# Designing of a Abnormal Traffic Distinction and Host Control System in the IPv6 Environment

*Changwoo Nam[1],Seunghae Kim[2], Kwangsub Go[2], Joobum Kim[2], Seongjin Ahn[3]*, Jinwook Chung[1]*

[1] Dept. of Electrical and Computer Engineering, Sungkyunkwan Univ., Suwon Kyounggi-do, Korea
[2] Korea Institute of Science and Technology Information, Daejeon, Korea
[3] Dept. of Computer Education, Sungkyunkwan Univ., Seoul, Korea

**Summary**
Even in IPv6, of which the security is enhanced relative to existing IPv4, the entire network security is under critical threats from unauthorized or malicious users and the worm virus scanning process possible in IPv6 is a menace to the IPv6 network. Thus, this research paper proposes an integrated IPv6 network management system that detects and blocks worm viruses that cause network disabilities and isolate authorized or malicious users from the network while enhancing the efficiency of network management.

***Key words:***
*Network Management, Network Security, Ipv6, Abnormal Traffic, Worm Virus, Worm Detection*

## 1. Introduction

As the scale of modern day networks expanding, network administrators of firms, research institutes, and schools are spending more and more time and money on network address (IP/MAC) managements with no great efficiency. In addition, illegal network address usages by unauthorized personnel are causing network address collisions, network failures, and security issues. The severity of such network management and security issues are not only presented in the current IPv4 networks, but also in the next generation IPv6 networks which are in occasion evaluated as some critical problems. This is because the same spoofing and sniffing attacks can technically be applied also on IPv6 systems[3][5].

In additions, instances where worm viruses damage the network by abusing the weak points of operating systems or the TCP/IP protocol is constantly increasing along with the development of network security technologies [1]. Although the security of IPv6 has been improved, new attack methods that aim at attacking the blind spots of the protocol are being developed and they are a lethal threat to us [2]. Therefore, an integrated measure that can isolate worm viruses that threat the network security by generating a substantial amount of traffic in the network thereby preventing from unnecessary network performance depreciation while improving the stability and credibility of the network and system through real-time platform technology research that can protect the network resources of major network devices or server hosts is required.

Thus, in order for an efficient management of the real-time IPv6 network resources and the blocking of worm viruses, this research would like to design a system that can detect and block worm viruses and provide network resources management and access control functions based on the status monitoring of the IP and MAC addresses that are used in the network in the Link-Local unit. This prevents users from tentatively or maliciously changing the network devices in use or the IP address or network interface card of the server host and by blocking worm viruses, it can prevent network performance depreciation by unnecessary traffic and also the spread of worm viruses [8]. Furthermore, the network can be more efficiently managed and prompt recovery is possible in case of a network trouble.

## 2. Worm Virus Detection Method

In this paper, common characteristics of the scanning strategy in worm viruses are used to detect various worms.

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[2][7].

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

Manuscript received August 5, 2007
Manuscript revised August 20, 2007

As mentioned previously, worm viruses randomly generate IP addresses in order to find the IP address of the victim and it consequently increases the number of connection failure because it attempts to connect to IP addresses that do not even exist [4][9]. Also, worm viruses search for a large number of IPs in a short period of time for a quicker transmission. Using such unique characteristics, the host can detect worm viruses that are based on the number of IP addresses communicated within the time unit. The usual network traffic learning technique can be considered in increasing the accuracy of worm virus detection. This can be realized by periodically analyzing usual network traffics and forming this into a database. By allowing the system to become suitable to different network environments, it can determine if a worm virus is detected when the number of connected hosts increases significantly when compared to the usual.

Also, for more efficient worm virus detection, appropriate analysis categories must be selected because the analysis category is also a crucial element and also because the number of categories is inversely proportional to the system performance while being directly proportional to the detection success rate. Thus, this research used the property of worm viruses that attempts many connections in a short amount of time and the investigation of whether a vulnerable port is open to determine as the packet analysis category the destination port number and the sending/receiving IP address.

```
V ← Vulnerable Port List, D ← Connection Count Database
α ← Threshold Value(absolute), β ← Threshold Value(relative)
PD ← Previous Connection Database

Packet-Count-Procedure
  Packet ← New Captured Packet
  IF ( (packet.protocol!= TCP) and (packet.protocol!= UDP) and
(packet.protocol!=SCTP)
     then Discard packet.
  ELSE IF ( packet.dst_port ∉ V)
     THEN Discard packet.
  ELSE IF ( packet.src_ip ∉ D[packet.src_ip] )
     THEN add packet.src_ip in D[packet.src_ip]
  ELSE increase ip_count in D[packet.crs_ip]
  END OF IF

end of Procedure

Periodically Called,
Worm-Detection-Procedure
  FOR ip_addr ← D.start_ip to D.end_ip
     ip_count ← count IP address in D[ip_addr]
     IF ( ip_count > α )
        Call WormVirus-Found-Procedure
     ELSE IF ( ip_count / β > PD [ip_count] )
        Call WormVirus-Found-Procedure
     ELSE PD [ip_addr] ← ip_count
     END IF
  END FOR
end of Procedure
```

