# 인터넷 카메라를 이용한 침입탐지 시스템의 설계 및 구현

박대원° 김경태 이정태
부산대학교 컴퓨터 공학과
goodjob@dreamwiz.com°, ktkim@pusan.ac.kr, jtlee@pusan.ac.kr

# Implementation of Intrusion Detection System Using Internet Camera

Dae-Won Park° Kyung-Tae Kim Jung-Tae Lee
Dept. of Computer Engineering, Pusan National University

요 약

현재 정부기관이나 은행 등과 같이 침입 탐지의 보안 서비스를 필요로 하는 곳에서는 주로 CCTV(Closed Circuit TV)와 DVR(Digital Video Recording)과 같은 보안 장비들이 사용되고 있다. 하지만 이러한 장비들은 고가이므로 일반 가정이나 소규모 사업장에 이를 도입하는 것은 어렵다. 이에 본 논문에서는 CCTV나 DVR과 같은 고가의 보안 장비를 저렴하게 대체할 수 있는 인터넷 카메라를 이용한 침입탐지 시스템인 IDS(Intrusion Detection System)를 설계 및 구현하였다. IDS는 침입 탐지 보안 시스템이 기본적으로 갖춰야 하는 모니터링, 녹화, 재생, 침입 탐지 등의 기능을 제공할 뿐만 아니라 인터넷을 이용하므로 거리상의 제약점을 극복하였으며, TCP/IP를 이용한 인터넷 카메라를 사용하여 CCTV나 DVR보다 매우 저렴하게 설치 가능하다.

## 1. 서 론

최근들어 범죄 예방을 위해 CCTV나 DVR과 같은 침입 탐지를 위한 보안 장비를 사용하는 곳이 늘어나고 있다. 하지만 CCTV나 DVR은 제품의 특성상 고가이므로 도입을 위해서는 많은 비용이 요구되고, 설치 또한 쉽지 않다. 이러한 단점 때문에 일반 가정이나 혹은 소규모의 사업장에서는 필요성에도 불구하고 이러한 보안 장비를 쉽게 도입할 수 없다.

이에 본 논문에서는 TCP/IP 칩을 이용한 인터넷 카메라를 이용하여 고비용을 요구하는 기존 보안 장비들을 대체할 수 있는 침입 탐지 시스템인 IDS(Intrusion Detection System)를 설계 및 구현하였다. 본 논문에서 구현한 IDS 시스템은 기존 보안 장비에서 제공되던 모니터링, 녹화, 재생, 침입 탐지등의 기능을 제공할 뿐만 아니라 인터넷에 기반하여 기존 보안 장비들이 가지고 있는 거리상의 제약점을 해결하였다. 또한 사용되는 인터넷 카메라가 기존의 웹카메라나 CCTV용 카메라에 비해 매우 저가이므로 전체 시스템 구축 비용이 매우 저렴한 장점을 가진다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 IDS 시스템을 구현하는데 필요한 관련 연구들을 살펴본다. 이어서 3장에서는 IDS 시스템의 전체 구성과 기본 설계 에 대해 소개하고, 4장에서는 실제 구현된 IDS 시스템의 성능 평가 결과를 기술 하였다. 끝으로 5장에서 결론 및 향후 IDS 시스템에서 개선되어야 할 사항들에 대해 논의 하였다.

## 2. 관련 연구

### 2.1 JPEG(Joint Potographic Expert Group)

JPEG은 국제 표준화 기구(ISO)와 국제 전신 전화 위원회(CCITT)라는 두 기관에 의해 제안된 컬러 정지영상의 압축표준이다. JPEG은 원래 영상을 연구하는 조직의 명칭이었으나, 최근에 와서는 MPEG과 마찬가지로 영상 압축 알고리즘 표준 그 자체를 지칭한다.

기본적으로 JPEG은 영상 정보를 고주파 영역과 저주파 영역으로 분리한 후 눈에 민감한 저주파 영역은 보존하고 눈에 덜 민감한 고주파 영역은 손실 시킴으로써 원 영상의 데이터 양을 줄이는 손실 압축 방식이다. 이러한 JPEG의 압축 방식은 크게 네 가지로 나눌 수 있다[1].

