인터넷 서비스거부공격을 방지한 원격 제어 서비스 알고리즘

권용성
광운대학교 전자공학과
전화 : 02-3665-1432 / 핸드폰 : 011-527-7186

Algorithm of Remote control service against Denial Of Service Attacks

Yong Seong Kwon
Kwangwoon University
E-mail : shine3535@yahoo.com

Abstract

This paper describes remote control RS232 communication using internet service, safety of exchange data and internet traffic by Denial of Service Attacks. In case of Denial of service Attacks, it makes connection of internet service failed. So in this paper, this solution was examined and implemented for receiving data in safety against Denial of Service Attacks by LabVIEW program of National Instruments.

I. 서론

인터넷을 통한 원격제어 서비스는 현재 인터넷을 사용하고 있는 사용자들이 생활과 밀접하게 연관되어 있으며 접근하기 용이하고 문제 발생시 원인을 분석하기 위하여 직접 이동해야 하는 시간적인 비용을 줄일 수 있고 멀티미디어 서비스를 지원할 수 있는 점에서 폭 넓게 연구되고 있으며 화상회의 및 원격 강의 같은 가상 공간에서의 교육적인 면에서 다용도로 응용하고 있다.

따라서 인터넷을 사용할 수 있는 어느 장소에서든 서비스를 받을 수 있는 장점으로 원하는 정보의 공유, 사용 및 제어를 효율적으로 운용할 수 있기 때문에 인터넷을 이용한 폭넓은 서비스의 안정된 정보를 얻을 수 있게 시스템 관리에 대한 연구가 필요하다.

본 논문은 인터넷 서비스를 이용한 RS232 통신을 원격제어 하면서 정보 교환에 안정성과 대량의 사용자들이 접속했을 때 생기는 인터넷 서비스 장애에 따른 문제점을 분석하고 인터넷 서비스 장애 및 접속의 폭주 시에 대체할 수 있는 경로 또는 사전에 예방 할 수 있는 대안으로 인터넷 서비스를 안정성 있게 운용할 수 있도록 구현하였다.

II. 서비스거부공격 구조

2.1 MAC address 구조

인터넷 서비스를 이용하는 것은 컴퓨터간의 상호 통신을 의미하며 컴퓨터는 네트워크 상에서 서로 구분이 필요한데 서로를 구분할 일종의 주소 MAC(Media Control Access) address가 필요하다. 통신을 위해서 각 장비마다 IP 주소가 배

정되고 TCP/IP로 통신을 하고 따라서 통신을 위해서 IP 주소를 사용한다. ARP(Address Resolution Protocol)는 IP 주소를 다시 MAC address로 바꾸는 절차로 컴퓨터 상호간에 ARP를 요청하고 ARP응답을 받으므로 주소를 확인한 다음에 통신을 시작하게 된다. ARP 요청과 응답은 그림 1과 같다.

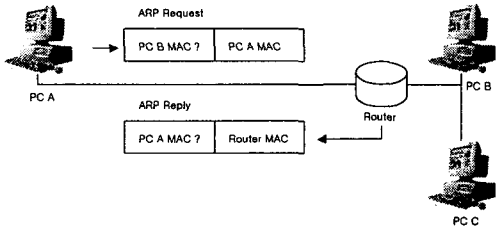

그림 3. ARP 요청과 응답 (ARP request and reply)

2.2 TCP segment 구조

TCP은 데이터를 전송하기 전에 데이터 전송변수를 설정하기 위한 서로간의 Handsake를 하게 된다. 즉 접속을 확인하는 준비 Segments를 주고받으면서 연결상태를 확인한다. 사용자가 처음으로 TCP Segment를 보내고 두 번째로 서버가 TCP Segment로 응답을 하고 마지막으로 사용자가 TCP Segment로 응답을 하는 것을 Three-way handshake라고 한다. 데이터는 Socket을 통해서 전해지고 Three-way handshake으로 형성된 TCP 송신 버퍼에 놓이면서 편리하게 Segment 형식으로 보내게 된다. Segment는 Network 계층으로 전해지고 Application에서 TCP connection's 수신 버퍼에 놓여진 데이터를 읽게 된다. TCP 송신 버퍼, 수신 버퍼는 그림 2와 같다.