Fig. 1 Worm Virus Detection Algorithm

The worm virus detection algorithm is largely broken down into the Packet Count Procedure and the Worm Detection Procedure and they are processed as follows.

① In the Packet count procedure, only the packets that use transport layer protocols such as TCP, UDP, and SCTP are accepted as the rest are discarded.
② Check if the packet's destination port is the predefined vulnerable port. If it's not a vulnerable port, discard the particular packet.
③ If the packet's destination address exists in the database, increment ip_count and add the IP address information otherwise.
④ The Worm detection procedure is periodically executed and it reads in the IP address information from the database.
⑤ If the IP address information count value obtained from the database is greater than the critical value $\alpha$, it is considered a worm virus.
⑥ When applying the increment critical value $\beta$ for enhancing the efficiency and if the connection value has become $\beta$ times the previous value, it is considered a worm virus.

## 3. Network Access Control Method

The general host and agent making up a network each have one network interface card of which each card has one fixed interface ID. When a host in an IPv6 network receives a unicast address through automatic address creation and duplicate address detection processing the host will be granted access to the network. Therefore, it is necessary to acquire a method that manages address authentications to control network access.

The network access control of the IPv6 host is executed in procedures of collecting network resource information, blocking network entrance, isolation of the IP address in use from the network, and policy upkeep on continuous reuse attempts. Unauthorized users must reexamine their initial IP to use through an ICMPv6 message in order to access the network. The access control system here checks whether the user is authorized based on the policies stored per Link-Local Scope and sends an ICMPv6 response message in cases of when the user is unauthorized which eventually prevents that user from using the network address.

### 3.1 Network Information Gathering

To operate the access control system of a universal network resource, it is vital to be aware of the information on the available resources in the Link-Local Scope. To collect the available resources, monitoring period on the network information on initial system operation is required and this time is identical to the time out period of neighbor unreachability detection of the default gateway router.

There are two meanings when the information collecting period of network resources equals the time out period of neighbor unreachability detection. First, every IPv6 hosts existing in the Link-Local Scope within the time out period of neighbor unreachability detection must send at least one packet to the network. The IPv6 host keeps the IPv6 neighbor entry cache in its memory. The neighbor nodes registered in this neighbor entry cache refreshes the information in the neighbor entry cache when packets are received that sets the corresponding address as the sender. If packets that set the corresponding addresses as the sender are not received during the time out period of neighbor unreachability detection, the corresponding node is deleted from the neighbor entry cache. Second, the identical neighbor entry cache with other IPv6 hosts in the Link-Local Scope can be maintained.

## 3.2 Network Intrusion and IP Blocking

The host using an IPv6 address must go through a duplicate address search procedures. This process is undergone in cases of receiving IPv6 address resources through manual address creation or automatic address allocation or also in cases of receiving IPv6 address resources through automatic creation due to address allocation. Hosts that wish to receive an IPv6 address must use neighbor request messages in their own solicited-node multicast address through an ICMPv6 message and then request for a 2 layer address. When there is a 2 layer request on the unauthorized host, the access control system creates and sends a response through a neighbor notification message to hide the fact that the corresponding IP resource is in use. If a duplicate address is found, the corresponding address cannot be allocated to the network interface.

