제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

IPsec을 이용한 원격 감시 및 제어 시스템에 관한 연구

윤철환*, 김희천*, 나종화*,
신승중*, 정광호*, 류대현*
*한세대학교 IT학부
e-mail:{chyoon, hck, jwna expersin, khjung,
dhryu}@hansei.ac.kr

A Study on Remote Monitering and Control System using IPsec

Chul-hwan Yoon*, Hee-chern Kim*, Jong- Whoa Na*,
Seung-jung Shin*, Kwang-ho Jung, Dae-hyun Ryu*
*Dept. of IT, Hansei University

요 약

본 논문에서는 IPsec을 지원하는 VPN을 이용하여, 인터넷과 같은 공중망을 이용하면서도 보안성이 우수한 원격 감시 제어 시스템을 개발하였다. 개발된 시스템은 리눅스를 탑재한 임베디드 시스템으로 개발되어, TCP/IP 프로토콜 처리와 암호통신 등의 기능을 수행하며, 무인 원격 방범기기를 포함한 다양한 응용 분야에 적용이 가능하다.

1. 서론

인터넷 보급 확산에 따라 웹을 기반으로 한 원격 감시 및 제어 시스템 개발에 관한 연구가 활발히 진행되어 왔다. 환경 감시, 전력 설비, 무인 공장, 원자력 제어, 보안 시스템과 같은 사람이 현장에서 직접 시스템을 운영하기 어려운 분야에 특성상 원격 감시 및 제어 시스템의 이용은 필수적이다.

이러한 원격 감시 및 제어 시스템은 초기에는 중앙 집중형을 기반으로 하여 구현되었으나 점차 분산처리를 기반으로 하는 환경으로 급속도로 변환되고 있다. 원격 관리 및 제어를 위해서는 필수적으로 컴퓨터 네트워크를 기반으로 하게 된다. 원격 감시 및 제어 시스템의 핵심을 이루는 네트워크의 경우, PSTN 망을 사용하여 보안 정보를 송신하거나 저속, 저가의 전용선을 통한 서비스를 수행한다면 서비스 사업자와 고객 모두에 다음과 같은 여러가지 문제를 야기할 수 있다.

우선 ISP(Internet Service Provider) 측면에서 살펴보면 네트워크의 고도화에 따라 저가의 전용선 사업을 점차 축소시켜 신규 증설을 억제하고 유지보수도 줄여나가고 있다. 이러한 ISP의 정책으로 인하여 무인경비 서비스 사업자와 같은 원격 감시 및 제어 시스템 사업자는 대체 망을 찾을 수밖에 없는 상황에 이르렀다. 뿐만 아니라, 센서에 기초한 침입 탐지 외에 영상 정보에 기초한 향상된 서비스를 제공하기위해서 기존의 네트워크 인프라의 대역은 크게 모자란 실정이다. 따라서, 고급 서비스에 대한 고객의 분명한 요구와 관련 기술의 지원이 가능함에도 불구하고, 저속의 네트워크로 인해 서비스가 불가능한 현실이다.

최근에는 ADSL/VDSL과 같은 광대역 정보 통신망의 등장으로 원격 감시 및 제어 시스템의 도입에 대한 요구가 크게 증가하고 있는 추세이다. 특히 인터넷이나 인터라넷을 기반으로 웹을 이용하는 시스템 환경 구축에 관한 연구가 활발히 진행되고 있다. 웹을 기반으로 하면 데이터베이스와 손쉽게 연동을 할 수 있으며 응용시스템의 개발이 용이하다는 장점을 가지고 있다.

그러나 지금까지 연구되어온 대부분의 원격 감시 및 제어 시스템의 경우 인터넷을 기반으로 하고 있

으나 보안상의 문제는 중요하게 생각하고 있지 않고 있다. 인터넷 기반의 원격 감시 제어 시스템에 있어서 정보 보안의 문제는 매우 중요하다.

본 논문에서는 IPsec을 지원하는 VPN(Virtual Private Networks)을 이용하여, 인터넷과 같은 공중망을 이용하면서도 보안성이 우수한 원격 감시 및 제어 시스템을 개발하였다. 개발된 시스템은 리눅스를 탑재한 임베디드 시스템으로 동작하며 TCP/IP 프로토콜 처리, IPsec을 이용한 암호통신 등의 기능을 수행한다.

