情 報 保 護 學 會 誌
第20卷 第3號, 2010. 6

분산 스마트 카메라 시스템 보안 이슈

류 대 현*, 한 종 욱**, 조 현 숙**

요 약

영상 보안 시스템은 다양한 영역에서 그 중요성이 부각되고 있으며 보통 공적 공간 및 사적인 환경에 사용되므로, 민감한 정보나 개인 정보에 접근하거나 정보의 조작에 대한 우려가 높아지고 있다. 최근 영상 보안시스템은 분산 스마트 카메라로 발전하고 있으며 이들의 보안 문제는 네트워크 임베디드 시스템 및 센서 네트워크의 경우와 유사한 점이 있지만 개인 정보 보호 및 실시간 동작 등 스마트 카메라 네트워크만의 특별한 요구도 있다. 이러한 영상 보안 시스템의 보안 문제는 전체적인 시스템 구조의 설계에서부터 보안과 개인정보보호 이슈를 고려해하여야만 이러한 문제들을 해결할 수 있다. 본 논문에서는 현재의 영상 보안 시스템의 보안 및 개인 정보 보호 문제를 다룬다. 영상 보안 시스템의 일반적인 보안 위험, 노드에서 문제를 분석하고 네트워크 수준에서 사용 가능한 솔루션을 제시하고 보안 요구 사항, 가능한 공격을 설명한다.

I. 서 론

CCTV(Closed Circuit Television)는 일정한 공간에 설치된 촬영기기를 통해 수집한 화상정보를 폐쇄적인 유/무선 전송로를 통하여 전송 후 특정인만이 수신할 수 있는 통신장비 일체를 일컬어 말한다[1].

CCTV는 디지털로의 진화 외에도 별도의 동축케이블 대신 인터넷을 이용함으로써 경제적이고 효율적인 분산형 시스템을 구현할 수 있는 네트워크 카메라로도 발전하고 있다. 최근에는 이와 같은 네트워크가 연결된 IP 카메라의 설치가 증가하면서 양방향 음성서비스나 움직임 감지, 폭발물 감지 등의 지능형 부가서비스도 활성화되고 있다. 따라서 IP 카메라 또는 네트워크 카메라 또는 스마트 카메라 등의 용어가 혼용되고 있으며 본 논문에서는 문맥에 따라 이들 용어를 혼용하되, 분산 스마트 카메라(Distributed Smart Camera)[5]라는 용어를 주로 사용한다.

한편, 공공성 등의 목적으로 설치되는 CCTV의 수가 급격히 증가하고 있으나, 사생활 침해와 같은 역기능 문제가 대두되고 있어, 이를 해결하기 위한 영상보안기술 개발이 필요하다. 향후 범죄를 예방하고 범법자를 색출하기 위한 감시산업의 규모가 커지게 되며 테러의 급증으로 감시공학 분야가 각광을 받을 것이다. 따라서 CCTV로 인한 역기능 문제 해소를 위해서는 관련 가이드라인 및 법안을 만족하면서 순기능을 강화할 수 있는 보안 기술의 도입이 필수적이다[2][3].

분산 스마트 카메라 시스템은 감시 분야에 주로 사용되는데 보통 개인 정보보호를 포함해서 엄격한 보안 요구 조건을 요구한다. 그 결과, 스마트 카메라 시스템 보안 자체가 전체적인 아키텍처의 설계에 중요한 요소가 된다. 한편, 분산 스마트 카메라 시스템은 분산 시스템들을 구성하며 계산적 능력이 뛰어난 센서 네트워크로 볼 수 있다. 따라서 스마트 카메라 시스템의 보안은 노드 레벨 보안 및 네트워크 레벨 보안 모두를 고려하여야 한다. 노드 및 네트워크 레벨 양쪽에서 보안 요구 사항은 적절한 데이터 보호 기능을 제공해야 한다. 따라서 모든 계층에서 인증 프로토콜 및 데이터 무결성 제어를 구현 할 수 있도록 하고, 이에 따라 데이터 비밀성 및 인증을 보증하게 된다. 또한 분산 스마트 카메라 시스템은 직접 공격, 부채널 공격 그리고 서비스 거부(DOS) 공격들을 포함하는 모든 종류의 공격에도 대응할 수 있어야 한다[6].

* 한세대학교 IT학부 (dhryu@hansei.ac.kr)
** 한국전자통신연구원 (hanjw@etri.re.kr, hscho@etri.re.kr)

본 논문에서는 분산 스마트 카메라 시스템과 관련된 가장 중요한 보안 이슈들에 대해 설명한다. 계층적 접근을 통하여 노드 레벨 네트워크 레벨 아키텍처 모두에서의 핵심 보안 요구 사항을 확인하고, 적절한 아키텍처를 제시하고자 한다.

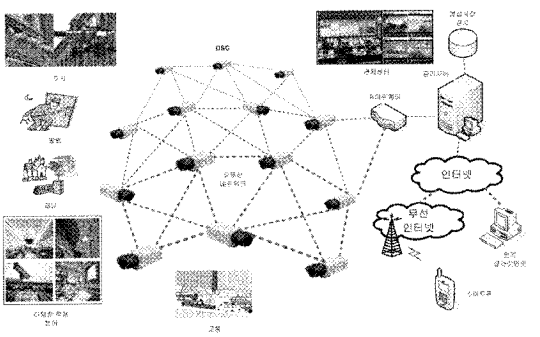
본 논문은 다음과 같이 구성되어 있다. II장은 분산 스마트 카메라 시스템 아키텍처를 보안 요구 사항에 초점을 맞추어 분석한다. III장은 분산 스마트 카메라 시스템이 충족해야 하는 보안 요구 사항을 소개한다. IV장은 스마트 카메라 노드 보안을, V장은 네트워크 보안을 다룬다. 마지막으로, VI장은 본 논문의 결론이다.

Ⅱ. 분산 스마트 카메라 시스템의 구조

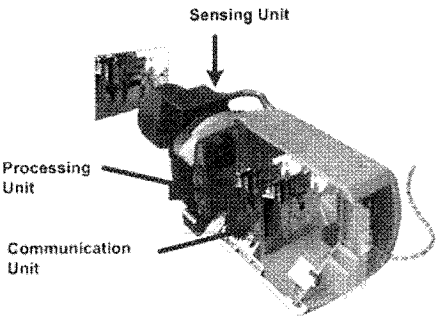
스마트 카메라 시스템의 보안 분석을 위해서는 아키텍처 특성[5], 특히 보안에 관계된 특성의 세부 사항을 이해할 필요가 있다. 분산 스마트 카메라 시스템은 일반적으로 노드들로 구성되어 있다고 볼 수 있는데, 노드에 해당하는 스마트 카메라 자체가 네트워크 인프라로 상호 연결되어 있다. 아키텍처에 따라 시스템은 완전히 분산되어 있거나 또는 일정 부분 중앙 제어가 가능하도록 되어 있다. 본 논문에서는 분산 스마트 카메라 시스템의 일반적인 아키텍처를 고려하면서 그림 1의 시스템 모델에 기초하여 분석한다.