- Baseline process(all DCT-based)
- Extended DCT-based processes
- Lossless processes
- Hierarchical processes

### 2.2 Change Detection

Change Detection은 일련의 프레임(frame)들의 변화에 기초하여 픽셀(pixel), 경계(edge), 영역(region)의 변화를 탐지하는 기법이다. 이러한 기법중 본 연구에서 실제로 사용한 DP(Difference Pictures) 알고리즘에 대해서 간단히 알아볼 것이다. DP 알고리즘은 간단히 다음과 같은 수식으로 표현된다[3].

$$DP_{jk}(x,y) = \begin{cases} 1 & \text{if } |F(x,y,j) - F(x,y,k)| > \tau \\ 0 & \text{otherwise} \end{cases}$$

DP 알고리즘에는 다음과 같이 크게 네 가지가 있다[3].

- Size Filter
- Robust Change Detection
- Accumulative Difference Pictures
- Difference Pictures in Motion Detection

본 논문에서는 구현이 쉬우면서도 Motion Detection에 매우 효과적인 Size Filter 알고리즘을 사용하였다[3].

## 3. IDS 시스템 설계

### 3.1 IDS(Intrusion Detection System)의 전체 구성도

[그림 1]은 본 논문에서 구현한 IDS의 전체 구성도를 보여준다.

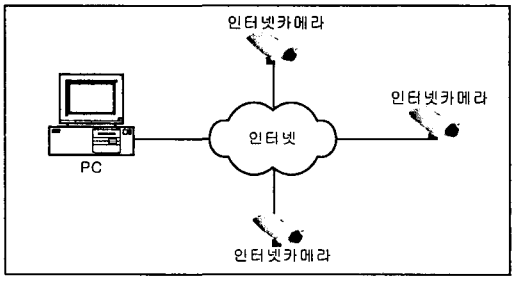


그림 1. IDS의 전체 구성도

그림과 같이 IDS 시스템은 다수의 인터넷 카메라와 보안 프로그램을 구동하는 호스트 PC로 이루어진다. 인터넷 카메라는 영상을 수집하여 접속된 PC로 전송하는 역할을 하고, PC는 모니터링, 침입 탐지, 녹화등의 기능을 제공하는 보안 프로그램을 구동하는 역할을 한다. 위와 같이 IDS는 인터넷을 기반으로 하기 때문에 장소에 관계 없이 보안 시스템을 설치 할 수 있는 장점을 가지고 있다.

### 3.2 인터넷카메라

본 논문에서 사용한 인터넷카메라는 연구실에서 기 개발된 인터넷 카메라 모듈을 이용하였다. 본 연구에서 이용한 인터넷 카메라의 특징은 다음과 같다[6].

- 저가의 인터넷 카메라
- 하드웨어로 구현된 TCP/IP 칩 내장
- 최대 4개의 채널 지원
- 초당 30프레임의 영상 압축
- TCP, IP, HTTP 등의 다양한 프로토콜 지원

하지만 기 개발된 인터넷 카메라는 단순한 영상 정보를 전송하는 기능만을 가지고 있기 때문에 보안 프로그램과 효율적인 상호 동작이 어렵다. 이를 해결하기 위해 본 연구에서는 인터넷 카메라의 펌웨어를 수정하여 [그림 2]와 같은 프로토콜로 이미지 정보를 전송하도록 수정하였다.

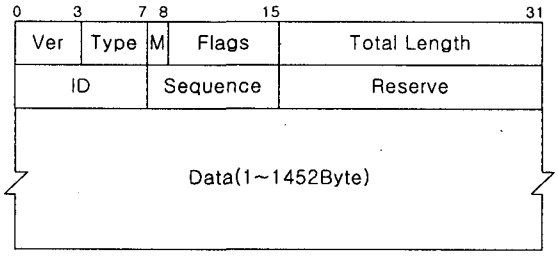


그림 2. IDS의 이미지 전송 프로토콜

"Ver" 필드는 인터넷 카메라의 버전을 나타내며 "Type" 이미지 데이터의 종류를 표시하고, "M" 필드 는 단편화 유무를 나타낸다. "Flags" 필드는 프레임의 특별한 정보 유무를 나타내고, "Total Length"필드는 데이터의 전체 크기를 나타낸다. "ID" 필드는 프레임을 구별하기 위해 사용되며, "Sequence" 필드는 단편화된 순서번호를 나타낸다. "Reserve" 필드는 향후 사용을 위해 남겨두었고, "Data" 필드는 이미지 정보로서 인터넷 카메라에 내장된 TCP/IP 하드웨어 칩의 특성을 고려하여 1~1,452 바이트의 가변 크기로 설정하였다.

