암호모듈을 이용한 CCTV 영상 데이터 보호 프로토콜에 관한 연구*

박치성[1], 이옥연[1], 윤승환[2], 김승찬[3]
[1]국민대학교 수학과 정보보안연구소
[2]고려대학교 정보경영공학전문대학원, [3]유비즈코아
parkcs01@kookmin.ac.kr

A Study on the Protocol to Protect the CCTV Multimedia Data using

Chi-Seong Park[1], Okyeon Yi[1], Seunghwan Yun[2], Seung-Chan Kim[3]
[1]Dept of Mathematics and CISI, Kookmin University
[2]Graduate School of Information Management and Security, Korea University, [3]Ubizcore

요 약

CCTV(Closed Circuit Television : 폐쇄회로텔레비전)는 산업, 교육, 교통관제, 범죄예방 등의 다양한 목적으로 이미 많은 분야에 활용되고 있다. CCTV의 사용목적이 다양화되면서 CCTV로부터 촬영된 영상 데이터는 굉장히 중요한 자료로 사용된다. CCTV는 영상 및 음성 데이터를 특정 사용자에게 전송하는 시스템으로 수신대상 이외에는 수신할 수 없도록 구성되어 있다. 이러한 CCTV 운영 시스템은 제 3자가 폐쇄회로 내부에 접근한 경우에 대한 보안이 취약하다. 즉 제 3자가 폐쇄회로 내에 접근하게 되면 데이터 포획, 데이터 위·변조가 쉽게 이루어 질 수 있다. 본 논문에서는 폐쇄회로 내에서 인가되지 않은 기기 및 공격자에 의한 데이터 포획, 데이터 위·변조 방지를 위한 프로토콜을 제안한다.

1. 서론

최근 CCTV는 산업, 교육, 교통관제, 치안등 다양한 분야에서 활용되고 있으며 활용되는 분야에 따라 그 목적이 다양하다. 산업분야에서는 사람이 직접적으로 감독할 수 없는 부분에 대해서 사용되며, 교통 분야에서는 교통의 흐름 및 사고 유무 등의 감시뿐만 아니라 교통량의 분석을 통한 현재 도로의 정체 상황 파악 등 다양한 목적으로 활용되고 있다. 뿐만 아니라 범죄현장을 촬영한 CCTV의 영상 데이터는 중요한 증거물로 활용되기도 한다. 또한 최근 CCTV 기술이 발전하면서 CCTV를 통해 촬영된 영상이 카메라에 직접 연결된 네트워크(network)를 통해 전 세계 어느 곳이든 실시간으로 전송이 가능해지면서 CCTV 영상 데이터에 대한 보안이 더욱 중요시 되고 있다.

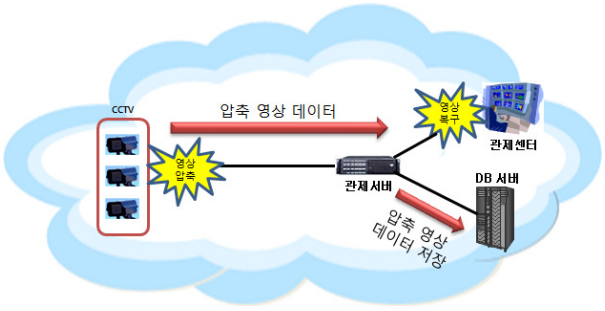
현재 CCTV는 폐쇄적인 네트워크를 구성하여 관제센터에서 제어하고 감시하는 방법으로 운영되고 있다. 수신대상 이외에는 임의로 데이터를 수신할 수 없도록 되어있으며 영상 데이터의 임의 수신이 불가능하다는 것을 전제로 전송되는 영상 데이터에 대한 보안이 취약한 실정이다. 인가되지 않은 제 3자가 해킹 등의 방법을 통해 CCTV 네트워크 내부에 접근하여 영상 데이터를 무단으로 포획한다면 포획한 영상 데이터를 쉽게 볼 수 있으며 데이터에 대한 위·변조가 가능하다. 이러한 문제가 사고현장 및 범죄현장을 촬영한 영상과 같이 중요한 데이터에 대해 발생하게 된다면 매우 심각한 문제일 수 있다.

본 논문에서는 CCTV 네트워크에 인가되지 않은 제 3자가 접근할 수 없도록 CCTV와 관제센터간의 인증체계 구축 및 영상 데이터 관리에 대한 프로토콜을 제안한다.