2.1 분산 스마트 카메라 하드웨어 구조

본 논문에서 일반적인 스마트 카메라 노드 아키텍처는 전원 유닛, 센서 유닛, 처리 유닛 그리고 통신 유닛으로 구성된 모델로 생각한다. 모든 이들 유닛은 하나의



〔그림 1〕 분산 스마트 카메라 시스템의 개념



〔그림 2〕 일반적인 스마트 카메라 노드 아키텍처

임베디드 장치로 구현될 수 있다.(그림 2)

전원 유닛은 필요한 노드에 필요한 전력을 공급하는 하부시스템이다. 동작 전력은 전력선으로 부터 끌어 오거나 주변 환경에서 만들어낼 수도 있다. 전원 유닛의 작동은 특히 에너지 자원이 제한되고 충분한 에너지 관리가 필요한 경우에 매우 중요하다. 센서 유닛은 물리적 세계에서 사건의 영상을 디지털 정보로 변환하는 하부 시스템이다. 센서 유닛은 CMOS 센서와 같은 빛에 민감한 디지털 센서와 광학 렌즈 시스템으로 구성되는데, 데이터 량이 많은 비디오 신호를 캡처하여 처리 유닛에 제공하는 기능을 수행한다. 처리 유닛은 디지털 신호 처리(DSP) 기능을 수행하는 하부 시스템인데 캡처된 비디오 자료를 분석하고 처리하는 스마트 카메라의 심장이라고 할 수 있다. 처리 유닛의 출력은 캡처된 비디오에 대한 디지털 처리 결과이거나 비디오 신호가 노드 외부로 전송되는 경우에는 비디오 신호 자체가 될 수 있다. 마지막으로, 통신 유닛은 모든 통신 기능을 수행하는 하부 시스템으로 이 유닛은 동기 및 제어 신호뿐만 아니라 스마트 카메라가 처리하는 정보를 송수신한다.

2.2 스마트 카메라 소프트웨어

스마트 카메라 노드에는 처리 테스크, 통신 테스크 그리고 제어 테스크와 같은 3개의 중요한 소프트웨어 테스크가 구현된다. 처리 테스크는 시스템의 핵심부에 해당하는 디지털 신호처리 기능을 포함한다. 이 테스크는 쌍 또는 그룹으로, 노드가 겹치는 지역에서 동작하거나 동일한 기능을 보조 처리하는 등, 상호 협력할 수 있도록 스마트 카메라 노드에 분산될 수 있다. 통신 테스

크는 통신 유닛에 할당되어 자체적으로 또는 중앙 제어 시스템과 통신하는 노드들과 관련된 모든 과정을 수행한다. 제어 테스크는 핵심 소프트웨어라고 볼 수 있는데, 처리 또는 통신유닛에 할당되어 다른 테스크를 시동시키고 동기화한다.

2.3 분산 스마트 카메라 네트워크

분산 스마트 카메라 시스템의 네트워크 아키텍처는 광범위한 상호 연결 기술, 토플로지, 프로토콜 등을 적용하고 있다. 일반적으로, 스마트 카메라 네트워크는 에드 혹(ad hoc) 네트워크와 많은 유사성을 가지고 있지만 노드가 다른 노드와 통신할 필요가 없는 경우가 많다. 또한 코 모니터링 또는 코 프로세싱을 위하여 쌍 또는 그룹으로 된 노드가 형성될 수 있다. 일반적으로 스마트 카메라 네트워크는 무인의, 공공의, 그리고 열악한 환경에서 동작한다고 가정한다.

스마트 카메라 네트워크의 노드에 있는 프로토콜 스택은 OSI 참조 모델과 유사한 4개 계층 즉, 물리계층, 데이터 링크 계층, 네트워크 계층 그리고 응용 계층으로 구성된다. 네트워크의 물리 계층은 유선 또는 무선 방식으로 가능하다. 스마트 카메라에 구현에서는 보통 유선 방식을 적용하는 것이 일반적이다. 최근 무선 기술이 크게 발전하고 있으므로 무선 기술의 적용이 가능하지만 보안상 해결 되어야할 많은 문제가 있다. 데이터 링크 계층은, 매체 접근 제어(medium access control) 하부계층을 포함하는데, 보안 스마트 카메라 통신에 매우 중요한 역할을 한다. 데이터 링크 계층은 매체 접속 제어 및 오류 탐지를 담당할 뿐만 아니라 암호 통신의 기반을 형성한다. 이 계층은 노드 수가 증가하면서, 네트워크에 대한 공정하고 일관성 있는 접속의 필요성과 함께 스마트 카메라 네트워크 운영에 있어서 매우 중요한 역할을 한다. 스마트 카메라 네트워크의 아키텍처에서 네트워크 계층은 분산 네트워크와 유사한데, 노드는 종단 장치로써 동작할 뿐만 아니라 또한 다중 호핑 통신 경로에서 라우터로서 동작할 수 있다. 모든 노드는 그 위치가 식별되며 쌍 또는 그룹 및 하부그룹으로 분리될 수 있으나 통상 글로벌 어드레싱은 불필요하다.

서비스 품질(QoS)은 영상의 모니터링이 필요한 경우, 다양한 QoS 수준 및 우선순위 수준(서비스 등급)의 동적 재배정에 대한 요구와 함께 매우 중요하다. 스마트 카메라 네트워크의 응용 계층은 노드 간 협력뿐만 아니라 네트워크의 분산, 테스크 관리 및 배분을 다룬다.

2.4 최근 기술 동향

일반적으로 스마트 카메라 시스템 구현 시, 범용 CPU 또는 멀티미디어 용으로 설계된 DSP를 사용한다. 기존의 스마트 카메라 시스템은 1 GHz 이상 클럭의 프로세스를 사용하여 강력한 계산 능력을 가지고 있으며, 보통 수 백 메가바이트까지의 메모리를 사용하고 영구 저장 장치로 플래시 메모리를 적용한다. 스마트 카메라 시스템 구성 요소들은 보통 시스템 버스, 혹은 PCI를 통해서 연결된다. 네트워킹 방법은 보통 유선 또는 무선 랜 형태의 이더넷 연결을 적용한다.

스마트 카메라 노드에서 리눅스 운영 체제가 많이 사용되는데 리눅스의 임베디드 버전은 제한된 자원을 잘 관리하고 실시간성이 우수하며, 프로그램 개발에 있어서 다양한 선택 사항을 제공한다. 또한, 리눅스 운영체제는 소프트웨어 개발을 용이하게 해주며 하드웨어 구성 요소에 대해 기존의 코드도 사용할 수 있도록 한다.

일반적으로 DSP는 그 DSP 칩에 특정한 소프트웨어를 개발하는데 사용되는 특정 소프트웨어 프레임워크와 함께 운영된다. 범용 CPU가 제어 프로세서로 사용될 때는 범용 툴을 사용하여 소프트웨어를 개발하는 것이 가능하다. 소프트웨어는 C/C++ 언어로 직접 작성되거나 다른 플랫폼으로부터 포팅해서 사용하는 것도 가능하다.

연구 목적의 스마트 카메라 프로토타입은 다양한 용도 사용할 수 있도록 개발되고 있다[4][7][8]. 보안 이슈는 아직 본격적으로 연구된 적은 없다. 최근까지도 주로 알고리즘 처리, 멀티미디어 처리와 같은 스마트 카메라 주기능에 초점을 맞추어져 있으므로, 이전에 개발된 스마트 카메라 네트워크 동작에 대한 보안 평가는 아직 이루어져있지 않다.