### 3.3 보안 프로그램

보안 프로그램은 다수의 인터넷카메라를 효율적으로 처리하기 위하여 멀티쓰레딩 모델로 설계되었다. 따라서 보안 프로그램이 설치되는 시스템과 네트워크의 대역폭이 허용하는 범위내에서는 다중 모니터링 및 침입탐지가 가능하게 된다. [그림 3]은 보안 프로그램의 내부 구조를 블록 다이어그램으로 표시한 것이다.

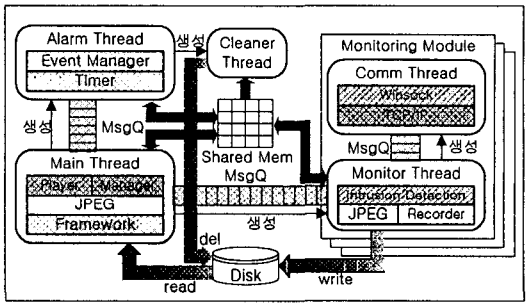


그림 3. 보안 프로그램의 구조

[그림 3]와 같이 보안 프로그램은 총 5 종류의 쓰레드로 구성된다. 이 중에서 Monitor Thread와 Comm Thread는 다중 모니터링을 위해 연결되는 인터넷카메라의 수만큼 생성된다. 각 쓰레드의 기능은 다음과 같이 요약할 수 있다.

- Main Thread : 사용자와의 interaction과 녹화된 영상의 재생을 담당한다. 또한 Alarm Thread를 생성하고 사용자의 요청에 의해 Monitor Thread를 생성한다.
- Alarm Thread : 등록된 예약작업(녹화, 침입탐지)을 처리하고, 매일 자정마다 Cleaner Thread를 생성한다.
- Cleaner Thread : Worker 쓰레드로써, 일정 보관 기간이 경과된 녹화 파일들을 삭제한다.
- Monitor Thread : 수신한 JPEG 영상을 디코드하여 화면에 출력하며, 녹화 및 침입탐지 기능을 수행한다.
- Comm Thread : 인터넷카메라와 1:1로 연결되어 전적으로 JPEG 영상을 수신하여 Monitor Thread에게 넘겨주는 역할을 담당한다.

본 연구에서 사용된 인터넷 카메라는 MJPEG 이미지를 사용한다. 따라서 녹화 및 재생 서비스를 효율적으로 제공하기 위해 AVI와 같은 표준 동영상 포멧을 사용할 경우 연산의 오버헤드로 다중 모니터링 및 녹화가 원활하게 이루어 지지 못한다. 이를 해결하기 위해 본 논문에서는 [그림 4]와 같은 IJP(Integrated JPeg) 파일 포멧을 정의하여 사용하였다.

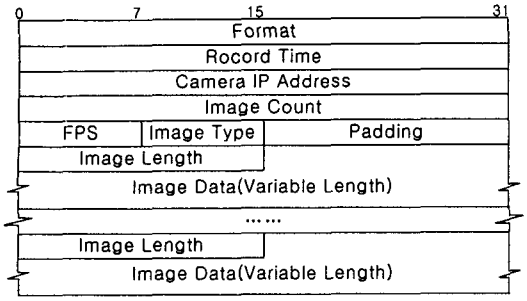


그림 4. IJP 파일 포멧

위와 같은 IJP 파일 포멧을 사용할 경우 별도의 연산없이 녹화 기능을 수행할 수 있을 뿐만 아니라 영상에 대한 추가적인 정보도 같이 저장되므로 보다 효율적인 침입 감지 서비스를 제공 할 수 있다.

## 4. IDS 시스템 구현 및 성능 측정

[그림 5]는 실제 IDS 시스템을 구동하여 원격 모니터링을 수행한 결과를 보여 준다. IDS 시스템은 원격 모니터링 외에 녹화, 재생, 침입탐지의 기능을 가지고 있다.

