use/unused IP addresses, policy setting based on the IP address and worm virus detection and blocking.

4.3 Agent System

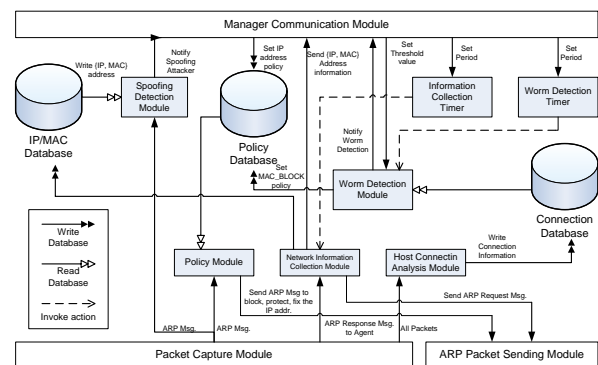


Fig. 6 Agent System Module Diagram

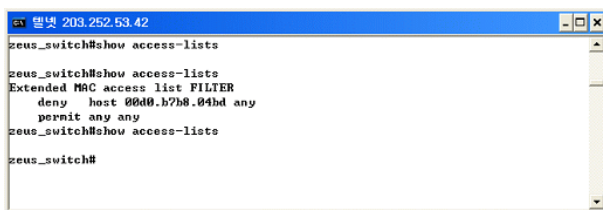
The agent system is installed in each ARP broadcasting domain. It collects the network's resource information and IP address and notifies them to the manager system, and controls the IP address according to the manager system's policy[5][6]. The agent also executes its worm virus detection and blocking function, preventing further

spreading of the worm virus. The system is modularized by functions, and is divided into a packet monitoring module, packet generating module and learning and detecting module.

The agent system is installed in each broadcasting domain and has functions for packet monitoring, packet generating, learning and detecting worm viruses. Major functions include packet analyzing and database recording, blocking unauthenticated IP/MAC users and detecting and learning worm viruses.

4.4 Switch Control

When a worm virus is detected, the agent system shows the IP address of the worm-infected host and detection method to the manager system. The agent system connects to the switch by telnet and controls so that the infected host cannot pass through the switch. When releasing the worm's blocking, it connects to the switch again to release the blocking setting. Figure 8 shows that there is nothing in the access lists at first, but when a worm is detected, the access lists are made in the switch, and removed when the blocking is released.



```

명넷 203.252.53.42
zeus_switch#show access-lists
zeus_switch#show access-lists
Extended MAC access list FILTER
deny host 00d0.b7b8.04hd any
permit any any
zeus_switch#show access-lists
zeus_switch#

```

Fig. 7 Switch Control Results

5. Conclusion

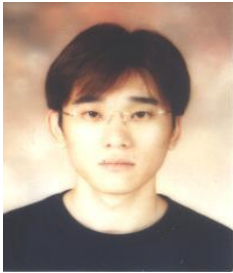
This paper researched into a learning-based system for detecting abnormal traffic which can protect the network from worm viruses and various attacks. A learning-based system detects Worm viruses based on traffic monitoring, and examines only packets attempting connection to vulnerable ports to increase the accuracy with the least cost for analyzing. The number of connections at each host was examined periodically to analyze abnormal operation, and previous data were utilized for accurate measurement, which made it possible to include a method learning the normal usage patterns. However, more testing is required for setting the critical value, and the number of packets to capture increase as the number of managed hosts increase, which may cause problems to the performance of the agent system.

The system in this paper is based on the common characteristics of a worm virus, giving it the advantage to

cope with mutated viruses and future viruses. A network management system can be developed based on this system using the SNMP MIB value of network devices. Adding a network traffic analysis factor, a traffic analyzing program can be made. In order to enhance this research, traffic sampling methods should be applied for a more flexible approach to the analysis items. Last, establishing an integrated security system in cooperation with a blocking method using the switch's access control list and previous intrusion prevention systems can be considered.

