이더넷 상에서 인터넷 프로토콜 주소 충돌 검출방법에 관한 연구

유상민°, 박기홍
군산대학교 컴퓨터 정보과학과
{smyu, kh.park}@cs.kunsan.ac.kr

A Study on Detection Method Internet Protocol Address Collision in a Ethernet

Sang-Min Yu°, Kihong Park
Dept. of Computer Information Science, Gunsan University

요 약

이 논문은 TCP/IP 기반 지역 망 내에서 개인용 컴퓨터의 사용에 있어 인터넷 프로토콜의 주소 충돌 해결 방법에 대하여 연구하였다. 현재 컴퓨터의 수는 계속해서 늘고 있지만 사용자는 IP 주소에 대한 지식이 없음으로 인해 고의나 실수로 자신의 것이 아닌 다른 사람의 IP 주소를 사용할 수 있고, 이로 인해 원래 사용자가 네트웍을 사용할 수 없게 된다. 본 논문은 사전에 지역 망 내의 관리 대상 컴퓨터들의 주소정보를 DNS 서버상에서 수집하여 현재 사용하는 주소 정보가 저장된 정보와 같은 지를 검사하는 방법으로 IP 주소 충돌 검출 방법을 제시하였다.

I. 서 론

1. 연구의 필요성 및 목적

본 연구 논문은 Ethernet을 사용하는 네트워크망(학내 망)에서 관리자가 User 에게 할당한 IP 주소를 실수 또는 불법으로 다른 사용자가 사용하게 되면 정식 사용자는 Network를 사용하지 못하게 될 것이다. 그 이유는 IP 주소는 전 세계에서 유일하게 사용되기 때문이며, 하나의 IP 주소를 두 사람이 사용하게 되면 먼저 Network에 접속한 사람은 사용할 수 있으나, 이후에 동일한 IP 주소를 가지고 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 없었고, 충돌한다는 메시지를 시스템에 따라서 보여주기는 하나 그것을 해결할 방법은 없었다.

위와 같은 문제로 인하여 본 논문에서는 Network 관리자의 입장에서 user에게 안전한 Network의 사용을 제공하기 위하여 충돌하는 IP 주소를 DNS Server에서 패킷을 검색(출발지 주소와 목적지 주소가 존재) 이때 패킷을 filtering 하여 NIC의 MAC 주소와 IP 주소를 검출, 실수 또는 불법으로 사용하는 사용자를 정식의 사용자에게 IP 주소를 돌려주기 위하여 연구하게 되었으며, 첫 번째로 실수 또는 고의로 사용하는 사용자가 TELNET으로 DNS(Domain Name Service) server에 접속하여 서비스를 이용하게 되면, "충돌하는 IP Address 입니다."라는 메시지를 보여주고 일정한 시간이 지난 뒤 접속을 끊게 하여준다.

본 논문의 구성은 서론에서의 연구의 필요성 및 목적과 관련연구에서의 각 NMS에 대한 설명 부문과 본 논문의 실제적인 시스템 설계, 구현 마지막으로 평가로 나누어져 있다.

본 논문의 중점으로는 Ethernet기반 네트워크상에서의 IP 주소 충돌을 MAC 주소로 찾아내어 인증하지 않은 ADDRESS의 사용자에게 경고메세지를 보내어 충돌에 대한 서비스 중단을 막아보고자하는 것에 의미를 두고자한다.

II. 관련 연구

1. NMS (Network Management System)

네트웍 관리 시스템이란 서로 다른 환경과 다른 회사 제품으로 복잡하게 연결, 분산되어 있는 네트웍에 대한 환경 관리와 물리적, 논리적인 연결에 대한 감시, 네트워크 사건의 감지와 그에 따른 적절한 보고 기능, 고장 시 경보 기능 및 자동 회복 기능 등을 해주는 강력하고도 정교한 통합적인 관리 시스템을 말한다. 이러한 광범위한 네트워크 통신 장비들을 관리

함으로써 사용자는 복잡한 네트워크 상태를 자세하게 알아 볼 수 있고, 문제가 발생하였을 때의 검출이나 수정, 또는 네트웍 구성의 변경 등을 신속하게 처리할 수 있다. 이와 같은 요소(관리자, 대리자, 긴밀한 연락, 상태 정보 등)들을 통틀어 네트워크 관리 시스템이라 하며 좁은 의미로는 관리자만을 지칭하기도 한다. 네트워크의 대형화, 복잡화, 네트워크를 이용한 업무의 증가 등으로 네트웍 관리에 대한 중요성이 부각되고 있고, 네트워크의 이상 종료 시에 신속한 대처는 기본이고 발생 가능한 사건을 사전에 제거하는 것이 중요하다. [1]

2. SNMP (Simple Network Management Protocol)

효과적인 전산망관리를 수행하려면 기본적으로 전산망관리 시스템과 피 관리 노드간의 관리정보를 주고받기 위해 관리정보 통신프로토콜, 관리정보구조, 관리정보의 정의 등의 전산망관리 메커니즘이 표준화되어야 한다. 이에 88년 초 IAB(Internet architecture Board)에서는 표준화가 작업을 시작했다.