Ⅲ. 분산 스마트 카메라 시스템 보안 요구 조건

분산 스마트 카메라의 보안 요구 조건은 일반적인 네트워크 시스템의 보안 요구 조건에 대한 고려 사항을 포함하고 있다. 분산 스마트 카메라 시스템에서는 정보는 카메라 내에서 처리될 뿐 아니라 네트워크로 전송된

다. 스마트카메라 네트워크는 보안상 민감한 데이터를 처리하므로 안전한 통신과 프라이버시가 동시에 고려되어야 한다. 본 절에서는 분산 스마트 카메라의 보안 요구 조건을 제시한다.

3.1 데이터 기밀성(Data Confidentiality)

데이터 기밀성은 일반적으로 도청에 대한 정보의 보호를 의미하는데, 암호기술, 암호화, 복호화 등을 필요로 한다. 이러한 암호화, 복호화는 복잡한 연산을 필요로 하므로(resource-demanding) 스마트 카메라의 리소스, 암호 알고리즘의 복잡성, 정보의 중요도(보안 민감성)등이 고려되어야 한다. 특히 이동 코드(mobile code)나 제어 신호(control signal)에 대해서는 높은 수준의 암호를 필요로 한다.

3.2 데이터 무결성(Data Integrity)

데이터 무결성은 노드에서 전송된 데이터가 다른 노드에 의해 변경되지 않고 수신되었다는 것을 의미한다. 여기서 변경이라는 의미는 일반적인 전송 에러는 해당되지 않고 데이터를 변경하기 위한 의도적인 개입을 했을 경우에 해당된다. 제 3자(third party)가 복호화된 데이터에 접근하지 않고 노드 간에 교환되는 데이터를 변경하는 것이 가능하다는 점에서 데이터 기밀성과는 구별되는 보안 요구 조건이다.

3.3 데이터 선명성(Data Freshness)

데이터 선명성은 악의적인 자가 기 전송된 데이터를 재전송하는 것을 검출하는 기술을 필요로 한다. 다양한 데이터 선명성 메커니즘(data freshness mechanisms)을 적용할 수 있겠지만 기존의 네트워크 동기 메커니즘을 이용할 수도 있다. 또한 시간, 날짜, 노드 데이터 등의 정보를 영상에 삽입하는 디지털 워터마킹 기술을 적용함으로서 데이터 선명성을 확보할 수도 있다.

3.4 피어 인증(Peer Authentication)/안전한 네트워크 접근(Secure Network Access)

분산 스마트 카메라 시스템에 있어서 인증되지 않은 노드를 삽입하여 시스템을 사용하는 것을 방지하기 위해서는 네트워크에 연결된 각 노드는 인증 과정을 필요로 한다. 그런데 분산 스마트 카메라 시스템이 동작 중에 노드 또는 네트워크 토플로지의 삽입, 제거 그리고 수정이 이루어 져야한다는 점을 고려하여 인증 메카니즘이 구현될 필요가 있다.

3.5 가용성(Availability)

DoS 공격은 일반적인 형태의 공격로서 과도한 트래픽이나 서비스 요청으로 네트워크의 정상적인 동작을 방해한다. 스마트 IP 카메라 시스템은 실시간 동작이 요구되므로 이러한 DoS 공격을 방어하거나 진단하는 메커니즘이 매우 중요하다.

3.6 개인 정보 보호(Privacy)

분산 스마트 카메라 시스템은 사람의 얼굴, 자동차 번호판, 주거 지역의 영상 등 민감한 정보를 처리하므로 데이터 기밀성에 대한 요구 뿐 아니라 프라이버시에 대한 요구가 존재한다. 스마트 IP 카메라 시스템에서는 정보의 비트 스트림 자체가 보호되어야 할 뿐 아니라 개인 데이터 같은 정보 자체의 실제적인 값도 보호해야 한다. 이러한 프라이버시 정보는 합법적인 운영자나 관리자에 대해서도 보호되어야할 필요가 있다.

일반적으로 영상이 스마트 카메라 외부로 전송되지 않도록 하는 방식도 생각할 수 있지만 선택적 전송이나 저장이 필요한 경우가 있다. 뿐만 아니라 전송 데이터의 선택적 또는 다단계 암호화를 통해 사용자의 보안 레벨에 따라 데이터에 접근 권한을 다르게 할 필요도 있다.

3.7 템퍼 레지스턴스(Tamper Resistance)

분산 스마트 카메라는 공공 장소 또는 옥외에 설치되는 경우가 많으므로 도난 되어 잠재적 공격자의 수중에 들어갈 가능성이 있다. 따라서 스마트 IP 카메라의 일부 또는 전부가 공격자의 수중에 들어가더라도 보안성을 가질 수 있도록 템퍼 레지스턴스 기능을 필요로 한다. 그러나 이러한 템퍼 레지스턴스 기능은 많은 비용이 소요될 수 있으므로 일부 취약한 노드에만 적용하는 등 예산을 고려하여야 한다.

뿐만 아니라 물리적 공격 또는 부채널 공격에 대해서도 대비가 있어야 한다. 부채널 공격(side-channel attack)은 타이밍 정보나 전력 분석 등 시스템의 물리적 구현 레벨에서의 정보 유출을 이용하는 방식이다. 물리적 공격은 배터리를 방전 시키거나, 비디오 화질에 영향을 주도록 시스템의 물리적 리소스를 공격하는 방식이다.

분산 스마트 카메라의 보안을 위해서는 전체적이고 레벨 상호간의 보안 계획(overall, cross-level security plan)이 필요하다. 또한 모든 요구조건을 전체적으로 다루어야 할 뿐 아니라, 각 요구 조건을 분리해서 다룰 필요가 있다.

Ⅳ. 노드 보안

이 장에서는 스마트 카메라 노드와 관련된 보안 이슈를 소개한다. 상호 연결된 스마트 카메라 노드를 만드는 첫 단계는 안전한 노드를 설정하는데서 부터 시작된다. 먼저 스마트 카메라 노드의 특성과 제한 사항을 이해하고, 노드의 능력과 제한사항을 고려하면서 통신 보안성을 제공하는 네트워크를 설계할 필요가 있다. 스마트 카메라 노드 보안은 임베디드 시스템 보안이라는 문맥으로 해석될 수 있다. 앞에서 언급 하였듯이 노드는 공격에 대해 여러 가지 취약점을 나타낼 수 있으며 처음부터 보안 고려사항을 가지고 설계될 필요가 있다. 이미 설계된 시스템에 보안 기능을 추가하는 것은 매우 어렵기 때문이다.

스마트 카메라 노드는 보통 공공 장소에 설치되며, 식별 및 접근이 용이한 경우가 많다. 따라서 이에 대한 보안 요구 조건은 매우 다양하며 엄격하다. 우선 각 노드에 사용된 프로세스 및 모듈은 보안 기능이 있는(security enabled) 시스템일 필요가 있다. 에드온(add-on) 구성요소로 하드웨어 보안 표준을 구현하기는 어려우므로 이렇게, 적용된 모든 기본 구성 요소는 설계 단계에 보안을 고려할 필요가 있다.

