논문 15-40-06-14 The Journal of Korean Institute of Communications and Information Sciences '15-06 Vol.40 No.06
http://dx.doi.org/10.7840/kics.2015.40.6.1102

실시간 영상 기반의 지능형 보안 관제 시스템을 위한 안전한 카메라 네트워크 시스템

양 수 미°◆, 고 은 경*

Secure Camera Network System for Intelligent Surveillance Systems Based on Real-Time Video

Soo-mi Yang°◆, Eun-kyung Ko*

요 약

사회 안전망 제공을 위한 실시간 영상 기반의 협동적 스마트 카메라 네트워크에서는 상황인지 추론 및 처리를 위하여, 스마트 카메라 간에 상황 인지 및 대응을 위한 데이터를 저장 및 전달한다. 특정 이벤트에 대해 카메라가 측정한 값을 다른 상황 데이터 및 추론 결과와 함께 RDB(Relational Data Base)에 저장하고, 해당 정보가 필요한 주변 카메라에 전달한다. 일부 RDB를 온톨로지 RDF(Resource Description Framework) 파일로 변환해 그 결과를 상황인지 추론에 이용한다. 스마트 카메라 간 연동은 ONVIF(Open Network Video Interface Forum) 표준을 따르며, 협동적인 지능형 관제시스템을 이룬다. 데이터 저장 및 전달에 있어서 기밀성과 무결성을 보장하기 위하여 정보보호 기술을 도입하며, 이를 적용한 프로토타입 시스템을 구현하여 오버헤드에 대한 분석을 수행하였다.

Key Words : surveillance, ONVIF, TLS, Smart camera network, Ontology

ABSTRACT

To provide social security and for cooperative smart camera context awareness processing, each camera stores and exchange context data. For a specific event, measured values with other context data is stored RDB. RDB is transformed to ontology RDF file and is used for context reasoning. Interoperability between smart cameras conforms to ONVIF and constitutes intelligent surveillance system. To guarantee the confidentiality and integrity, securiy techniques are adopted. Security overhead between agents is analyzed in the prototype system implemented.

Ⅰ. 서 론

사회 안전망이나 재난 감시의 용도로 광역 보안 관제 시스템이 다수 운영되고 있다. 본 논문에서는 실시간 영상을 기반으로 하는 지능형 보안 관제 시스템에서의 안전한 데이터 전송 및 저장을 다룬다. 지능형 관제 시스템에서는 카메라가 직접 데이터를 분석해 주변에 있는 카메라들이 능동적으로 움직여 상황을 빠르게 대처 할 수 있게 하고자 한다[1]. 이는 카메라에 부속된 에이전트가 상황인지를 위한 기능을 갖추고, 주변 카메라와 통신할 때 가능하다. 현대 사회는 스마트 카메라와 빅 데이터와의 결합을 통해 재난 관리 및

※ 본 연구는 본 연구는 경기도 지역협력연구센터 (GRRC SUWON 2014-B1) 지원에 의하여 수행되었습니다.
°◆ First and Corresponding Author : The University of Suwon Department of Information Security, smyang@suwon.ac.kr, 정회원
* The University of Suwon Department of Information Security, ro_d18@naver.com
논문번호 : KICS2015-03-069, Received March 23, 2015; Revised May 27, 2015; Accepted May 27, 2015

범죄예방 효과를 기대하고 있다. 이에 온톨로지 기반의 추론을 통해 상태변화 지식 확장이 가능한 온톨로지 모델을 제안하며, 이를 통해 온톨로지 기반의 인식 기술을 통한 안전한 지능형 관제시스템을 설계한다. 보안 감시 데이터의 안전성은 인증과 암호화를 통한 무결성과 기밀성의 제공을 의미한다. 협동적 카메라 네트워크에서 스마트 카메라는 PTZ(Pan Tilt Zoom) 값 등의 상황 데이터를 요청받는 서버 역할을 수행할 수 있어야 한다. 능동적 카메라 네트워크에서 자신의 추론엔진이 필요로 하는 데이터를 근접한 카메라에게 요구하는 클라이언트 역할도 필요하다. 서버와 클라이언트의 특성을 모두 갖춘 P2P기반의 네트워크 구성이 요구된다. 서비스를 병렬적으로 실행하기 위해 다수의 스레드가 작업을 분담하며, 이로써 효율적 실행이 가능하다.