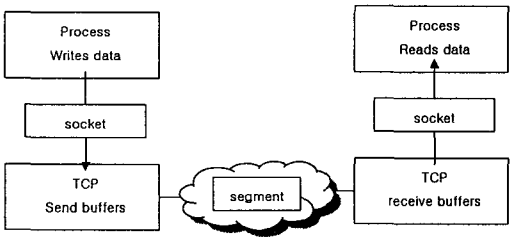

그림 4. TCP 송신 버퍼, 수신 버퍼
(TCP send buffers, receive buffers)

2.3 서비스거부공격 구조

인터넷 서비스 운용에 있어서 1대1 상황에서 다수의 접속으로 통신 및 정보를 전송 할 때 정보를 여러 번 전송함으로 인터넷 서비스 시스템의 무리를 줄 수가 있고 전송 속도 역시 영향을 받게 된다. 인터넷 서비스 시스템은 Transport 계층의 TCP/IP를 이용하여 대량의 사용자들이 접속하게 되면 사용자들과 계속적으로 연결상태와 정보를 요청하고 응답을 기다리므로 Traffic을 증가시켜 서비스 장애를 갖게 된다.

현재 서비스 장애를 일으키는 서비스거부공격(DoS, denial of service)이 이용되어지는데 서비스거부공격은 특정 사이트에 컴퓨터가 처리할 수 없을 만큼 대량의 접속신호를 보내 해당 인터넷 서비스를 마비시킴으로 서비스 시스템의 정상적인 수행에 문제를 일으키고 인터넷 서비스로부터 발생할 수 있는 손실된 비용과 그런 공격들에 의해 소모되는 막대한 분량의 대역폭 비용이 크다. 이런 공격들은 심각한 경제적인 영향을 가져온다. 만약 이들을 탐지하고 완화시키는 능력이 없다면, 네트워크를 초과 설비해야 하며 더 많은 대역폭을 구입해야만 한다. DDoS(Distributed Denial of Service) 역시 지난해 세계적인 인터넷 서비스를 다운시켰고 최근 등장한 웹서버용 해킹법으로, 해당 IP주소로 집중적 접속을 시도해 엄청난 Traffic을 유발함으로써 서버를 마비시키는 매우 고전적 수법이다. 그림 3은 다중접속을 나타내었다.

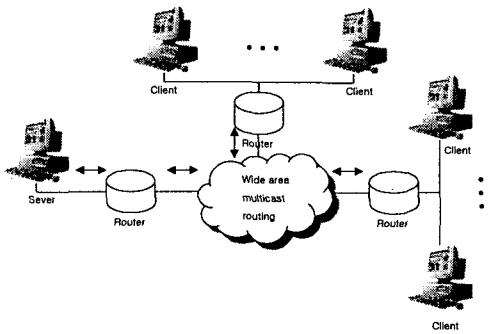

그림 5. 다중 접속

III. 인터넷 서비스거부공격을 방지한 알고리즘 검증

3.1 서비스거부공격 대안 알고리즘 구현

(1) 서비스거부공격 대안

평상시와 달리 유난히 Traffic 양이 많아지고, 서버에 대한 서비스 요구가 평균치를 훨씬 웃돈다면 이는 DoS/DDoS 공격 신호라고 할 수 있다. 이때는 Traffic 분석과 서비스 요청 패턴을 판별해냄으로써 공격을 막을 수 있는 방법을 강구해야 한다.