4.1 템퍼 레지스턴스, 물리적 공격, 부채널 공격

템퍼 레지스턴스는 앞에서 언급한 것처럼, 공격자에게 탈취 되더라도 보안을 유지하기 위한 장치의 기능이다[9]. 이 기능은 일반적으로 많은 비용이 소요되므로 모든 스마트 카메라 노드에 반드시 적용해야하는 것은 아니다. 그러나 가능한 안전하게 관리해야 하는 베이스 스테이션과 같은 특별한 노드에는 반드시 적용될 필요가 있다. 일반적으로 베이스 스테이션과 같은 중요한 노드는 템퍼링에 대해 안전한 제한된 환경에 설치되어 있어야 하지만, 본 논문에서는 이러한 특별한 노드가 불안전한 환경에 존재할 수 있다고 가정한다. 다음 장에서 설명되겠지만 이러한 특별한 노드는 정보를 통합하거나 암호 키 분배를 지원하는 경우도 있다.

접근 가능하거나 남의 수중에 들어간 시스템을 템퍼하는 데는 여러 가지 방법이 있는데 우선, 노드에 대한 물리적 공격이 가능하다. 노드의 물리적 조작은 전자기 간섭과 같이 즉각적 물리적 접촉을 요구하지 않는 공격뿐만이 아니라 센싱 기능에 영향을 주거나 정보를 얻기 위하여 노드의 특정 부분에 접근하도록 침입하는 것도 포함한다. 이러한 물리적 공격은 소프트웨어 기술뿐만 아니라 특수 설계된 하드웨어를 사용하여 탐지할 수 있다. 예를 들어 노드 내부에 침입이 감지되거나 센싱 데이터에서 비정상 패턴을 탐지하였을 때 시스템을 제대로 동작하지 않도록 하는 하드웨어나 비정상 패턴을 탐지하는 소프트웨어 등이 있을 수 있다. 물리적 공격은 대부분의 경우 사후 대응이 어렵기 때문에 이에 대한 전략은 사전 검출 또는 분석하는 것이어야 한다. 물리적 공격이 존재하는 경우에는, 노드가 공격자에게 민감한 정보를 노출하거나 잘못된 정보를 송신할 수 있는 상황에 놓이게 되므로 계속 작동하는 것 보다는 오히려 작동을 멈추는 것이 더 낫다.

앞 장에서 설명한 하드웨어 구성요소 중, 전원 유닛과 센싱 유닛에 특별히 유의해야 한다. 많은 물리적 공격은 배터리 소모와 같은 에너지 자원을 목표로 전원 유닛을 공격한다. 또한, 센싱 유닛은 특수 설계된 빛 방출 또는 다른 물리적 장애물 이용하여 감광성 센서에 피해를 주거나 혼란시키는 공격과 같은 물리적 공격에 취약하다. 프로세싱 부에서 작동하는 DSP 소프트웨어는, 비슷한 패턴을 녹화하는 같은 노드 그룹과 같이 녹화된 이미지에서 비정상 패턴을 탐지하고 제어할 수 있어야 한다.

부채널 공격은 물리적 시스템에서 추가적이고, 대규모의 공격으로 구성된다. 예를 들어, 타이밍 분석에서, 암호 수행 걸리는 시간과 암호 키 값 사이의 연관성 찾는데는 통계적 방법이 사용된다[10]. 스마트 카메라 환경

에서, 이러한 공격은 노드에 저장된 키를 찾는데 사용될 수 있다. 또다른 부채널 공격은 전력에 대한 공격인데, 타이밍 공격과 동일한 원리가 적용되지만 이 경우에는 회로에서 흘러나오는 전류를 분석 파라메타로 사용한다. 또한, 전자기 분석 공격이 시도될 수 있는데, 이것은 장치의 특정 부분에서 방출한 전자기파를 측정함으로써 비밀 정보를 찾는 방법이다. 마지막으로, 저장 용량에 제한은 있지만 노드는 암호 키나 추후 송신하기 위해 수집된 자료와 같은 정보를 저장할 필요가 있기 때문에, 노드의 유실에 대비하여 노드는 자료 검색을 사실상 불가능하게 하는 안전한 저장 메커니즘, 예를 들어 암호화된 저장장치 등을 사용하여야 한다.

4.2 소프트웨어 이슈

스마트 카메라 노드에서 작동하는 소프트웨어는 점점 더 복잡해지고, 이 복잡성이 잠재적인 취약점을 발생시킬 수 있다. 스마트 카메라는 복잡한 비디오 처리 작업을 수행하고 이에 따라 프로그램 사이즈도 커지고 복잡해진다. 성능 향상은 중요한 목표지만, 스마트 카메라의 어플리케이션 개발에 있어서 성능이 모든 것을 해결해 주지는 않는다.

버퍼 오버플로우 등과 같은 일반적인 공격에 대한 효율적 보안 메커니즘을 제공하는 소프트웨어 플랫폼을 선택할 필요가 있다. 대부분 임베디드 시스템은 C/C++ 환경을 바탕으로 개발되는데[11], 이것은 매우 효율적이지만 이러한 공격에 대해서는 그다지 안전하지는 않다.

스마트 카메라 네트워크처럼 바이러스 또는 트로이 목마와 함께 가능한 소프트웨어 공격이 다수의 노드에 퍼질 수 있는 네트워크화 된 환경에서 안전한 프로그래밍에 특별한 주의를 기울이는 것이 매우 중요하다.

스마트 카메라 노드에 있어서 사전에 프로그램 된 노드를 사용하고 재 프로그래밍(업데이트 등의 목적으로) 기능을 제한함으로써 보안 위험을 현격히 감소시킬 수 있다. 그러나 실제로, 스마트 카메라 노드는 모바일 코드[12]를 사용하여 작동 중 성능을 업데이트하고 재 프로그래밍 할 필요가 있다. 이러한 기능은 노드에서 실행되는 테스크를 수정하고, 버그를 수정하거나, 노드 소프트웨어의 최신버전을 설치하는 등의 서비스를 제공한다. 이 부분이 스마트 카메라 노드에 가장 중요하면서도 가능성 있는 취약점인데, 이 과정에서 시스템의 주요 부분을 부작동 또는 불안전하게 하는 악성 소프트웨어 실행을 가능하게 하기 때문이다. 다음 장에서 설명하겠지만 모바일 코드의 통신은 연계되어야 하고 노드 능력 범위에서 가장 강력한 암호 프로토콜을 적용해야 한다. 노드 내부에는, 코드 서명 등과 같은 안전한 코드를 인식하는데 사용할 수 있는 기술들이 적용된다[13]. 모바일 코드의 사용에 따른 취약점을 최소화하기 위한 다른 선택사항은 심각한 보안 위험이 없는 소프트웨어 부분에만 모바일 코드를 사용하도록 제한하는 것이다. 이 기술은 모바일 코드를 필수 시스템 구성 요소에서 분리시켜 놓는 방법을 사용해서 구현될 수 있다. 이런 방법을 사용하면, 필수 시스템 소프트웨어는 업데이트 될 수 없고 주 시스템 서비스에서 분리된, 일반적인 테스크 만이 모바일 코드를 통해 접근될 수 있다.