이 때까지 연구가 진행됐던 HIMS, SGMP, CMIP/CMIS중에서 SGMIP를 발전시킨 SNMP를 표준으로 채택했다. SNMP는 TCP/IP 환경에서의 네트워크 관리 프로토콜이며 허브처럼 지속적인 관리가 요구되는 장비에는 SNMP 에이전트 소프트웨어가 탑재되어 원격 지에서도 포트별 작동 상황을 감시할 수 있다. 그러나 여러 가지 문제점으로 인해 구현이 힘들어서 결국 IAB는 몇 가지 결정을 내렸다. 첫째, 기본적으로 SNMP를 채택하였고, 둘째, IAB가 업체들은 ISO CMIS/CMIP를 기반으로 한 망 관리 시스템을 개발하여 발전시켰다. 셋째, SNMP와 관련된 작업은 IETF가 책임지고, 끝으로 이전의 연구 작업 결과를 적극 수용하는 것이다. 이렇게 출발한 SNMP는 구현이 쉽고 간단하여 오늘날 가장 일반적인 네트웍 관리 프로토콜이 되었고, CMIP는 구현의 복잡성, 방대함으로 인해 아직도 망 관리의 중심으로 자리잡지 못하고 있다. 전산망의 효율적인 관리를 목표로, TCP/IP를 기반으로 하는 전산망을 관리하기 위해 간단히 운용할 수 있는 구조와 시스템을 제공하며, 국내 전산 망이 개방시스템 상호접속(OSI)으로 완전히 전환되기 전까지는 전산망관리 잠정표준으로서 전산망에 적용된다.[2], [3]

III. 시스템 설계

1. 시스템의 기본 방향

본 시스템은 지역 망 내에서 운용되는 컴퓨터들의 IP 주소와 Mac 주소에 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 일맥 상통한다. 각각은 독립적인 하나의 메뉴로 되어 있으므로 필요한 부분을 실행 할 수 있다. 메뉴의 종류 및 기능은 다음과 같다.

첫째, 망 내에 있는 관리 대상 컴퓨터들의 IP 주소와 Mac 주소를 데이터 파일로 생성, 관리하는 부분이다. 둘째, 지역 망 내에 떠도는 패킷들의 주소 정보를 추출하는 부분이 있다. 이는 임의의 시간에 서버가 추출하며 24시간 계속 적으로 실행 될 수 는 없다. 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. 끝으로, 잘못된 사용자의 접속을 종료하는 부분이다. 이 부분은 사용자에게 불이익을 줌으로써, 문제해결을 유도한다.

IV. 구 현

1. 설계 및 구현

1.1 설계

1) 착안점

설계에 있어서 우리가 알아야 할 것은 지금 사용중인 Personal Computer는 사용자가 일부러 이든 실수이든 자신의 IP 주소를 바꾸는 것에 아무런 제약이 없다. 또한, 자신의 IP 주소가 아닌 것을 사용해도 통신이 가능하며, IP 주소의 소유에 관한 제약이 없다. 이를 해결하려는 것이 본 연구의 목표이다.

1.2 구현

1) Source Data Management)

Mac Address와 IP Address, 사용자 정보에 대한 자료 처리는 추가, 삭제, 검색, 삭제표시 된 자료삭제의 Sub Menu가 있다. 자료의 변경은 프로그래밍하지 않았으므로 직접 관리자 Data 파일에서 처리해야한다.

2) IP Address Search

IP Address에 대한 정보수집은 packet -v arp 명령어의 결과를 File에 저장하는 방법을 이용하였다.

참고로 packet은 패킷의 정보를 보여 주며 이 정보 안에는 sender의 IP 주소와 Mac 주소에 대한 자료가 있다. 여기서는 arp packet만을 수집하도록 하였다.

3) View Collision Detection

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 사용중인 PC의 IP Address가 올바른 것인 지를 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 Address 및 IP Address, 그리고 정식으로 등록된 Mac Address에 대한 IP Address, 학과, 연락처가 출력된다.

4) 사용자 메시지 전송(Send Message for Connector)

우선 현재 server에 접속한 사용자의 정보를 수집하여 who.txt파일에 기록하고, Who.txt 파일에서 IP Address와 User ID를 추출하여 who_r.dat에 기록한다. 이 자료를 충돌 검색에서 생성된 report.dat의 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.

V. 평가

1. Program의 효과

본 연구는 실제 User들의 입장에서 IP 주소의 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 판단할 문제로 남겼다. IP Address를 도용한다고 해도 다른 그룹의 IP 주소는 사용할 수 없다.

네트워크 관리자는 IP 주소에 대한 관리를 통해 사용자의 편의와 IP 도용에 따른 보안에 이르기까지 관리를 해야 한다. 또한 이로 인해 사용자 편의 등도 무시해서는 안될 것이다.

그래서 본 연구에서는 IP 주소의 충돌에 대하여 충돌을 발생시킨 컴퓨터가 어느 것인지 Mac 주소에 의해 알아냄으로 써 해결의 실마리를 찾고, 그 Computer를 사용하는 User에게 올바른 IP 주소를 알려줌으로써 해결할 수 있도록 하였다. 고의적인 IP 주소도용에 대한 해결책으로는 DNS Server에 접속한 사용자에게 Message전송 후 연결을 강제로 종료함으로써 대응하도록 하였다.

2. Program의 제한점

본 연구의 제한점은 다음과 같다.

첫째, Ethernet을 사용하는 내부망내에서 만을 고려 하였다는 것. 외부에서의 사용에 대해서는 의미가 없었다.

둘째, 여러 가지 서비스중에 telnet 서비스에 대해서만 다루었다는 것. 나머지 Web과 Ftp 서비스에 대해서는 차후 연구 과제해서 풀어나가려 한다.

셋째, 본 연구 결과물의 실행에 있어서의 제한은, 우선 망내에의 모든 개인 Computer에 대하여 MAC 주소와 할당해준 IP 주소에 대한 정보를 모두 가지고 있어야 한다. 이 내용은 곧 Network 관리자가 모든 할당하여준 IP 주소와 MAC 주소를 데이터베이스화 하여야 한다는 것이다.

이상의 것이 본 연구의 제한점이지만, 이 문제들은 계속적인 연구개발이 필요하며 모두 해결 할수 있으리라 생각된다.

참고문헌

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

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

[3] Case, J., M. Fedor, 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.