정보의 기밀성과 무결성을 제공하기 위해 스마트 카메라간, 데이터베이스, 사용자 인터페이스에서 TLS(Transport Layer Security)[2]를 사용한다. 이를 위해 인증서버의 활용이 필요하며, 인증서가 보안기능 전반에 사용된다.

논문은 2장에서 관련연구를 소개하고, 3장에서 전체 시스템의 설계 내용을 설명한다. 4장에서 소켓 통신 구현 내용을 설명하고, 5장에서 실험 및 성능 분석 결과를 보이며, 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

안전한 통신 시스템을 제공하기 위하여 IETF (Internet Engineering Task Force)[3]에서는 X.509[4] 인증서를 기반으로 TLS 프로토콜을 정의하였다. 이는 다양한 통신 응용에 적용되고 있으며 카메라 네트워크 호환 표준의 하나인 ONVIF[5]에서도 TLS의 사용이 권고되고 있다.

ONVIF는 물리 보안에 사용되는 다양한 IP (Internet Protocol) 카메라의 호환을 목적으로 표준을 제정하고 있는 산업체 표준화 단체이다. 다양한 표준화 명세를 제정하고 있으며, 네트워크 비디오 장치 간의 정보 교환을 위한 장치 발견, 비디오 스트리밍, 지능형 메타데이터 등을 정의하고 있다.

ONVIF를 활용하는 다양한 보안감시 시스템이 연구되고 있다[6,7]. 그러나 지능형 보안관제를 위하여 협동적 온톨로지를 활용하고, 단계별 안전성을 제공하고자 하는 연구는 미비하여 본 논문에서는 안전한 보안관제를 위한 단계별 안전성 제공 기법을 모색하고자 한다.

Ⅲ. 안전한 카메라 네트워크 시스템

본 논문에서는 실시간 영상 기반의 협동적 스마트 카메라 네트워크로 구성된 관제 시스템에서 카메라 및 에이전트, 사용자 간에 전달되는 상황 데이터를 안전하게 전송하고자 한다. 현재 운영 중인 관제 시스템에서는 상황인지 처리를 위하여, 스마트 카메라 간에 상황 데이터를 저장 및 전달한다. 특정 이벤트에 대해 카메라가 측정한 값을 다른 상황 데이터와 함께 RDB(Relational Data Base)에 저장한다. RDB를 온톨로지 RDF(Resource Description Framework) 파일로 변환해 그 결과를 상황인지 추론에 이용한다. 스마트 카메라 간 연동은 ONVIF 표준을 따르며, 그림 1과 같은 전체 구성도를 형성하는 지능형 관제시스템을 이룬다. 추적기능에 의해 변화하는 카메라 시선 값을 빠르게 불러와 시간별로 데이터베이스서버에 입력하여 현재까지의 이동기록을 분석하여 앞으로의 이동방향을 추론하고 제시 할 수 있도록 한다. 직접 데이터를 분석해 주변에 있는 카메라들이 협동적으로 움직여 상황에 빠르게 대처할 수 있게 한다. 이러한 과정에서, 이벤트 데이터를 비롯한 추론과 관련된 정보가 전송되는데, 개인 정보를 포함하여, 시설물에 대한 정보, 향후 상황 대응 절차에 이르기까지 중요한 정보가 포함되므로 이에 대한 보안 기법이 요구된다.

보안 기술의 적용은 세 단계에서 각각 이루어진다. 카메라와 에이전트간, 데이터베이스, 여러 에이전트 간에 기밀성과 무결성의 유지를 위한 보안 기술이 적용된다.