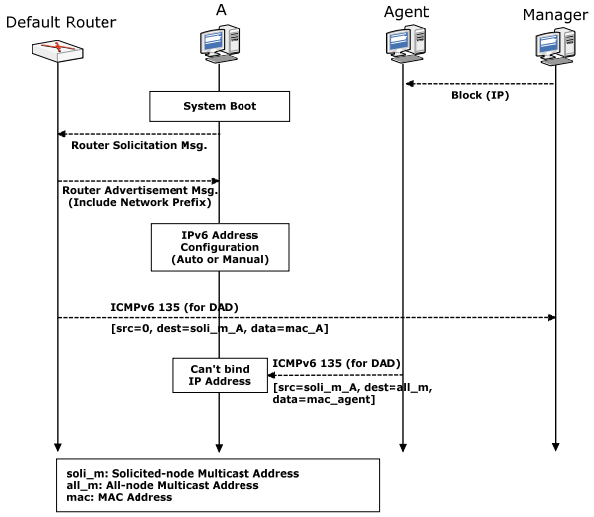



Fig. 2 Unauthorized IP addresses blocking process

Isolation of the IP resource in current use from the network requires methods other than binding it with the network interface through duplicate addresses. A method to handle neighbor request messages and path redirection messages is used in such cases.

The method to handle neighbor request messages is used to prevent authorized hosts from sending packets to hosts to isolate. Firstly, set the IPv6 address to isolate from the network as a 3 layer sender address and then create a neighbor request message with an address of other hosts located in the Link-Local Scope like the isolation subject host B. The data in this packet holds random 2 layer addresses and such packets are sent to the network. External hosts located within the Link-Local Scope alike the host subject for isolation has 2 layer addresses that holds data of packets that are created and sent by the agent at their neighbor entry cache and therefore these two random 2 layer addresses are used to send packets through the IP resource subject for isolation. In this case, the 2 layer address subject for address change request does not exist in the actual network or is the 2 layer address of the agent which prevents all hosts within the network affiliated to host B that is subject for isolation from sending packets to host B.

The handling method of path redirection messages is used to make the host targeted for isolation to misrecognize the next hop for packet transfer. This prevents the IPv6 terminal subjected for isolation from sending packets within the network by targeting the IP resource for isolation and setting the wrong data for the next hop address.

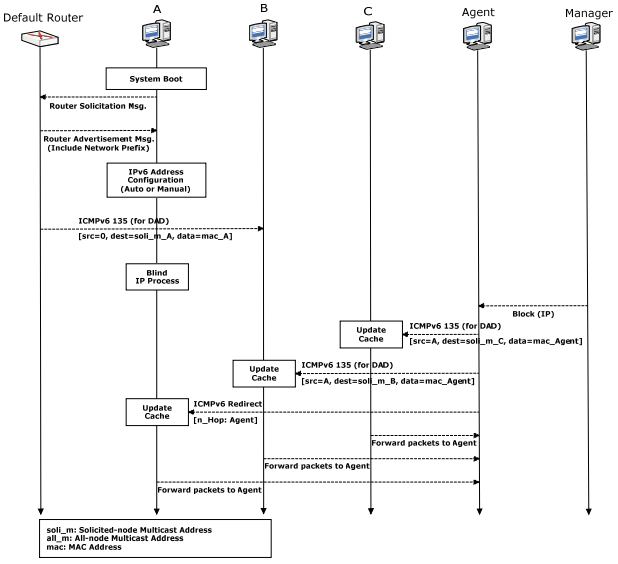



Fig. 3 IP address isolation process

## 4. Distinction of Abnormal Traffic and Host Control System

The system is largely divided into agents that are installed in each Link-Local Scope unit network and a manager that manages these agents. The agents capture packets in the LINUX environment and generate manipulated packets to detect worm viruses.

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. An agent is present in each Link-Local Scope unit network and it manages the network of the corresponding Link-Local Scope unit network.

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.

### 4.1 Agent System

An agent system is installed in each Link-Local Scope unit network to collect the network's resources information and IP addresses to report to the control system and it controls the IP addresses according to the policy of the control system. Also, it detects and blocks worm viruses to prevent the spread of worm viruses.

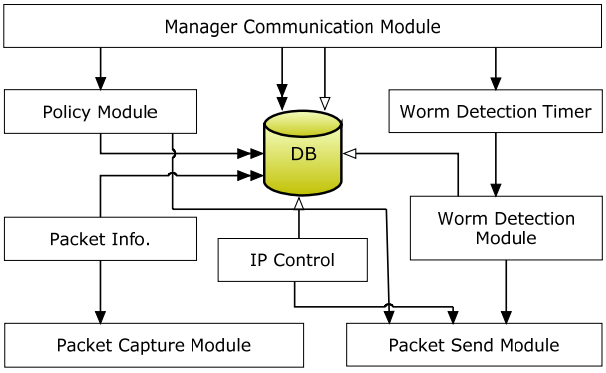



Fig. 4 Agent Module Diagram

An agent system is made into a module by each function and some examples of functions are packet analysis and database recording, specific IP and unauthorized IP blocking, and worm virus identification.