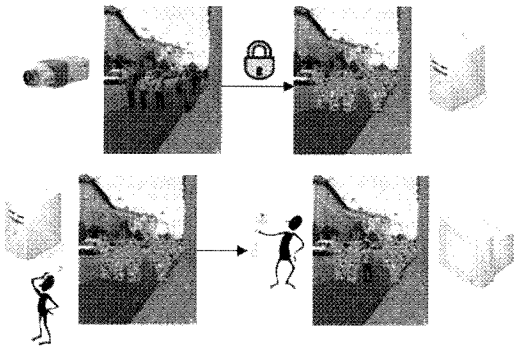
4.3 개인 정보 보호

스마트 카메라 네트워크는 사람들을 모니터 하거나 민감한 정보를 수집하는데 사용될 수 있으므로 개인 정보 보호 이슈는 매우 중요하다. 가능한 공격으로 부터 개인 정보 보호가 침해되지 않도록 해야 하지만, 시스템의 합법적 사용자로부터도 개인 정보 보호가 침해되지 않도록 해야 한다. 가능한 공격자로부터 개인 정보를 보호하는 데는 두 가지 방법이 있을 수 있다.

노드 간 통신에 암호를 사용하거나, 어떤 통신이 누설된 경우에 개인 정보 보호 침해에 대한 효과를 낮출 수 있도록 교환되거나 기록된 정보의 양을 최소화 함으로써[14] 개인 정보를 보호할 수 있다. 이러한 접근방법은 다른 방법과 같이 구현할 수 있는데, 각 노드가 송신하는 정보를 시스템 운영의 절대 최소량까지로 제한함으로써 가능하다.

스마트하고 효과적인 알고리즘은 노드-내 처리(in-node processing)를 증가하고 기록된 정보를 적게 취합 것을 목표로 구현될 필요가 있다. 그러나 많은 경우 있어서 비디오 신호 자체가 노드에서 전송되어야만 하는 경우가 있다.

영상보안 시스템의 설치 및 운용에 있어 가장 중 요한 이슈는 사생활 침해방지 및 프라이버시 보호의 문제일 것이다. 보안감시를 주목적으로 하는 영상보안 기술은 프라이버시 침해라는 역기능으로 인하여 설치, 운영에 관한 법적 기준의 마련 및 준수가 중요한 요소로 부



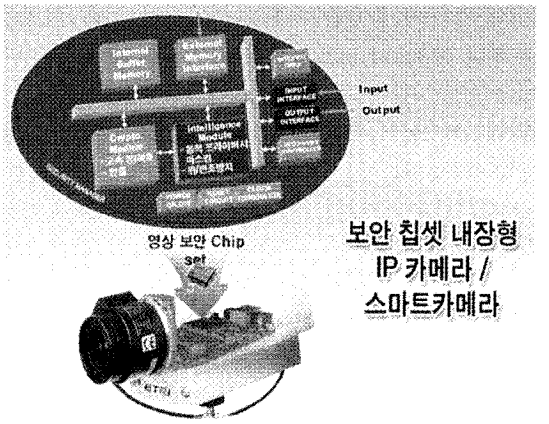
〔그림 3〕 프라이버스 마스킹의 예

각하였다. 선진 각국은 영상보안 시스템의 설치, 운영을 위한 사생활과 프라이버시 침해에 대응하기 위한 관련 법규를 제정하고 있는 추세이다. 또한 기술적으로는 획득된 영상정보에서 얼굴을 모자이크 처리하거나 추출된 사람을 암호화하여 저장하고, 필요한 경우에만 허가된 사람에 한하여 검색할 수 있는 권한을 부여하는 기술 등을 개발하고 있다.

그러나 이러한 기술들은 배경과 사람의 분리를 전제로 하고 있어 성능상의 한계 및 높은 하드웨어 비용을 필요로 하고 있다. 따라서, CCTV/DVR기반의 영상보안 기술에 적용하기에는 한계를 가지고 있다. [그림 3]은 영상감시 시스템 프라이버시 보호 기술의 한 예를 보여주고 있다.

예를 들어, 스마트 카메라는 어떤 특별 요구사항이 충족되거나[15] 어떤 특별한 사건이 탐지될 때, 영상의 저장을 위해서 베이스 스테이션에 특정 비디오 신호를 송신할 수 있다. 비록 이 경우 전송 데이터가 암호화 되었더라도, 그것은 여전히 보통 전송된 비디오에 일상적으로 접근하는 시스템 운영자와 관련된 개인 정보보호 침해 위험은 존재한다.

이 문제에 대한 해결책은 사람들의 얼굴과 같은, 적절한 이미지 부분을 인식하여 선택적으로 암호화하는 것이다[16]. 이러한 방법에서 선택된 이미지 부분은 1 급 키를 사용하여 암호화 될 수 있으며 2 급 키는 전체 신호를 암호화 하는데 사용된다. 즉 2 급 키만을 가지고 있는 사람들은 민감한 이미지 부분에 접속할 수 없다. 높은 우선권을 가지는 사용자에게만 가용한 1급 키는 필요시 전체 신호를 해독하기 위하여 사용될 수 있다. 이 방법을 조금 더 엄격하게 적용한다면, 민감한 정보는



〔그림 4〕 보안 칩셋 내장형 스마트 카메라

암호화되는 대신 영구적으로 삭제될 수도 있다.

몇몇 디지털 저작 관리(DRM) 프로토콜 및 방법들은 통상 디지털 소비자 시장에서 오디오 및 비디오에 접근을 제한한다[17]. 비록 그 적용 범위가 분산 스마트 카메라 네트워크와는 완전히 다르지만, 암호화된 동영상에 대한 필요성, 사용자 별 라이센스 그리고 일회성 라이센스처럼 많은 유사성이 존재한다. 기존의 DRM 프로토콜은 적절히 보완하고 조정한다면 감시시스템, 특히 운영 요원이 시스템과 상호 작용하는 응용에서, 개인 정보보호 침해를 방지하는데 적용될 수 있다.

V. 네트워크 보안

노드 간의 통신 보안, 또는 네트워크 보안은 일반적으로 암호화 프리미티브를 사용하여 구현된다. 전통적인 네트워크 시스템에서, 강력한 암호화 방법은 고도의 보안성을 제공한다. [그림 4]는 ETRI에서 개발한 보안 칩셋 내장형 스마트 카메라의 블록도를 나타내고 있다.

그러나 제한된 처리 능력을 가지며 네트워크 자원이 효과적 보안 아키텍처를 요구하는 네트워크된 임베디드 시스템에서의 상황은 더욱 복잡해진다. 일반적인 스마트 카메라 네트워크는 센서 네트워크와 많은 유사성을 공유하지만, 일부 차이가 존재한다. 이러한 차이점에는 적은 수의 스마트 카메라 네트워크 노드, 보다 많은 가용한 하드웨어 자원, 그리고 스마트 카메라 네트워크에서는 정보량이 매우 큰 비디오 자체를 센싱 한다는 사실 등이 있다. 예를 들어, 거리 교통을 모니터하는 스마트 카메라 네트워크의 경우, 노드 수는 비교적 적고(센

서 네트워크에 존재할 수 있는 수백 또는 수천 개 보다는 훨씬 적음), 각 노드는 녹화된 이미지에서 발전된 비디오 분석을 할 수 있을 정도로 강력할 필요가 있다. 센서 네트워크에서 보안 이슈에 대한 세부 분석은[18]에 잘 설명되어 있다.