References

- [1] Guofei Gu, Monirul Sharif, Xinzhou Qin, David Dagon, Wenke Lee and George Riley, Worm Detection Early Warning and Response Based on Local Victim Information, Computer Security Applications Conference, 2004. 20th Annual
- [2] K. Kwon, s. Ahn, and J. Chung, Network Security Management using ARP Spoofing, Lecture Notes in Computer Science Springer-Verlag Vol.3043, 2004
- [3] Vincent Berk, George Bakos and Robert Morris, Designing a Framework for Active Worm Detection on Global Networks, Preceeding on IWIA'03, 2003
- [4] S. Whalen. An Introduction to ARP Spoofing. http://packetstorm.securify.com/papers/protocols/intro_to_a_rp_spoofing.pdf june 2001
- [5] Behrouz A.Forouzan, TCP/IP protocol Suite, McGrawHill, 2006
- [6] Behrouz A.Forouzan, TCP/IP protocol Suite, McGrawHill, 2006
- [7] N. Weaver, V. Paxson, S. Dataniford, and R. Cunningham. A taxonomy of computer worms. In proceedings of ACM CCS Workshop on Rapid Malcode (WORM'03), Octobr 2003
- [8] C. C. Zou, D. Towsley, and Gong, On the performance of Internet worm scanning strategies, J. Performance Evaluation, 2005.
- [9] Jason C. Hung, Kuan-Cheng Lin, Anthony Y. Chang, Nigel H. Lin and Louis H. Lin, A Behavior-based Anti-Worm System, Preceeding on AINA' 03, China, 2003
- [10] X. Qin, D. Dagon, G. Gu, W. Lee, M. Qarfield, and P. Allor. Worm detection using local networks. The recent Advances of Intrusion Detection TAID'04, September 2004.
- [11] Cisco Catalyst 2950 Datasheet http://www.cisco.com/global/KR/products/pc/switches/2950/ds_index.shtml



Changwoo Nam received the B.S. degrees in Electronic Engineering from Kyonggi University in 2006. He is currently working towards the M.S. degree in Electrical and Computer Engineering with the school of Electrical and Computer Engineering, Sungkyunkwan University, Korea. His research interests include network management, network security, wireless network, embedded system.



Chanyeol Park received the B.S. degree in Mathematics and the M.S. and Ph.D. degrees in Computer Science from Korea University in 1993, 1995 and 2000 respectively. He is currently a senior research worker at Korea Institute of Science and Technology Information, Korea. His research interests include P2P Computing, Mobile Agent, Web Services, Check pointing and Rollback Recovery.



Huhnkuk Lim received the B.S. degrees in Electrical Engineering from Hankuk Aviation University and M.S. and Ph.D. degrees in Information & Communication Engineering from Gwangju Institute of Science and Technology in 1999, 2001 and 2006 respectively. He is currently a senior research worker at Korea Institute of Science and Technology Information. His research interests include Optical Network, Optical Packet/Burst Switching, Data/Control Plane Design for R&D Networks G-MPLS Protocol.



Seongjin Ahn received the B.S., M.S. and Ph.D. degree in information and communication engineering from Sungkyunkwan University, Korea in 1988, 1990 and 1998, respectively. For more than five years, he was a Researcher in Electronics and Telecommunications Research institute (ETRI), Korea. He is currently an assistant professor department of computer education, Sungkyunkwan University, Korea. His research interests include network management, network security, and information assurance.



Jinwook Chung received the B.S. and M.S. degree in electric engineering from Sungkyunkwan University, Korea in 1974, 1977, respectively, and the Ph.D. degree in computer science from Seoul National University, Korea, in 1991. For more than ten years, he was a section chief in Electronics and Telecommunications Research institute (ETRI), Korea, since 1984 he has been a professor of the school of Information and Communication Engineering, Sungkyunkwan University, Korea. In 2002 he served as President of the Korea Information Processing Society (KIPS). His research interests include data communications, computer networks, network management, and network security. He has guided more than 150 M.S./Ph.D. students in this area of study and has published more than 100 papers in technical journals and conference proceedings.