ONVIF에서는 인증과 암호화를 위한 기술을 여러 가지 제시하고 있다. 본 논문에서는 카메라 네트워크를 통한 데이터의 전송에 초점이 맞춰져 있으므로 인증서를 이용한 인증 및 암호화를 TLS상에서 구현하는 기술을 적용한다. 그림 2와 같이 인증서 발급 및 관리를 위한 인증기관을 두고, 이를 관제 시스템에 관련된 프로그램, 시설 및 사용자가 이용하도록 한다.

클라이언트는 Device(스마트 카메라)에 연결되기

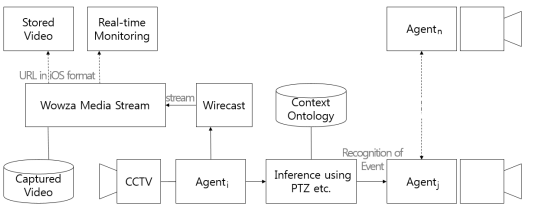

그림 1. 지능형 관제 시스템 전체 구성도
Fig. 1. Structure of an Intelligent Surveillance System

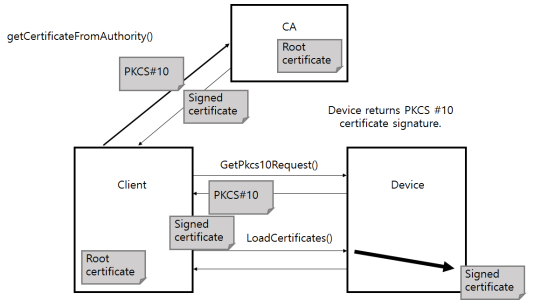

그림 2. 인증기관을 포함하는 인증서 배포 절차[5]
Fig. 2. Certificate distribution procedure including certificate authority

위해서 TLS를 이용한다. 이를 위해 ONVIF는 다양한 인터페이스를 제시하고 있고, ONVIF를 준수하는 카메라는 이를 구현하는 SDK를 제공하고 있다. 예를 들면 인증서의 install과 delete, 인증서 내용 보기 등이다.

https를 통하여 실시간 스트리밍을 하는 절차는 그림 3 과 같다. NVT(Network Video Transmitter)는 인증서를 갖추고 있어야하며, 이는 그림 2의 절차를 따른다. 이후 그림 3의 절차와 같이 URI(Uniform Resource Identifier)를 전송하여, 필요한 데이터를 얻는다.

카메라가 특정 사물을 발견하고 따라간다면 촬영되는 동영상 및 카메라의 시선 좌표 값은 계속 변화할 것이다. 그 변화하는 값을 능동적으로 저장해 데이터를 총괄해 낼 수 있는 데이터베이스 서버가 필요하다. 이는 상황 온톨로지와 함께 에이전트의 상황인지 추론에 사용된다. 데이터베이스를 위한 암호 기술이 필요하다. 데이터베이스의 보안도 인증서를 통한 키 관리를 하며 그림 2의 인증 서버가 그 역할을 한다.