5.1 키 관리 전략

노드 간의 암호화 통신에 있어서 암호화 및 인증을 위해서는 적절한 암호화 키를 노드로 분배하는 것이 필요하다[20]. 키 분배 전략은 암호 통신을 위한 매우 중요한 첫 단계인데 키 분배가 안전한 통신을 위한 기반을 형성하기 때문이다. 키가 안전하게 셋업 되면 통신의 보안성을 획득할 수 있다고 볼 수 있다.

어떤 암호화 방법을 적용할 것 인가가 보안 수준 뿐만 아니라 통신 및 처리 비용을 결정하므로 효율적인 전략을 따르는 것이 필요하다. 공개 키 암호화[20]는 계산량이 많은 즉 고비용의 방법이지만 노드 간 통신을 암호화 하기위한 효과적인 방법이다. 일반적인 임베디드 시스템 능력을 고려할 때, 공개키 암호화는 스마트 카메라 노드, 특히 노드별로 한 개의 키를 사용할 때, 많은 수의 키를 요구하는 거대한 네트워크의 처리 능력을 넘어선다. 반면, 타원 곡선 암호화는 매력적 대안으로, 강력한 보안성과 낮은 계산 비용을 가지므로 스마트 카메라 시스템에의 적용을 고려할 필요가 있다.

가장 최소의 계산 비용으로 키를 설정하는 방법은 모든 노드에 동일한 글로벌 비밀 키를 사용하는 것이 것이다. 그러나 일반적으로 노드가 템퍼 레지터턴트하지 않을 것이라는 가정 하에서 글로벌 키 방식은 최소한의 안전한 선택이다. 비록 단 하나의 노드라도 공격자들의 수중에 들어간다면, 키가 유출되고 따라서 전체 시스템은 불안전한 것으로 간주될 수 있다.

각 노드에 통신을 위한 키를 설치하거나 제거하기 위하여 한시적으로 글로벌 키를 사용하는 것은 가능하다. 이 방법은 키 분배 문제를 해결하고 동시에 노드가 도난 당하는 경우에도 시스템을 안전하게 할 수 있다. 그러나 이 경우, 새로운 한시적 글로벌 키가 필요할 것이기 때문에, 전체 네트워크 설치 과정이 처음부터 시작되지 않는다면, 네트워크가 다수의 노드로 확장·축소가 용이하지 않게 된다. 스마트 카메라 네트워크는, 어떤 다양한 환경에서도 교체될 수 있어야 하기 때문에, 노드의 장착, 제거 및 재설치가 유연해야 한다.

키 관리 문제에 대한 또 다른 해결책은 키 설치를 위한 기본 스테이션 또는 특수 노드를 사용하는 것이다. 비록 모든 노드를 템퍼 레지터턴트하게 만드는 것이 용이하지 않지만, 템퍼 레지터턴트한 기본 스테이션이나 통제된 환경에 위치한 기본 스테이션을 사용할 수 있어야 한다. 그러나 비록 템퍼 레지터턴트한 키 분배 노드가 내장된 비밀 키를 보호한다 하더라도, 그것을 탈취함으로서 네트워크를 작동하지 못하게는 할 수 있다.

이중화는 키 배포 노드의 위험을 감소시킬 수 있다. 센서 네트워크에 종종 사용되는 효과적인 방법은 랜덤 키 분배이다[21]. 이 방법에서 각 노드에는 많은 세트의 키의 하부 세트가 제공된다. 절차가 다소 복잡하지만 충분히 많은 하부 세트가 각 노드에 제공되면, 모든 노드가 공통 키를 공유하는 적절한 노드 경로를 통하여 모든 다른 노드와 통신하는 것이 가능하다. 그러나 절차는 다소 복잡하다.

현재 매우 효과적인 전략은 암호화되는 정보의 중요성에 따라 다른 암호 수준을 사용하는 것이다[22]. 노드 간에 교환된 모든 정보가 다 똑같이 중요하지는 않기 때문에, 모바일 코드 또는 제어 정보를 위해서는 가장 강력한 암호를, 사소한 정보를 위해서는 덜 강력한 암호를 사용할 수 있다. 경우에 따라서는 정보의 중요성은 그런 통신이 얼마나 자주 일어나는가에 달려있기도 하다. 예를 들어, 보다 덜 중요한 제어 신호는 계속적으로 교환되는 한편 모바일 코드는 네트워크에서 아주 가끔 전달된다. 이것은 다양한 비밀 요구 수준에 대한 선택의 중요성을 더욱 증가시킨다. 뿐만 아니라 각 패킷에 할당된 암호 수준은 지역에 따라서 또는, 가능한 보안 위반 정도로 결정될 수 있다[22]. 전체 네트워크와 관련된 통신이 최대 수준의 암호가 요구되는 반면, 노드의 지역그룹 사이의 통신은[23] 낮은 수준의 암호 요구가 될 수 잇다. 모든 전략이 장단점이 있지만 교환된 메시지의 가치에 따라 암호 방법의 다양한 복잡성 수준을 사용하는 것이 가장 효과적인 방향일 것이다.

현재 스마트 카메라 네트워크를 위한 특정 네트워크 프로토콜은 존재하지는 않는다. 스마트 카메라 노드가 센서 네트워크에서의 일반적인 모드는 아니기 때문에, 센서 네트워크의 기존 프로토콜을 수정할 필요가 있다. 중요한 차이점은 처리 능력 및 가능한 실시간 비디오 통신 필요성이다. 또한 스마트 카메라 노드는 일반적인

센서 네트워크 보다 노드의 숫자가 적으며, 외부에서 전력이 공급되므로 사용시간이 길고, 실시간으로 지속적으로 동작해야 하므로 각 노드의 사소한 결함이 센서 네트워크에서 보다 네트워크에 더욱 중요한 영향을 미칠 수 있다. 이러한 점은 보안 요구사항 뿐만 아니라 다양한 서비스-품질로 연계된다.

5.2 암호 통신과 인증

키가 분배된 후, 키는 여러 레이어에서 노드 간의 통신을 암호화하는 데 사용될 수 있다. 암호화는 링크 레이어 레벨에서 구현하는 것이 가장 효율적이고 일반적이다. 그러나 이 방식은 가장 간단한 형태로 네트워크 전체의 글로벌 키를 요구하므로 앞에서 설명한 것과 같은 보안 위험을 갖는다. 노드 간의 키 쌍을 갖는 점대점 암호화는 매우 안전하지만 모든 키를 저장하기 위해서는 매우 큰 메모리를 필요로 한다. 링크 계층 암호화의 효율 구현은 10 %, 정도로 낮은 네트워크 오버헤드로 구현될 수 있지만 다양한 매개 변수에 의존한다[24]. 링크 계층 암호화의 전형적인 구현은 이른바 메시지 인증 코드(MAC)의 사용을 기반으로 하며 코드는 메시지에 대한 암호학적 처리의 결과로 생성된다. 인증 코드는 그 내용 확인을 위해서 메시지에 첨부되어 목적지로 전달된다. 일반적으로, 인증 메커니즘에서 각 패킷은 보낸 사람을 확인하는 데 사용되는 단순한 메시지 인증 코드를 포함하고 있다. 또한, 암호화 메카니즘에서 각 패킷의 페이로드는 MAC의 계산 전에 암호화될 필요가 있으며, MAC은 암호화된 콘텐츠를 인증하고 확인하는 데 사용된다.