Firewall이 있다면 서버로 가해지는 서비스거부공격은 어느 정도 예방할 수 있다. 하지만 공격자가 목표가 되는 네트워크의 대역을 넘치게 하면 서버 상에서는 이를 막을 수 있는 방법이 없기 때문에, 서버 관리자가 할 수 있는 최상의 대비책은 서버가 과부하 걸리기 전 Packet Filtering 하는 것이다. 과도한 Traffic이 내부 특정 호스트에서 나온다면 그 호스트는 서비스거부공격을 위해 이용당하고 있다고 판단하고 대처해야 한다. 공격이 예상되면 서비스 설정을 임시로 바꾸거나 외부에서 오는 접속을 관리함으로써 이를 막을 수 있지만, 서비스 질이 떨어질 우려가 있다. 또 연결에 대한 타임아웃 시간을 줄임으로써 부하를 감소시킬 수도 있지만, 이렇게 하면 정상적인 접속이 끊어질 수 있다는 점도 염두 해야 한다.

(2) 서비스거부공격 대안 알고리즘 구현

서비스거부공격을 받았을 때 인터넷 서비스를 제공하는 시스템의 안정성을 보장하고 사용자들의 인터넷 서비스를 중단 없이 제공받을 수 있도록 구현한다.

인터넷 서비스 시스템은 National Instruments에서 고안된 LabVIEW 프로그램을 이용하여 구현하였으며 메인 서버로 제1 종속 서버, 제2 종속 서버와 정보를 공유하므로 서비스거부공격으로부터 정보 보존과 접속을 유지하게 하므로 정보 손실을 막는다. 사용자들은 제1 종속 서버와 접속을 하면서 메인 서버의 정보를 얻게된다. 따라서 사용자들은 메인 서버의 정보를 얻지만 실제 접속은 제1 종속 서버와 하게 된다. 서비스거부공격이나 대량의 접속으로 서비스 장애가 일어나기 전에 제1 종속 서버는 제2 종속 서버와 접속을 가능하도록 사용자에게 알리고 서비스 장애가 발생했을 때는 제1 종속 서버와 접속이 불가능하므로 접속중이였던 사용자들은 제2 종속 서버와 자동으로 접속을 재기하므로 중단 없이 서비스를 받을 수 있다. 사용자의 메인 서버 접속 구조는 그림 4와 같다.

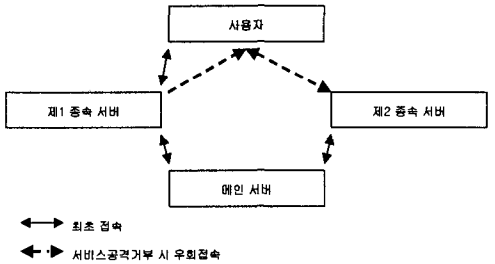

그림 6. 메인 서버 접속시

3.2 서비스거부공격 대안 알고리즘의 검증

메인 서버에서는 RS232 통신 장비로부터 정보를 얻으면서 사용자가 접속할 때까지 대기한다. 그림 5는 메인 서버에서 RS232 통신 장비로부터 얻은 정보를 그래프로 실행한 화면이다. 그림 5의 그래프는 사용자 접속시 다음과 같은 주기로 전송된다.

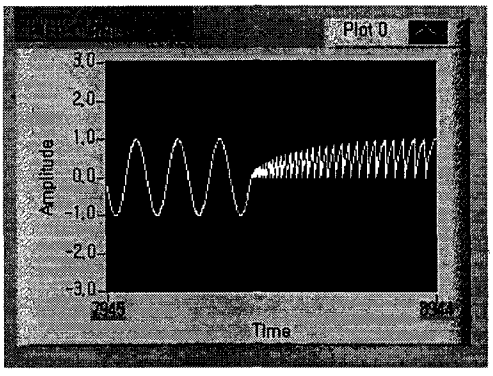

그림 7. 메인 서버

사용자가 접속을 시도하면 제1 종속 서버를 통해서 메인 서버의 정보를 전송을 받는다. 그림 6의 윗부분의 그래프는 사용자가 제1 종속 서버에 접속하고 받은 정보를 그래프로 나타내고 있다.