본 논문에서 개발된 시스템은 무인 원격 방범기기 뿐 아니라 가정용 보안 게이트웨이로 부가 서비스를 제공할 수 있다. 또한 원격 감시 보안시스템, 원격 제어, 원격 환경 감시, 군사용 감시 및 제어 시스템, Remote Banking System 등으로 활용범위를 넓힐 수 있다. 뿐만 아니라 향후 음성 통신기능, 멀티미디어기능 등과 다양한 네트워크 인터페이스를 제공함으로써 가정용 게이트웨이 또는 통합형 접속장비(Integrated Access Device) 시장을 장악하는 제품으로 발전할 가능성을 갖고 있다.

2. 시스템 구성 및 요구사항

본 연구에서 개발한 전체 시스템은 단말 시스템과 관제센터의 서버 앞단에서 암호화된 데이터를 복호화하는 서버측 게이트웨이 시스템으로 구성된다. 단말 시스템은 알람센서나 계측기 등에서 보내온 RS232C 방식의 통신 데이터를 TCP/IP 방식으로 변환 및 암호화하여 인터넷 등의 공중 통신망을 통해 관제센터로 전송한다. 암복호와 관련하여 표준 프로토콜인 IPsec을 사용하므로 관제센터의 서버 앞단에는 IPsec을 지원하는 상용 VPN을 사용할 수도 있다. 시스템 구성도는 그림 1과 같다.

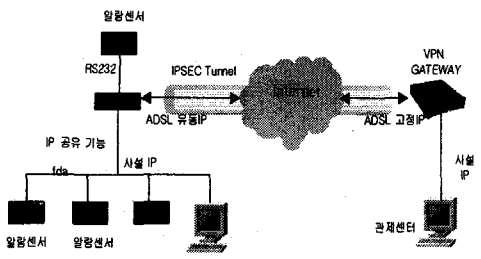

그림 1 시스템구성도

따라서 본 시스템은 H/W로 RS232C 통신 Interface, TCP/IP Stack, RS232C - to-IPSec, 공유기 기능이 내장될 필요가 있다. 개발 시스템은 좁은 대역의 알람 기기 데이터 전송장비로서의 기능 뿐 아니라 높은 전송 속도로 가지게 되므로 멀티미디어 서비스 제공도 가능할 것이다.

개발 시스템은 ADSL Modem 또는 Cable Modem에 연결하여 사용할 수 있다. 보안성 이요구되는 경우에 데이터는 모두 암호화를 해서 관제 서버로 전송이 되며, 일반 사용자들은 인터넷 망을 사용할 수도 있다. 이때 데이터는 암호화 없이 인터넷 망으로 나가게 된다. 또한 4port 스위칭 HUB가 내장되어 있으며, 외부의 HUB를 이용할 경우 254개의 PC를 연결해서 사용 할 수 있다.

단말 시스템의 기능은 다음과 같다.

- 센서 기기의 RS232C 신호를 수신
- 사용자에게 TCP/IP 통신을 가능하게 해줌
- IP 공유기 기능 제공
- RS232C를 IPSec Protocol로 변환
- 통신 신호의 암호화 복호화(IPsec 기능)

또한 다수의 단말 시스템은 인터넷 망을 이용해서 관제 센터에 있는 VPN 게이트웨이로 데이터를 전송한다.

본 시스템의 요구 사항을 H/W와 S/W로 나누어 보면 다음과 같다.

< H/W 부분 >

(1) RS232C 통신 interface

- 외부 알람 기기와 통신이 가능한 interface제공

(2) TCP/IP 통신 Interface

- 알람 기기의 데이터를 Internet 망으로 보내기 위한 기능 제공

< S/W 부분 >

(1) Network protocol stack

- ARP , TCP/IP , DHCP , ICMP등의 Network protocol stack을 제공.
- RS-232C ⇔ TCP/IP protocol 변환 기능 : RS232C 포트의 데이터를 Ethernet을 통해서 송수신 하는 기능 제공
- 암호화 모듈 : 알람 기기 데이터를 암호화 하여 IPSec protocol로 만드는 기능 제공
- IP 공유기 기능 : NAT , DHCP를 이용한 IP공

유기 기능 제공

- 보안기능 : 방화벽, 추적기능, 유해사이트 차단 기능, URL 필터링 기능 제공

3. 시스템 설계 및 구현

가. 하드웨어 구성

본 시스템의 하드웨어 구성은 그림 2와 같다.