데이터 선명성은 일반적으로 암호 통신을 통해 구현할 수 있다. 그러나 보안 수준 향상을 위해 사진과 동영상 저작권 소유자를 식별하는 데 사용되는 것과 같은 디지털 워터마크 기술을 사용하여 구현할 수 있다. 시간, 날짜 그리고 노드 데이터를 사용하여 비디오 신호 정보를 워터마크 함으로써, 공격자가 비디오 신호를 재현하는 것을 어렵게 만들 수 있다. 예를 들어, 밤에 건물을 모니터링 하는 스마트 카메라 네트워크에서는 오랜 기간 동안 기록된 신호에 거의 또는 전혀 변경 사항이 표시되지 않는다.

가능한 공격 중의 하나는 기록된 신호를 'freezing'하는 것인데, 신호가 타임스탬프로 워터마킹 된 경우에는 입력 신호의 선명성이 공격당했다는 것을 검출하는 것이 가능하다. 워터마크는 처리 유닛에서 구현할 수 있으나, 센서 유닛이 이 작업을 지원하는 것도 가능하다.

5.3 서비스 거부(DoS) 공격

DoS 공격은 노드 간 통신의 다양한 프로토콜 레이어(링크, 네트워크 그리고 물리 계층 등)에서 이루어 질 수 있다[25]. 물리적 DoS 공격은 유선 스마트 카메라 시스템에서는 쉽지 않지만 무선 시스템에는 대한 심각한 위협이 될 수 있다. 따라서 분산 스마트 카메라는 유선이 보다 안전하다. 뿐만 아니라, 유선의 경우는 전원도 통신 케이블을 통해 공급될 수 있다는 장점을 갖는다. 그러나, 대규모 설치시 경우에 따라서 원격지에의 설치나 이동성 노드가 요구될 수 있으며 이러한 경우 무선 연결이 필요하다. 무선 통신 시스템에 가장 확실한 공격은 주파수에서 통신에 사용되는 간섭을 발생시키는 것이다. 이 공격은 신호 대 잡음비를 제한하여 통신을 어렵게 만드는 데, 주파수가 고정되거나 사전에 약속된 통신은 이런 종류의 공격에 취약하다. 이에 대한 해결책 중의 하나는 대역 확산 스펙트럼 기술을 사용하는 것이다. 이 기술은 넓은 주파수 대역으로 통신신호를 확산함으로서 이러한 주파수 재밍을 막을 수 있다. 또한 비정상적인 간섭을 감지하는 메카니즘을 통신 유니트에 적용할 수 있다. 이러한 메커니즘은 문제점을 검출하여 시스템을 통보하거나 통신 방식을 적절히 변경하도록 할 수도 있다. 또한, 어려운 조건에서 지속적인 통신 시도는 에너지를 소모한다.

매체 접근 제어를 담당하는 링크 계층 또한 DoS 공격에 대한 주요 대상이 된다. 이 경우 가능한 공격은 동시에 프레임을 전송함으로써 충돌을 발생시키는 등의 통신 장애를 일으킬 수 있는 링크 계층 프로토콜의 취약점을 이용한다. 이러한 상황은 반복 재전송 시도를 유발하여 네트워크의 응답을 감소시키고 에너지와 프로세싱과 같은 중요한 리소스를 고갈시킨다. 이러한 공격을 선택적으로 적용하면, 키 분배, 또는 네트워크 토폴로지에서 배치와 같은 특별한 미션을 갖는 특정 노드를 공격함으로써 불공평 또는 비대칭 트래픽을 만들 수 있다.

분산 스마트카메라 시스템에서는 보통 처리 노드 기능과 더불어 다른 노드 간의 통신을 위한 라우터의 이중 기능을 수행하므로 각 노드는 중요하다.

네트워크 계층에서의 DoS 공격은 네트워크에 있는 모든 노드를 공격 대상으로 할 수 있는데, 이는 중앙 집중형 네트워크에서는 특정 노드에서만 라우팅기능이 수행되는데 반해 노드 모두가 라우팅 기능을 수행하기 때문이다. 공격자가 확보한 노드를 이용하여 잘못된 라우팅을 하도록 하는 공격도 가능하며, 노드로 하여금 그 자신의 패킷 라우팅을 편향되게 하도록 함으로써 정당한 라우팅을 감소시키고 의도된 혼잡과 높은 부하 상태로 만들 수 있다.

또 다른 방법 중 하나는 잘못된 방향으로 라우팅 하게 하여 네트워크 트래픽을 증가시키고 통신 지연을 유발시킬 수 있다. 미스 라우팅은 특정 목적지에 여러 개의 패킷을 보내어 패킷 홍수를 발생시키도록 할 수도 있다.

이러한 공격에 대한 방어 메커니즘은 각 목적지에 대한 대체 경로를 동시에 차례로 사용하거나 네트워크 토폴로지의 중요한 부분에 대해 노드를 중복 사용하는 것이다. 이러한 메커니즘은 미스 라우팅 노드의 효과를 줄일 수 있다. 또 다른 해결책은 각 노드에 대해 그 이웃 노드의 라우팅 행태를 모니터링하고 가능한 이상 행동을 기록하는 것이다. 사전 프로그램 된 패턴은 "불법"적인 행태의 검출을 가능하게하고 대체 노드의 네트워크 경로를 찾을 수 있도록 한다. 이러한 지속적인 모니터링은 계산량을 필요로 하므로, 어느 수준까지 구현해야 할지는 사용 가능한 리소스 및 네트워크 토폴로지에서 노드의 중요성 따라 달라진다.

VI. 결론 및 추후 연구 방향

기존의 CCTV나 DVR에서는 한 대의 서버 시스템에서 다수의 카메라로부터 입력 받은 영상을 실시간 압축 및 저장하는 기술을 사용하고 있다. 이에 반하여 지능형 영상보안 기술은 하나의 카메라로부터의 입력영상을 실시간 분석하는 데도 많은 컴퓨팅 파워 및 비용을 요구한다. 따라서 기존의 방식으로 지능형 영상보안 시스템을 구현하려면 엄청난 계산량과 하드웨어 비용의 문제에 직면하게 된다. 분산 처리 구조를 갖는 분산 스마트 카메라 시스템은 기존의 고성능 컴퓨터 기반 지능형 영상감시 기술과 임베디드 프로세서를 기반으로 하고 있다. 분산 스마트 카메라 시스템은 일정부분의 영상처리는 스마트 카메라에서 수행하고 그 결과를 전송 받는 분산처리 구조를 가짐으로서 기존 기술의 한계극복 을 위한 새로운 솔루션이 될 수 있을 것으로 예측되고 있다.

