인터넷 주소 충돌 감지에 관한 연구

위선정 · 임영희 · 이태헌 · 박기홍

A Study of Internet Address Collision Detection Method

Seon-jung Wi* · Yeng-hee Lim* · Tae-hun Lee* · Ki-hong Park*

요 약

현재 개인용 컴퓨터의 수는 기하급수적으로 늘어나면서 일반 개인들은 ip에 대한 특별한 지식 없이 isp업체에서 제공하는 유동아이피를 사용하고 있다. 하지만 고정아이피를 사용하는 학교나 회사의 경우 일반 사용자의 대부분은 TCP/IP 주소에 대한 지식이 없기 때문에 고의 또는 실수로 자신의 것이 아닌 다른 사용자의 TCP/IP주소를 사용하여 네트워크 전체를 마비시키며, 원래 사용자가 네트워크를 사용할 수 없게 만든다. 이에 본 논문에서는 사전에 네트워크 관리자가 망 내부의 관리 대상 개인 컴퓨터와 네트워크 시스템들의 주소 정보를 데이터베이스화한 뒤 현재 사용하는 주소 정보가 저장된 정보와 같은 지를 웹을 통해 패킷을 검출하고, 잘못된 TCP/IP 주소의 사용을 사용자에게 통보하여 고의나 실수에 의한 IP주소 변경에 따른 네트워크 시스템의 마비를 막을 수 있는 방법을 제시 하고자 한다.

ABSTRACT

Currently possibility of the change of seal computer it increases geometrical progression and the general individuals the knowledge which is special regarding the ip are using the flow child blood which it provides without from the isp enterprise. But most of the case peon of the school which uses the fixation child blood or the company because is not the knowledge against a TCP/IP address is not oneself at deliberation or real income and it will use the TCP/IP address of the different user and the network whole it will paralyze, the original user will not be able to use the network and it makes. With information where address information where the network administrator present time after data base anger one uses address information of the civil official objective personal computers and network systems of the watch inside in the dictionary is stored will be same from the dissertation which it sees hereupon and the web which it will yell it leads and packet it detects, the use of the TCP/IP address which goes wrong in the user and it notifies the method which is the possibility of closing the paralysis of the network system which it follows in the IP address fringe land due to a deliberation or a real income to sleep it presents it does.

Ⅰ. 서 론

1. 연구의 필요성 및 목적

본 연구 논문은 지역 망(학내 망)에서 관리자가 User에게 할당한 IP Address를 실수 또는 불법으로 다른 사용자가 사용하게 되면 정식 사용자는 Network를 사용하지 못하게 될 것이다. 그 이유는 IP Address 는 전 세계에서 유일하게 사용되기 때문이며, 하나의 IP Address를 두 사람이 사용하게 되면 먼저 Network에 접속한 사람은 사용할 수 있으나, 이후에 동일한 IP Address를 f가지고 접속하게 되면 IP Address의 충돌로 인하여 사용할 수 없기 때문이다.

많은 사용자가 있을 경우에 하나의 충돌하는 IP Address를 찾는다는 것은 어렵다. NMS(Network Management System)가 있으나 해결방법이 전무하였고, 충돌한다는 메시지를 시스템에 따라서 보여주기는 하나 그것을 해결할 방법은 없었다.

이상과 같은 문제로 인하여 본 연구 논문에서는 Network 관리자의 입장에서 정식으로 사용하는 User에게 안전한 Network의 사용을 제공하기 위하여 충돌하는 IP Address를 DNS(Domain Name Service) Server와 router 상에서 Packet에는 출발지 주소와 목적지 주소가 존재한다. 이때 패킷을 filtering gi여 NIC(Network Interface Card)의 MAC Address 와 IP Address를 검출, 실수 또는 불법으로 사용하는 사용자를 정식의 사용자에게 IP Address를 돌려주기 위하여 연구하게 되었으며, 첫 번째로 실수 또는 고의로 사용하는 사용자가 TELNET으로 DNS(Domain Name Service) Server에 접속하여 서비스를 이용하게 되면, "충돌

하는 IP Address입니다." 라는 메시지를 보여주고 일정한 시간이 지난 뒤 접속을 끊게 하여 준다.

본 논문의 구성은 서론에서의 연구의 필요성 및 목적과 관련연구에서의 각 NMS, SNMP, CMIP, RMON과 TCP/IP프로토콜에 대한 설명 부문과 본 논문의 실제적인 시스템 설계, 구현 마지막으로 평가로 나누어져 있다.

본 논문의 결론으로는 단일네트워크상에서의 IP Address 충돌을 MAC Address로 찾아내어 인증하지 않은 Address의 사용자에게 경고메시지를 보내어 충돌에 대한 서비스 중단을 막아 보고자 하는 것에 의미를 두고자 한다.