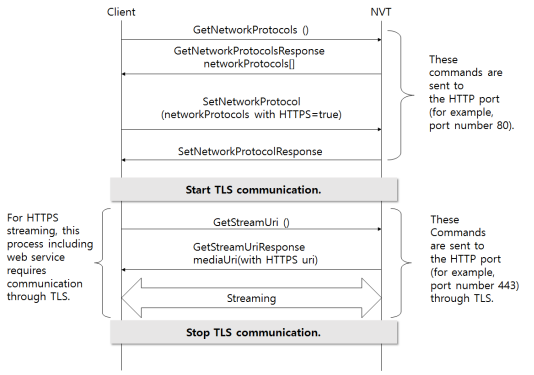

그림 3. TLS를 통한 실시간 스트리밍 절차[5]
Fig. 3. Real-time streaming procedure through TLS

Ⅳ. 구 현

카메라 간에 이루어지는 통신은 일반적인 소켓 통신을 하며 Input_PortNo&IP는 이벤트를 발생시켜 클라이언트가 서버에 통신 요청을 한다. 서버는 run() 함수를 수행하여 클라이언트의 접속을 기다리고 있다. 소켓 통신이 이루어지면 클라이언트는 서버와 같이 데이터를 기다리는 상태가 된다. 서버는 동시다발적인 요청에 대해 응답할 수 있어야 하므로 멀티스레드로 수행한다. 이 때, 선점형기반이기 때문에 스레드는 기다리는 시간이 비교적 짧다. 각 서버와 클라이언트를 클래스로 구현하고 메인에서 객체를 생성하여 활용할 수 있도록 한다. 한 스마트 카메라 내의 서버와 클라이언트는 프로세서를 독점하는 것과 같은 효과를 낸다.

Ⅴ. 실험 및 성능 분석

본 논문에서는 협동적 카메라 네트워크를 포함하는 지능형 관제기능의 프로토타입 시스템을 구축하고 실시간으로 데이터를 제공하여, 효율적인 데이터통신을 가능하다는 것을 보여주고 있다. 발생한 이벤트에 대해 분석하고 그 결과를 토대로 향상된 실시간 영상 기반의 IP카메라 보안 관제를 제공한다.

성능 분석을 위하여 추적 기능에 의해 변화하는 카메라 시선 값을 빠르게 불러와 시간별로 데이터베이스서버에 입력하여 현재까지의 이동기록을 분석하여 앞으로의 이동방향을 추론하고 제시하는 시나리오를 구성하였다. 이 데이터는 TLS 프로토콜을 사용해 보안과정을 거친다. 암호화된 데이터를 Topbraid[8]에서 온톨로지 기반 지능형 추론을 하여 예상 경로와 이상 징후를 포착하여 다른 카메라의 움직임을 제어한다. Topbraid는 온톨로지 설계도구로써, 온톨로지의 생성 및 관리를 위한 개발에 사용된다.

카메라 시선 값은 실수형태의 타입으로 해당 카메라가 제공하는 API을 이용해 알아낼 수 있다. 그림 4 과 같이 java에서 wget명령어를 사용해 그 값들을 버퍼에 저장한다. 버퍼에 저장된 값들은 곧바로 mysql 로 넘겨져 RDB를 형성한다. 이 데이터는 TLS 프로토콜을 사용해 취득한 암호키를 이용해 보안과정을 거친다. 암호화된 데이터를 Topbraid에서 온톨로지 기반 지능형 추론을 하여 예상 경로와 이상 징후를 포착한다.

삼성 테크윈에서 제공하는 SUNAPI(Samsung Unified API)는 ONVIF의 구현을 제공하고 있다[9].

```
main throws IOException {
        String []cmd={
                                "/bin/sh",
                                "-c",
                                "wget -N http://카메라ip주소/cgi-bin/ptz.cgi?query=ptz"
                        };
        Process process = Runtime.getRuntime().exec(cmd);

        File aFile = new File("/root/workspace/wgetSample/ptz.cgi?query=ptz");
        FileReader filereader = new FileReader(aFile);
        BufferedReader reader = new BufferedReader(filereader);
        String readline = null;

        while((readline = reader.readLine()) != null){
            String[] arr = readline.split(":");
            System.out.println("arr[0] : " + arr[0]);
            System.out.println("arr[1] : " + arr[1]);
        }
        reader.close();
}
```

그림 4. PTZ 값의 획득
Fig. 4. Acquisition of PTZ values

그림 5와 같이 카메라가 현재 바라보고 있는 위치인 PTZ값을 읽어 오기 위해 http://(카메라ip주소)/cgi-bin/ptz.cgi?query=ptz를 사용한다. 표준 규격화된 주소에 사용하고자 하는 카메라의 아이피 주소를 넣고 권한 필요시 사용자의 아이디와 패스워드를 입력하면 네트워크 상에서 데이터를 다운받는 명령어로서 유저와의 상호작용이 필요 없는 자동화된 다운로더 시스템을 구성할 수 있다.