스마트 카메라 네트워크에 대한 보안은 대부분의 스마트 카메라 응용 분야에 있어서 민감하거나 개인적인 정보를 포함 한다는 점에서 매우 중요한 특성이다. 보안 문제는 보안 시스템 아키텍처 및 설계의 초기 단계에서 고려되어야하며, 이미 설계된 시스템 및 프로토콜에 쉽게 추가할 수 없다. 본 논문에서는 분산 스마트 카메라 시스템에 포함될 필요가 있는 다양한 메카니즘과 필요한 보안 관련 프로토콜을 조사하였다.

센서 네트워크 프로토콜에 있어서는 약간의 성능 저하를 감수한다면 안전한 시스템을 구현하는 것은 가능하다. 그러나 스마트 카메라 노드는 일반적인 센서의 노드보다 강력 하며 더 집중적인 처리 작업을 수행한다. 따라서 스마트 카메라 네트워크에서는 성능과 보안 사이의 정확한 균형에 관한 연구가 필요한데, 이는 센서와 네트워크의 경우와 유사하다. 노드 및 네트워크 수준의 보안 요구 사항은 상호 보완적이므로 노드 보안 요구를 강하게 할 것인지 네트워크 보안을 강하게 할 것인지는 각 응용 분야의 특성에 따라 달라진다.

향후 스마트 카메라 시스템은 유비쿼터스 시스템의 일부가 될 것이고 u-City, U-Airport 등 대규모 응용 시스템에 적용될 것이다. 이러한 경우 민감한 개인 환경을 포함하고 통합하게 될 것이므로 개인 정보 보호는 스마트 카메라 시스템에 있어서 심각한 문제가 될 것이다. 뿐만 아니라, 향후 증거 수집을 위한 영상검색기술, 지능형 비디오 포렌식 기술 등 본 논문에서 다루지 못한 다양한 기술에 대한 연구도 이루어져야 할 것으로 생각된다.

참고문헌

[1] 유기영외, "CCTV 기반 얼굴검출 및 인식 시스템 보안 프레임워크에 관한 연구", 한국인터넷진흥원, 2009.7

[2] 유장희, 문기영, 조현숙, "지능형 영상보안 기술현황 및 동향", 전자통신동향분석 제 23권 제 4호 2008년 8월

[3] 서현수 외, "분산 스마트 카메라의 보안에 관한 연구", 제5회 한국사이버테러정보전학회 춘계학술발표대회, 2010.05

[4] 나동호 외, "분산 스마트 카메라 플랫폼의 설계 및 구현", 제9회 한국인터넷방송통신학회 춘계학술발표대회, 2010.05

[5] Rinner and Wolf, "An Introduction to Distributed Smart Cameras", Proceedings of the IEEE, Vol. 96, No. 10, October 2008

[6] Serpanos and Papalambrou,"Security and Privacy in Distributed Smart Cameras", Proceedings of the IEEE, Vol. 96, No. 10, October 2008

[7] W. Wolf, B. Ozer, and T. Lv, "Smart cameras as embedded systems," Computer, vol. 35, no. 9, 2002.

[8] M. Bramberger, B. Rinner, and H. Schwabach, "An embedded smart camera on a scalable heterogeneous multi-DSP system," in Proc. Europ. DSP Educ. Res. Symp. (EDERS 2004), Birmingham, U.K., Nov. 2004.

[9] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper resistance mechanisms for secure embedded systems, in Proc. 17th Int. Conf. VLSI Design 2004, Mumbai, India, 2004.

[10] E. English and S. Hamilton, "Network security under siege: The timing attack," Computer, vol. 29, no. 3, 1996.

[11] H. Broers et al., "Architecture study for smart cameras," in Proc. EOS Conf. Ind. Imag. Mach. Vision, Munich, Germany, 2005.

[12] N. Reijers and K. Langendoen, "Efficient code distribution in wireless sensor networks," in Proc. 2nd ACM Int. Conf. Wireless Sensor Netw. Applicat., San Diego, CA, 2003.

[13] A. D. Rubin and D. E. Geer, Jr, "Mobile code security," IEEE Internet Comput., vol. 2, no. 6, Dec. 1998.

[14] H. Chan and A. Perrig, "Security and privacy in sensor networks," Computer, vol. 36, no. 10, 2003.

[15] A. Hampapur et al., "Smart surveillance: Applications, technologies and implications," in Proc. 2003 Joint Conf. 4th Int. Conf. Inf., Commun. and Signal Process. 2003 and 4th Pacific Rim Conf. Multimedia, vol. 2, Dec. 15-18, 2003.

[16] A. Chattopadhyay and T. E. Boult, "PrivacyCam: A privacy preserving camera using uCLinux on the Blackfin DSP," in Proc. IEEE Conf. Computer Vision Pattern Recognition (CVPR'07), Minneapolis, MN, Jun. 2007.

[17] F. Hartung and F. Ramme, "Digital rights management and watermarking of multimedia content for m-commerce applications," IEEE Commun. Mag., vol. 38, no. 11, Nov. 2000.

[18] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Commun. Surv., vol. 8R 2nd quarter, 2006.

[19] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Commun. ACM, vol. 47, no. 6, 2004.

[20] R. Watro et al., "TinyPK: Securing sensor networks with public key technology," in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., Washington, DC, Oct. 25, 2004.

[21] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. 2003 Symp. Security Privacy, Oakland, CA, May 11-14, 2003.

[22] S. Slijepcevic et al., "On communication security in wireless ad-hoc sensor networks," in Proc. IEEE 11th Int. Workshop Enabling Technol.: Infrastruct. Collab. Enterprises (WET ICE 2002),

[23] J. Deng, R. Han, and S. Mishra, "Security support for in-network processing in wireless sensor networks," in Proc. 1st ACM Workshop Security Ad Hoc Sensor Netw., Fairfax, VA, 2003

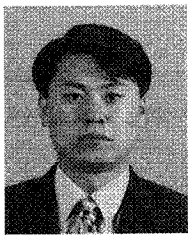
[24] P. Ganesan et al., "Analyzing and modeling encryption overhead for sensor network nodes," in Proc. 2nd ACM Int. Conf. Wireless Sensor Netw. Applicat., San Diego, CA, Sep. 19, 2003.

[25] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, 2002.

〈著者紹介〉

류 대 현 (Ryu, Dae-Hyun)
정회원

1985년 2월: 부산대학교 전자공학과 석사
1997년 2월: 부산대학교 전자공학과 박사
1987년 3월~1998년 2월: 한국전자통신연구원
1998년 3월~현재: 한세대학교 IT 학부
<관심분야> 센서네트워크, 영상처리, 정보보호



한 종 욱 (Han, Jong Wook)
정회원

1985년 2월: 광운대학교 전자공학과 졸업
1991년 2월: 광운대학교 전자공학과 석사
2001년 2월: 광운대학교 전자공학과 박사
1991년 3월~현재: 한국전자통신연구원 책임연구원/융합서비스보안연구팀장
<관심분야> 융합보안, 물리보안

조 현 숙 (Cho, Hyun Sook)
정회원

1979년 2월: 전남대학교 수학교육과 졸업
2001년 2월: 충북대학교 박사
1982년 3월~현재: 한국전자통신연구원 책임연구원/지식정보보안연구부장, 정보보호연구본부장 역임
<관심분야> 정보보안