II. 시스템 설계

1. 시스템의 기본 방향

본 시스템은 지역 망 내에서 운용되는 컴퓨터들의 IP Address와 MAC Address에 대한 정보를 데이터 파일로 작성한 후 이에 맞지 않는 주소 정보를 사용하는 컴퓨터에 대하여 사용자에게 올바른 주소 정보를 제공함으로써 지역 망 내에서의 IP 주소 충돌에 대한 해결책을 제시하려 한다. 관리자는 사용자에게 메시지 전송과 연결 종료를 선택적으로 실행 할 수 있다.

2. 시스템의 구성

본 시스템은 크게 다섯 가지 큰 줄기로 나눌 수 있다. 이것은 주 메뉴의 메뉴들과도 일맥상통한다. 각각은 독립적인 하나의 메뉴로 되어 있으므로 필요한 부분을 실행 할 수 있다. 메뉴의 종류 및 기능은 다음과 같다.

첫째, 지역 망 내에 있는 관리 대상 컴퓨터들의 IP 주소와 MAC 주소를 데이터 파일로 생성, 관리하는 부분이다. 여기서는 임의의 주소에 대한 검색과 삭제, 새로운 주소 정보의 입력 등이 이루어진다. 둘째, 지역 망 내에 떠도는 패킷들의 주소 정보를 추출하는 부분이 있다. 이는 임의의 시간에 서버가 추출하며 24시간 계속 적으로 실행 될 수 는 없다. 이 정보를 기초로 하여 모든 프로그램이 실행된다. 셋째, 검색한 패킷의 주소 정보와 데이터로 저장되어 있는 정보와의 비교하는 부분, 이 곳에서 잘못된 주소를 사용하는 사용자의 존재 여부를 판단해 낸다. 넷째, 서버에 접속한 사용자 정보를 추출하는 부분이다. 이 부분은 잘못된 IP 주소를 사용하는 사용자에 대하여 관리자가 메시지를 보내기 위한 정보를 얻게 한다. 마지막으로, 잘못된 사용자의 접속을 종료하는 부분이다. 이 부분은 사용자에게 불이익을 줌으로써 문제해결을 유도한다.

III. 구 현

1. 설계 및 구현

1.1. 설계

1) 착안점.

설계에 있어서 우리가 알아야 할 것은 지금 사용 중인 Personal Computer는 사용자가 일부로 이든 실수이든 자신의 IP Address를 바꾸는 것에 아무런 제약이 없다. 또한, 자신의 IP Address가 아닌 것을 사용해도 통신이 가능하며, IP Address의 소유에 관한 제약이 없다. 이를 해결하려는 것이 본 연구의 목표이다.

1.2. 구현.

1) Data 파일 관리.(Address Management)

Mac Address와 IP Address, 사용자 정보에 대한 자료 처리는 추가, 삭제, 검색, 삭제 표시된 자료삭제의 Sub Menu가 있다. 자료의 변경은 Programming 하지 않았으므로 직접 Data 파일에서 처리해야 한다.

2) IP Address 정보 수집. (Catch Packet Information)

IP Address에 대한 정보 수집은 snoop v arp 명령어의 결과를 File에 저장하는 방법을 이용하였다. 참고로 snoop는 Packet의 정보를 보여 주며 이 정보 안에는 sender의 IP Address 와 Mac Address에 대한 자료가 있다. 여기서는 arp packet만을 수집하도록 하였다.

1번 Catch Packer Information을 수행하면 상기한 내용의 정보가 sample.dat 파일에서 우리가 필요로 하는 정보인 IP Address와 Mac Address만을 추출하여 기록하여 진다. 또한 snoop command는 같은 Address를 여러 번 수집하기도 하므로 program에서 중복된 Address를 삭제하는 routine이 추가되어 있다. 이 routine으로 인해서 temp.dat 파일이 생성 된다.

3) 충돌 검색. (View Collision)

IP Address의 충돌의 검색은 address.dat 파일과 out.dat파일을 비교함으로써 이루어진다. 상기한 내용처럼 address.dat 파일에는 등록된 IP Address 정보가 기록되어 있고, out.dat 파일에는 지금 사용중인 IP Address가 기록되어 있다. Program은 address.dat를 out.dat에 기록된 Mac Address를 가지고 탐색하여 지금 사용 중인 PC의 IP Address가 올바른 것인지를 검사한다. 만일 올바른 것이라면, 다음의 주소를 검색하고 모두 검색이 끝난 후 결과를 화면과 report.dat로 출력한다.

report.dat 파일에는 두개의 IP Address가 기록되는데 이는 잘못된 IP Address와 등록된 IP Address가 순서대로 기록되어 있다. 화면에 출력되는 내용으로는 잘못된 주소정보의 Mac Address에 대한 IP Address, 학과, 연락처가 출력된다.