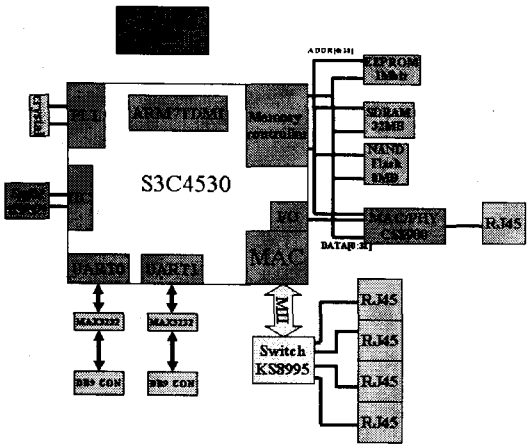

그림 2 하드웨어 구성

S2C4530은 ARM사의 ARM7TDMI Core를 이용한 MCU이다. 내부에는 네트워크 기능을 강화 할 수 있는 H/W 블록을 가지고 있다. 내부의 MAC 블록은 switch chip을 제어할 때 유용하며, 메모리는 EDO DRAM, SDRAM, SRAM 모두를 지원하지만 가장 저렴한 SDRAM을 사용하였다. 또한 WAN 인터페이스를 위한 NIC로는 CIRRUS LOGIC의 CS8900을 사용하였다. CS8900은 direct ISA interface NIC로 내부에 MAC과 PHY를 포함하고 있다. 따라서 S3C4530의 Ext I/O영역에 매핑하여 사용한다. UART는 S3C4530 내부에 2개가 있으므로, 외부에 드라이버만 장착하여 사용한다. UART0는 프로그램 개발 기간동안은 console port로 사용을 하고 linux porting이 끝난 후에는 알람 기기의 데이터를 관제 센터로 보내는 기능으로만 사용한다.

나. Embedded OS

운영체제로는 Vitals systems사의 vlinux를 이식하였다. Vlinux는 기본적으로 MMU가 없는 ARM7TDMI 용으로 최적화된 OS이며, linux kernel 2.2.14 버전이 올려져 있다. 그러므로 kernel 2.2.14 버전에 포함되어 있는 기본적인 네트워크 기능이 지원된다

다. IPsec

IPsec 암호화 기능은 freeswan 1.9 Open Source를 ARM7TDMI MCU에 맞도록 porting하여서 구현하였다. 삼성에서 제작한 ARM7TDMI 칩은 어드레스 선(address line)이 반드시 4byte align 되어야 하는 제약조건이 있는데, 이점을 유의하면 어렵지 않게 porting할 수 있다.

라. Serial to Ethernet 변환 (seiper 프로그램)

Serial to ethernet 변환 기능은 세가지의 프로그램으로 구성된다.

Seiper: (serial to ip changer) : 단말 시스템에서 동작하는 응용 프로그램으로서 센서로부터 데이터를 RS-232C로 받고, udp패킷으로 작성하여 udpserver의 slmon port(7101)로 전송한다.

Udpserver: 관제서버에 탑재되는 프로그램으로서 seiper 프로그램이 전송한 udp 패킷을 해석하여 그 내용을 보여주는 프로그램이다.

Udpsender: 관제서버에 탑재되는 프로그램으로서 알람센서에 제어데이터를 보낼 때 이용하는 프로그램이다. 단말 시스템의 slcontrol port(7102)로 보내면 seiper 프로그램이 이를 잡아내어 serial 라인으로 전송한다.

현재 serial line으로 통신할때의 통신 규약은 seiper 프로그램내부에 하드코딩되어 있으며, 다음과 같은 규격을 준수한다.

- Nonblocking IO
- 7bit, even parity, 1 stop bit
- baud rate: 300 bps ~ 56Kbps

마. 암호화 통신 구현

개발 시스템과 관제서버 앞단에 있는 VPN게이트웨이와는 서로 암호화된 터널(tunnel)을 형성한다. 개발 시스템상에 동작하는 seiper 프로그램과 관제서버에서 동작하는 udpsender 프로그램은 통신하는 대상이 모두 암호화된 더널 내부에 해당하므로 개발 시스템과 VPN게이트웨이 사이에서 IPsec의 ESP 프로토콜에 의해 암호화 된다.

3. 시험 및 평가

시험 및 평가를 위해 그림 3과 같은 시험환경을

구성하였으며 관제센터 쪽의 VPN 게이트웨이는 상용 VPN을 사용하였다.