2. CCTV 운영 시스템

CCTV 카메라를 통해 촬영된 영상 데이터는 (그림 1)과 같이 DCT(discrete cosine transform) 알고리즘, DWT(discrete wavelet transform) 알고리즘 등의 영상 압축 알고리즘을 이용하여 압축된 형태로 관제서버에 전송된다. 관제서버는 전송된 압축 영상 데이터를 관제센터로 전송하여 실시간 모니터링을 할 수 있도록 하거나 압축된 형태로 DB(data base) 서버에 저장될 수 있도록 분기한다. 이러한 기존의 CCTV 운영 시스템은 VPN(virtual private network)을 구성하여 폐쇄적인 네트워크 환경에서 운영된다. CCTV 카메라로부터 촬영된 영상 데이터는 압축과정만을 거치게 되므로 인가되지 않은 제 3자가 해킹을 통해 영상 데이터를 포획한다면 쉽게 영상을 볼 수 있으며 또한 DB 서버에 압축된 영상이 저장되므로 DB로부터 영상 데이터를 추출하면 쉽게 영상을 볼 수 있다.

* 본 연구는 국토해양부 첨단도시개발사업의 연구비지원(07첨단도시 A01)에 의해 수행되었습니다.
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No.2011-0029927).



(그림 1) 기존의 CCTV 운영 시스템

3. CCTV 영상 데이터의 보호

3.1 CCTV 영상 데이터의 기밀성(confidentiality)

데이터를 보호하기 위해서는 전송되는 데이터의 암호화를 통해 데이터에 대한 기밀성을 보장해야만 한다. 데이터를 암호화한다는 것은 암호화하는 사람만이 알 수 있는 고유한 암호화 키를 이용해 평문(의미를 알 수 있는 형식) 데이터를 암호문(의미를 알 수 없는 형식)으로 변환하는 것이다. 또한 이렇게 암호화된 평문 데이터를 복구하기 위해서는 복호화가 이루어져야 한다. 데이터를 복호화 하기 위해서는 데이터를 송·수신하는 개체간의 약속된 복호화 키를 필요로 한다. 즉, 데이터를 암호화함으로써 복호화 키를 알지 못하는 제 3자가 데이터를 무단으로 포획해도 평문 데이터의 내용을 확인할 수 없도록 할 수 있다.

3.2 CCTV 영상 데이터의 무결성(integrity)

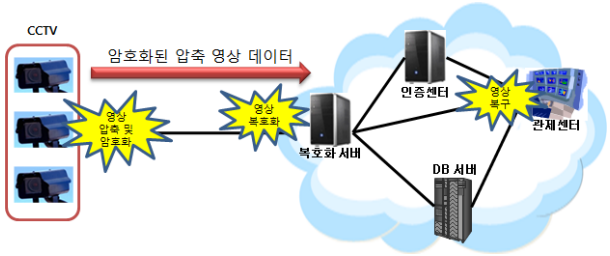
데이터에 대해 기밀성이 보장된다고 해서 영상 데이터를 온전히 보호할 수 있는 것은 아니다. 제 3자가 평문 데이터를 위·변조하여 수신자에게 보낸다면 수신자는 잘못된 데이터를 수신하게 될 것이다. 하지만 수신자는 수신된 데이터가 올바른 데이터인지 위·변조된 데이터인지 구분할 수 없다. 이러한 데이터 위·변조를 방지하기 위해 데이터에 대한 무결성이 보장되어야 한다.

무결성을 보장하기 위해 평문 데이터를 입력으로 해쉬기반 메시지 인증 코드 (HMAC : hash-based message authentication code)와 같은 알고리즘을 이용하여 MIC(message integrity code) 데이터를 만들고 평문 데이터와 함께 수신자에게 전송한다. 수신자는 평문 데이터에 대한 MIC 데이터의 일치 여부를 확인함으로써 기존의 평문 데이터에 대한 위·변조 여부를 확인할 수 있다.

4. CCTV 영상 데이터 보호를 위한 프로토콜

CCTV 영상 데이터를 보호하기 위해 데이터에 대한 암호화를 통해 기밀성과 무결성이 보장한다. 데이터를 암호화하기 위해서는 암·복호화 키에 대한 관리가 이루어져야 한다. 키 관리를 위해서는 키 인증 및 일치에 관한 프로토콜이 반드시 뒤따라야한다.

본 논문에서 제안하는 프로토콜은 기존의 폐쇄적인 망에 국한하지 않고 유·무선에 관계없이 누구나 접근 가능한 인터넷 망에서의 영상 데이터 보호를 목적으로 한다. (그림 2)와 같이 복호화 서버, 인증센터, 관제센터, DB 서버는 같은 네트워크에 속하여 폐쇄적인 망을 구성하고 CCTV로부터 촬영된 데이터는 복호화 서버를 통해 망에 들어와 관제센터 또는 DB 서버에 전송된다.