온톨로지 기반 추론엔진은 상황을 인지하고 속성을 자동으로 생성하여 파일에 저장한다. 서버는 데이터를 요청한 클라이언트에게 자신의 정보를 제공한다. 앞서 설명한 것과 같이 추론 결과 이벤트 값 또한 클라이언트의 로그파일에 저장된다. 이벤트 값은 엔지니어가 미리 정해 놓은 물리적인 값이다. 그 예로 사람은 0번, 사물은 1번의 이벤트 값이 주어지는 것과 같다. 구성된 온톨로지의 일부 예는 그림 6과 같다.

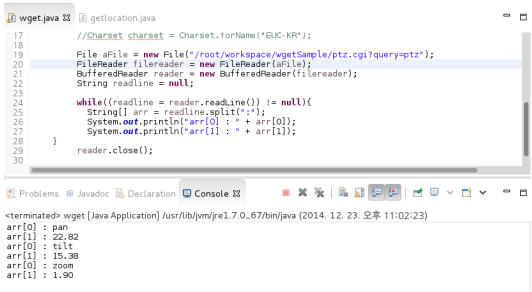

그림 5. PTZ 값의 저장
Fig. 5. PTZ values stored

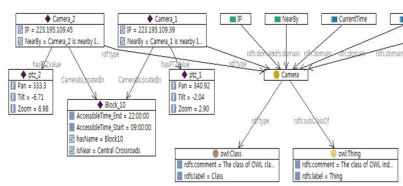

그림 6. 온톨로지 예
Fig. 6. An example of ontology

데이터 전송의 기밀성 확보를 위하여 데이터베이스 및 카메라간 네트워크에서 암호화를 제공하였다. 그림 7은 암호화된 데이터 베이스의 예제이다. 이미지 데이터의 암호화도 가능함을 보이고 있다. 그림 8은 데이터베이스 암호화에 따른 오버헤드 분석결과이다. 데이터 크기의 증가에 따라 오버헤드가 크게 증가함을 볼 수 있다. 비디오 데이터의 암호화를 위해서는 데이터의 선별적 암호화가 필요함을 알 수 있다.

카메라 에이전트간 데이터 전송은 소켓 통신에서의 암호화를 적용하였다. 그림 9는 암호화된 데이터가 전송되는 예를 보여준다. 그림 10은 소켓 통신에서의 암호화에 따른 오버헤드 비교 그래프이다. 데이터의 크기가 증가함에 따라 오버헤드가 급속히 증가됨을 볼