### 4.2 Manager System

The manager system receives the network information and IP addresses collected by the scattered agent systems to establish a critical value and policy of the worm virus detection function and the centralized IP address management function. Examples of these functions are used/unused IP address management, policy configuration by IP address, worm virus detection, and blocking function.

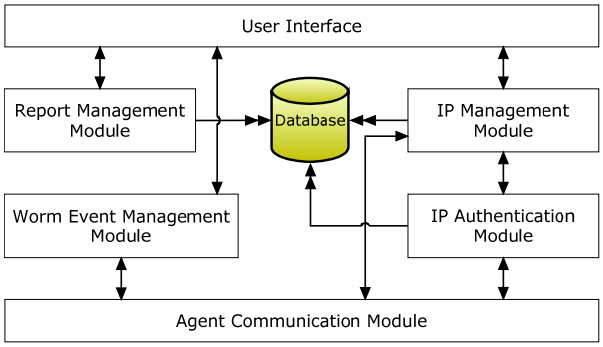



Fig. 5 Manager Module Diagram

## 5. Conclusion

This research paper designed a system that blocks worms viruses that damages the network and a function that prevents unauthorized users who are in use of the network from attempting to get IPv6 resource allocation or utilizing the already-allocated resources by using functions managed by ICMP and ARP of IPv4 such as network address configuration, repetitive address search, address change between classes, and path redirection to continuously use the network system.

Abnormal traffic distinction and host control system by IPv6 address control requires a more sophisticated form of functions compared to those of IPv4 due to the enhancement of IPv6's address management and it inevitably consumes more system and network resources. However, the abnormal traffic distinction and host control system proposed in this research can run with only the Link-Local Scope unit agent depending on the network system's security policy and the presence of security-

threatening users without any additional protocols or network devices.

However, the system will become overloaded when generating packets and sending to all hosts except those that are subject to isolation or to all hosts in the Link-Local system and therefore further researches on the critical value configuration for more accurate worm virus detection is required. Also, the system performance may experience difficulties because the number of packets to gather increases as the number of hosts in the Link-Local Scope unit network increases. Lastly, the lack of broadcast-type packet delivery method that leads to performance issues as state above can be improved and therefore will be considered in prospective researches.

## 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] Steven M. Bellovin, Bill Cheswick, Angelos D. Keromytis, Worm Propagation Strategies in an IPv6 Internet, Login Vol.31 No.1, 2006

[3] K. Kwon, s. Ahn, and J. Chung, Network Security Management using ARP Spoofing, Lecture Notes in Computer Science Springer-Verlag Vol.3043, 2004

[4] Vincent Berk, George Bakos and Robert Morris, Designing a Framework for Active Worm Detection on Global Networks, Preceeding on IWIA'03, 2003

[5] S. Whalen. An Introduction to ARP Spoofing. http://packetstorm.securify.com/papers/protocols/intro_to_arp_spoofing.pdf june 2001

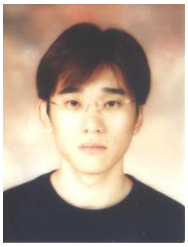
[6] Behrouz A.Forouzan, TCP/IP protocol Suite, McGrawHill, 2006

[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), Octobrt 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] W.Richard Steavens, TCP/IP Illustrated, Volume 1 The Protocol, Addision-Wesley, 1999

**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 Electical and Computer Engineering, Sungkyunkwan University, Korea. His research interests include network management, network security, wireless network and, embedded system.

**Seunghae Kim** received the B.S. degree in Info. & Comm. From Hannam University and the M.S. and Ph.D. degrees in Information Science from Chonbuk University in 1997, 2003 and 2006 respectively. He is currently a senior research worker at Korea Institute of Science and Technology Information, Korea.

**Kwangsub Go** received the M.S. degrees in Information & Communication from Soongsil University in 1999 respectively. He is currently a senior research worker at Korea Institute of Science and Technology Information

**Joobum Kim** received the B.S. degree in Electronic and Communication Engineering From Kwangwoon University and the M.S. degrees in Information & Communication Engineering from Gwangju Institute of Science and Technology in 1999 and 2002 respectively. He was a senior research worker in Samsung Electronics. He is currently a research worker at Korea Institute of Science and Technology Information, Korea.

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 then 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.