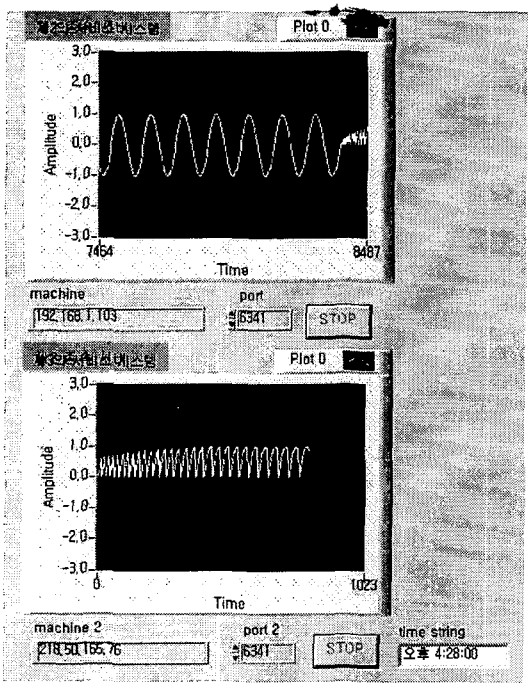

그림 8. 제1 종속 서버와 제2 종속 서버 접속 화면

서비스거부공격을 받으면 제2 종속 서버와 접속을 시도한다. 그림6의 아랫부분의 그래프는 제1 종속 서버에서 접속 실패로 받은 정보 다음부터 제2 종속 서버로부터 받고있다.

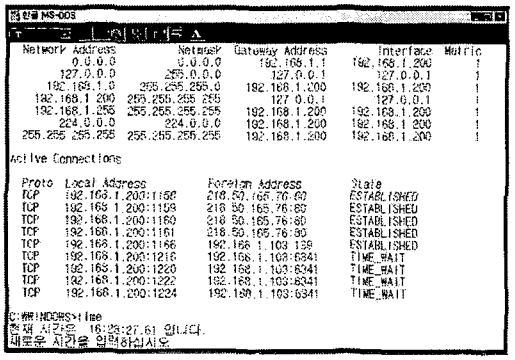

그림 9. TCT/IP 네트워크 연결상황

제2 종속 서버와 접속을 제기한 직후 사용자의 TCP/IP 네트워크 연결상황을 그림 7로 보여 주고 있다.

서비스거부공격으로부터 정보 보존과 접속을 유지하게 하므로 정보 손실을 없이 동작함을 검증하였다.

Ⅳ. 결론

이번 논문은 RS232 통신장비를 원격 제어하고 통신장비의 정보를 어느 장소에서든 인터넷 서비스를 이용해서 얻을 수 있으며 인터넷 서비스 시스템의 능력에 한하여 다수의 접속이 가능하지만 서비스거부공격을 받아서 인터넷 서비스 장애가 발생했을 때 RS232 통신장비의 제어와 작동 상태정보를 인터넷 서비스 중단 없이 이용할 수 있게 구현하였고 정보의 손실 없이 동작함을 확인하였다. 앞으로 인터넷의 수용능력이 크게 향상시키는 것이 중요한 과제이며, 다방면으로 서비스거부공격의 문제해결이 요구되며 본 논문은 실시간으로 정보를 이용하거나 인터넷 서비스의 관련된 기관에 안정된 운용을 할 수 있도록 활용될 수 있을 것이다.

참고문헌

[1] Kurose, James F./ Ross, Keith W. "Computer Networking" Addison wesley.

[2] Jeffrey Travis. "Internet Applications in LabVIEW" PH PTR.

[3] Hunt Craig. "TCP/IP Network Administration 2/E" March. 1999. O'Reilly

[4] Donahoo, Michael J./ Calvert, Kenneth L. "Pocket Guide to TCP/IP Sockets" Morgan Kaufmann Pub.