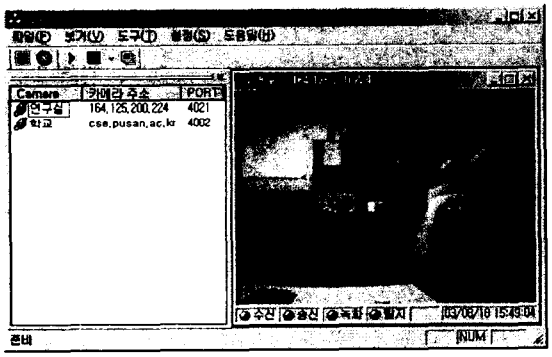

그림 5. IDS 시스템을 사용한 원격 모니터링

표 1. 수행작업별 성능 측정 결과

| 카메라 대수 | 작업종류 | 다운로드 | FPS | CPU Usage |
|---|---|---|---|---|
| 1 | M | 150kbps | 15 | 8% |
| | M, R | 141kbps | 15 | 11% |
| | M, R, I | 140kbps | 15 | 15% |
| 2 | M | 275kbps | 15 | 8% |
| | M, R | 270kbps | 15 | 12% |
| | M, R, I | 282kbps | 15 | 17% |
| 3 | M | 420kbps | 15 | 22% |
| | M, R | 412kbps | 15 | 41% |
| | M, R, I | 414kbps | 15 | 63% |

*M : Monitoring, R : Recording, I : Intrusion Detection

[표 1]은 IDS 시스템의 성능을 측정 측정 결과를 보여준다. 성능 측정은 모니터링, 녹화, 침입탐지 기능별로 네트워크 사용량과 PC의 연산량을 측정하였다. 성능측정에 사용된 네트워크는 연구실 내의 LAN망을 사용하였고 펜티엄4 2.66GHz의 PC를 사용하여 보안 프로그램을 구동하였다. [표 1]에서 보는 바와 같이 보안 프로그램은 작은 대역폭을 사용하면서도 효율적인 모니터링을 할 수 있고, 모든 기능을 사용하더라도 PC 한대당 3대 이상의 인터넷 카메라를 통한 침입 탐지가 가능하다.

## 5. 결론 및 향후 과제

본 논문은 기존의 CCTV와 DVR과 같은 침입 탐지를 위한 보안 장비가 가지고 있는 단점을 해결하기 위한 인터넷 카메라를 이용한 저가의 침입 탐지 시스템의 설계 및 구현에 관한 논문이다. 특히 연구의 결과물인 IDS 시스템은 모니터링, 녹화, 재생, 침입 탐지와 같은 기능들의 제공은 물론이거니와 기존 보안 장비들이 가지고 있는 거리상의 제약점을 해결하였으며 저렴한 가격으로 설치가 가능한 장점이 있다. 또한, 기존 보안 장비들의 정적인 화면 구조 대신 동적인 화면 구조를 채택하여 효율적인 모니터링이 가능하다.

향후 과제로는 침입 탐지 기능이 수행될 때마다, 보안 프로그램의 CPU 사용량이 많이 증가하는데, 이는 침입 탐지를 위해 사용하는 DP 알고리즘의 많은 비교 연산으로 인하여 발생하는 현상이다. 따라서 이 부분의 문제점을 해결하기 위해 효율적인 알고리즘을 설계하여 구현할 예정이다.

### 참고 문헌

[1] ITU Org., "Digital Compression and Coding of Continuos-Tone Still Images □ Requirements and Guidelines", Sep. 1992.

[2] John Miano, "Compressed Image File Formats", Addison Wesley, 1999.

[3] Ramesh Jain, "Machine Vision", McGraw-Hill, 1995

[4] W. Richard Stevens, "TCP/IP Illustrated Volume 1", Addison Wesley, 1994.

[5] W. Richard Stevens, "Unix Network Programming Vol.1", Prentice Hall, Jan. 1998.

[6] Wiznet Inc., "IICam User's Manual V1.0", 2002

[7] Intel Inc., "IJL Developer's Guide V1.5", 2001.

[8] 이상엽, "Visual C++ Programming Bible 6.x", 영진출판사, Nov. 1998

[9] 김상형, "Windows API 정복", 가남사, Jan. 2001.

[10] 공인엽, "동적 IP를 이용한 웹 기반 영상 모니터링 시스템의 설계 및 구현," 부산대학교, Feb. 2002.