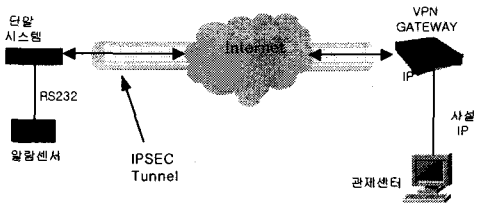

그림 3 시험환경 구성

개발 시스템은 유동 IP를 얻어서 인터넷에 접속한다. 터널과 관련된 파라메타들은 Web Interface를 통하여 설정할 수 있다. 터널을 형성하는 과정은 크게 두가지로 나누어진다. 처음의 과정에서는 eth0 network interface위에 ipsec 이라는 가상의 interface를 추가하는 과정이며, 두번째 과정에서는 whack이라는 명령어를 이용하여 터널 설정 정보를 커널에 전달하고, 터널을 생성 하게 된다.

개발 시스템과 사용 VPN 게이트웨이와 VPN 터널이 연결된 상태에서 개발 시스템에서 VPN 게이트웨이로 ping을 날려보고 되돌아오지 않으면 VPN 터널이 문제가 발생한 것으로 보고 VPN 터널을 다시 생성한다. ADSL 또는 전용선 케이블이 제거되었거나 ADSL 모뎀 전원이 꺼졌거나 VPN 게이트웨이에서 VPN 터널을 일방적으로 중지 해 버리면 ping이 되돌아오지 않을 것이다. 이럴 경우 VPN 터널을 다시 생성하려고 계속 시도한다.

4. 결론

본 논문에서는 IPsec을 지원함으로서, 인터넷과 같은 공중망을 이용하면서도 보안성이 우수한 원격 감시 및 제어 시스템을 개발하였다. 개발된 시스템은 원격 감시 및 제어 시스템에서는 정보의 암호화 뿐만 아니라 방화벽기능, 공유기능, 유해사이트 차단 기능 등을 종합적으로 제공하는 가정용 네트워크 보안 게이트웨이의 기능도 추가할 수 있다. 따라서 유비쿼터스(Ubiquitous)의 연장선에서 고려될 수 있는 가정용 게이트웨이(Residential Gateway)에도 적용될 수 있을 것이다.

논 논문에서 개발된 시스템은 원격 감시 보안시스템, 원격 제어, 원격 환경 감시, 군사용 감시 및 제어 시스템, Remote Banking System 등으로 활용 범위를 넓힐 수 있다. 이러한 기술의 적용이 성공적으로 이루어 질 수 있다면 초고속정보통신망에서 분산 멀티미디어 이용 기술의 확산으로 원격 영상감시, 제어뿐만 아니라 물류 및 통합 공정시스템 등 다양한 분야에 활용할 수 있는 기술 개발이 가능해진다. 따라서 초고속 정보통신망 하에서 원격 감시 및 제어 시스템의 시장성을 대단하다고 볼 수 있고, 전체 산업 발전에 끼치는 영향은 크다고 할 것이다.

한편, 현재까지 그 가능성으로 한껏 기대를 모았던 가정용 게이트웨이는 고객의 입장에서 그 필요성이 명확하지 않아 상품화로써의 장벽을 넘지 못하였다. 하지만, 이미 확고한 시장을 확보하고 있는 무인경비 서비스의 고도화를 통해 고객에게 접근함으로써 가정용 게이트웨이 또는 통합형 접속장비(Integrated Access Device) 시장을 장악하는 제품으로 발전할 가능성을 갖고 있다. 이를 위해서는 가정용 보안 게이트웨이로의 부가 서비스 제공 뿐 아니라, 향 후 음성 통신기능, 멀티미디어기능 등과 다양한 네트워크 인터페이스가 제공되어야 할 것이다.

참고문헌

[1] Roger S. Pressman "Software Engineering A Practltiners' Approach" 3rd Ed. McGraw Hill

[2] Craig M. Wittenbrick, Eric C. Rosen, Darrell D. E. Long, "Real-time System for Managing Environmental Data." Proceeding of Conference on Software Engineering and Knowledge Engineering, June 1996

[3] Theodore R. Haining, Darrell D. E. Long, Patric E. Mantey, Craig M. Wittenbrink, "The Real-Time Environmental Information Network and Analysis System(REINAS), "Proceeding of COMPCON, March 1995

[4] 이정배, 김 인홍,"원격 영상 감시 및 제어 자동화,"정보처리학회지, 1997. 7

[5] 이정배, 김용대, 박남섭, 홍영일,"웹을 기반으로 한 컨베이어 원격 제어시스템 구현에 관한 연구",한국정보처리학원, 「정보처리 '98 춘계합동학술논문발표 논문집」, 1998. 4.