4) 사용자 메시지 전송. (Send Message for Connector)

우선 현재 server에 접속한 사용자의 정보를 수집하여 who.txt 파일에 기록하고, who.txt 파일에

서 IP Address와 User ID를 추출하여 who_r.txt 파일에서 IP Address와 비교한다. 이때 동일한 IP Address로 접속한 사용자가 존재한다면, 잘못된 IP Address임을 알리는 메시지와 원래의 IP Address를 전송하여 주고, 접속 종료를 위해 user.dat에 해당 IP Address를 기록한다.

5) 메시지 전송 후 강제 접속 종료

user.dat에 기록된 IP Address를 사용하는 User의 PID를 shell Program으로 검출하여 Kill 시킴으로써 접속을 강제 종료시킨다.

IV. 평 가

1. Program의 효과

본 연구는 실제 User들의 입장에서 IP Address의 충돌에 의해 통신을 할 수 없다는 것은 무시할 수 없는 불편함이라는 것을 생각할 때 이에 대한 해결책이 필요하다고 하겠다.

Packet이 Router를 벗어나지 않는 같은 Router의 범위 내에서 충돌 여부를 밝혔으며, Router 밖의 Packet은 그 Packet이 속해 있는 그룹에서 판달할 문제로 남겼다.

IP Address를 도용한다고 해도 다른 그룹의 IP Address 는 사용할 수 없다.

네트워크 관리자는 IP Address에 대한 관리를 통해 사용자의 편의와 IP 도용에 따른 보안에 이르기까지 관리를 해야 한다. 또한 이로 인해 사용자 편의 등도 무시해서는 안 될 것이다. 그래서 본 연구에서는 IP Address의 충돌에 대하여 충돌을 발생시킨 컴퓨터가 어느 것인지 Mac Address에 의해 알아냄으로써 해결의 실마리를 찾고, 그 Computer를 사용하는 User에게 올바른 IP Address를 알려줌으로써 해결할 수 있도록 하였다. 고의적인 IP Address 도용에 대한 해결책으로는 Server에 접속한 사용자에게 Message 전송 후 연결을 강제로 종료함으로써 대응하도록 하였다.

2. Program의 한계.

본 연구의 한계성은 다음과 같은 것이 있다.

첫째, 서론에서 언급한 대로 LAN환경의 지역망 내에서 만을 고려하였다는 것.

외부에서의 사용에 대해서는 고려하지 않았다는 것이다. 이것은 라우터에서 Access List를 사용하여 커버할 수 있으리라 생각된다.

둘째, 여러 가지 통신 서비스 중 Telnet Service에 대해서만 다루었다는 것. 나머지 Service에 대해서는 차후 연구 과제로 남기려 한다.

셋째, 본 연구 결과물의 실행에 있어서의 한계는, 우선 지역 망 내의 모든 Personal Computer에 대하여 Mac Address와 할당해준 IP Address에 대한 정보를 모두 가지고 있어야 한다. 이 내용은 곧 네트워크 관리자가 모든 할당하여준 IP Address로 Mac Address를 데이터베이스화하여야 한다는 것과 일맥상통 한다. 또한, snoop에 의한 IP Address 정보 수집은 Server에 Overhead를 주므로 계속적으로 실행을 할 수가 없다. 이것은 최악의 경우 잘못된 사용자가 접속을 하여도 그 때 snoop이 실행되지 않는다면 그 사용자의 정보는 찾아 내지 못할 수도 있다는 문제가 발생한다.

이상의 것이 본 연구의 한계이지만, 이 문제들은 계속적인 연구가 필요하며 해결을 할 수 있을 것으로 기대된다. 서버의 Daemon으로 기동하여 해결할 수 있는 실마리를 찾을 수 있으리라 기대된다.

참고문헌

[1] Cerf, V., "IAB Recommendations for the Development of Internet Network Management Standards", RFC 1052, IAB, April 1988.

[2] Case, J., Fedor, M., Schoffstall, M., and J. Davin, Simple Network Management Protocol (SNMP), RFC 1157, SNMP Research, Performance Systems International, Performance Systems International, MIT Laboratory for Computer Science, may 1990.

[3] Rose, M., and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based Internets", RFC 1065, TWG, August 1988.

[4] McCloghrie, K., and M. Rose, "Management Information Base for Network Management of TCP/IP-based Internets", RFC 1066, TWG, August 1988.

[5] Case, J., M. Gedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol(SNMP)", RFC 1098, (Obsoletes RFC 1067), University of Tennessee at Knoxville, NYSERNet, Inc., Rensselaer Polytechnic Institute, MIT Laboratory for Computer Science, April 1989.