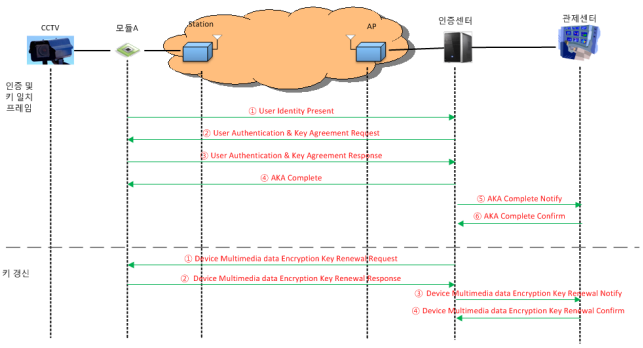


(그림 2) 프로토콜 전체 구성도

4.1 키 인증 및 키 일치 프로토콜

키 인증 및 키 일치 프로토콜에서는 인증센터와 CCTV 간의 상호인증을 통해 기기 입장에서는 정당한 관제센터 여부를 관제센터 입장에서는 정당한 기기인지 여부를 판단해 인가되지 않은 제 3자의 접근을 막는다.

최초 CCTV와 인증센터는 CCTV가 갖는 고유한 마스터 키(master key)를 저장하고 있다. 마스터 키는 최초 기기 등록 시에 발급되며 이를 이용하여 영상 데이터를 암·복호화 할 시에 암호 알고리즘의 키로 사용되는 세션 키(session key)를 생성하게 된다. 세션 키를 생성하는 과정에서 CCTV와 인증센터 간의 상호인증과 키 일치가 이루어지게 된다. (그림 3)은 키 인증 및 키 일치 프로토콜에 대해 설명한다.

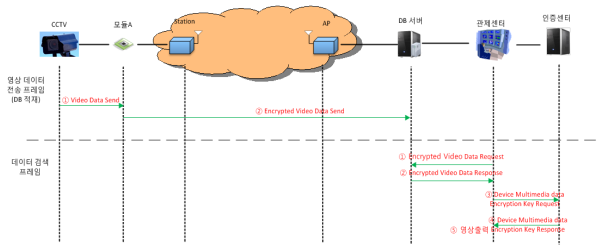


(그림 3) 키 인증 및 키 일치 프로토콜

4.2 CCTV 영상 데이터의 전송 및 검색

CCTV와 인증센터간의 상호 인증 및 키 일치가 완료되면 CCTV는 영상 데이터를 관제센터 또는 DB 서버로 전송한다. 관제센터로 전송되는 데이터는 복호화 서버에서 암호화된 압축 영상 데이터를 복호화하여 실시간 모니터링이 가능하도록 해주며 DB 서버로 전송되는 데이터는 복호화하지 않고 암호화된 형태로 DB 서버에 저장되게 된다. 암호화된 형태로 저장되어 있는 영상 데이터는 인가

되지 않은 제 3자가 접근하여 DB로부터 데이터를 추출해 내도 마스터 키를 알지 못한다면 내용을 확인 할 수 없다. (그림 4)는 데이터 전송 및 검색 프로토콜에 대해 설명한다.



(그림 4) 데이터 전송 및 검색 프로토콜

5. 결 론

기존의 CCTV 운영 시스템에서는 해킹등의 침입에 대해 취약점을 갖고 있다. 이를 보완하기 위해 본 논문에서는 인가되지 않은 제 3자가 침입해도 영상 데이터를 온전히 보호할 수 있는 방법과 프로토콜을 제안하였다.

본 논문에서 제안된 프로토콜을 실제 CCTV 운영 시스템에 적용시키기 위해서는 데이터 전송 및 암·복호화를 위한 헤더(header) 정보 구성과 프로토콜에서 키 인증 및 일치를 위해 사용될 값의 생성에 대해 구체적으로 논의되어야 한다.

참고문헌

[1] 김용희, 박미애, 조진웅, 이현석, 이장연, 이옥연, “Binary CDMA 망을 위한 안전한 AKA 프로토콜”, 정보보호학회논문지, 20(1), 2010. 2. p.51-61

[2] 김대영, 최용강, 김상진, 오희국, “프라이버시와 완전한 전방향 안전성을 제공하는 UMTS 키 동의 프로토콜,” 정보보호학회논문지, 17(3), 2007. 6. p.81-90

[3] 강민석, 배지수, 장태민, 강민석, “AES 암호 알고리듬 기반 디지털 영상 보안 시스템의 설계”, 보안공학연구논문지, 8(2), 2011. 4. p.277-288

[4] 이한덕, 이상일, 조대근, 최정민, 박능수, “CCTV 시스템 응용 사례 및 동향”, 한국멀티미디어학회지, 14(3), 2010. 9. p.19-27