그림 7. 암호화된 데이터베이스 예
Fig. 7. An example of encrypted database

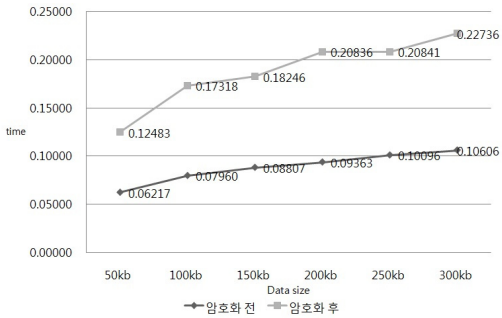

그림 8. 데이터베이스 암호화 오버헤드 비교
Fig. 8. Comparison of database encryption overhead

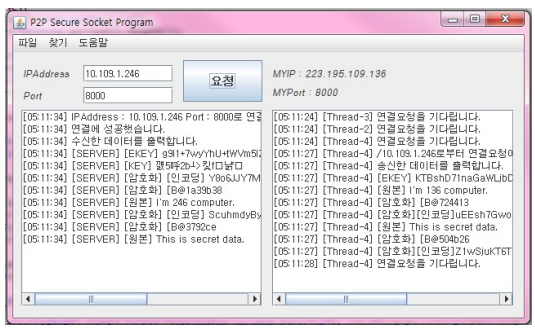

그림 9. 소켓 통신 암호화 예
Fig. 9. An example of encrypted socket communication

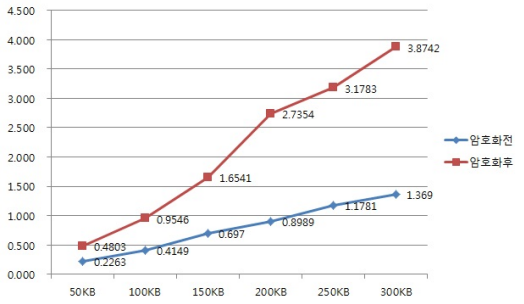

그림 10. 소켓 통신 암호화 오버헤드 비교
Fig. 10. Comparison of socket communication encryption overhead

수 있다. 암호화된 멀티미디어의 전송은 네트워크 대역폭의 고갈 이외에 과도한 지연을 초래하게 된다. 영상 인식의 결과, 추론 결과 또는 센서로부터 인식된 바이오 데이터 및 이벤트 데이터가 우선적으로 전송되어야하며, 가공되지 않은 순수한 영상 데이터의 안전한 전송을 위해서는 프레임의 선별적 암호화를 수행함으로써 시간 오버헤드를 감소시켜야 한다.

Ⅵ. 결 론

본 논문에서는 광범위한 지역을 관리하는 보안 관제 시스템에서 협동하는 카메라 간에 전달되는 데이터, 데이터베이스에 저장되는 데이터 등을 안전하게 관리하는 기법을 설계 및 구현했다. 이는 유비쿼터스 환경을 지향하는 소비자의 요구에 따라 관제 시스템의 범위가 확대되고, 다양한 정보 및 중요한 정보가 전달됨에 따라, 그 기능의 안전성을 높인 것이다. 이를 통해 IP기반의 스마트 카메라 네트워크 감시 분야는 범죄 예방은 물론, 사회 안전망 구축의 토대로서 다양한 분야에 활용될 수 있다.

References

[1] R. J. A. Sankaranarayanan, A. Veeraraghavan, and R. Chellappa, "Object detection, tracking and recognition for multiple smart camaras," in *Proc. IEEE*, vol. 96, no. 10, pp. 1606-1624, 2008.
[2] http://tools.ietf.org/html/rfc6176
[3] http://www.ietf.org/
[4] http://www.itu.int/rec/T-REC-X.509-201210-I/en
[5] http://www.onvif.org/
[6] Y. Tsai, J. Hsu, Y. Wu, and W. Huang, "Distributed multimedia content processing in ONVIF surveillance system," in *Proc. 2011 Int. Conf. Future Computer Sci. Appl.*, pp. 70-73, Jun. 2011.
[7] M. Patzold, R. Eangelio, V. Eiselein, I. Keller, and T. Sikora, "On building decentralized Wide-Area surveillance networks based on ONVIF," in *Proc. Workshop on Multimedia Systems for Surveillance*, pp. 420-423, 2011.
[8] http://www.quadrant.com/
[9] http://www.samsungcctv.co.kr/

양 수 미 (Soo-mi Yang)

1985년 2월 : 서울대학교 컴퓨터공학과 졸업
1987년 2월 : 서울대학교 컴퓨터공학과 석사
1997년 2월 : 서울대학교 컴퓨터공학과 박사
1988년 3월~2000년 9월 : 한국통신 연구소 선임연구원
2004년 9월~현재 : 수원대학교 정보보호학과 교수
<관심분야> 시스템 보안, 보안 관제, 네트워크 보안

고 은 경 (Eun-kyung Ko)

2012년 3월~현재 : 수원대학교 정보보호학과 학생
<관심분야> 네트워크 보안, 데이터베이스 보안, 보안 관제