교통감시・제어시스템을 위한 센서게이트웨이 암호화 연구

임일권* ・김영혁* ・박소아* ・Li Qi Gui* ・이재광* ・박우전* ・천병구**

*한남대학교 컴퓨터공학과 ・**NAS(주)

The encryption research of the sensor gateway for traffic surveillance and control system

Lim Il Kwon*, Kim young Hyuk*, Park So Ah*, Li Qi Gui*, Lee Jae Kwang*, Park Woo Jun*, Cheon Byeong Gu**

*Dept of Computer Science, Hannam University, **Nas Inc.

E-mail : {iklim, yhkim, soapark, qgli, jklee, wjpark}@netwk.hannam.ac.kr*, meso99@nas21.com**

요 약

본 논문은 교통흐름 제어와 원격감시를 위한 교통감시・제어시스템을 Internet망을 사용하기 위하여 센서게이트웨이를 개발하고, 그에 필요한 프로토콜을 제시하여 인증과 암호화를 하였다. 교통감시・제어시스템은 국내・외에서 첨단 네트워크 기술을 활용하여 교통체계의 효율성 증대와 새로운 교통서비스를 제공함으로써 교통문제를 해결하는 데 목적을 두고 있는 지능형 교통시스템(ITS: Intelligent Transportation System)의 중요한 역할을 하게 되는 서비스로써, 교통감시・제어시스템의 TCP/IP 및 Internet 망의 사용은 인가되지 않은 사용자의 접근으로 인한 피해가 발생할 수 있음을 의미하며 그에 따른 데이터의 인증과 암호화는 필수적이다.

ABSTRACT

This paper develops a sensor gateway for using Internet for traffic flow control and remote monitoring, it suggest the required protocol with authentication and encryption. The traffic Surveillance and Control System is an important service to the ITS(Intelligent Transportation System). The traffic surveillance and control system's TCP / IP and the Internet network using is may cause damage means accessing from unauthorized users, Subsequent authentication and encryption of data is essential.

키워드

교통감시, 교통감시・제어시스템, ITS, 센서게이트웨이, 암호화

Ⅰ. 서 론

자동차 등록대수는 2009년 4월말 현재 전국적으로 16,972,008대로써 서울과 경기가 약 40.45%를 차지하고 있다[1]. 이에 따른 과거 10년('98~'07)간 총 241만 건의 교통사고가 발생하였고, 8만 명이 사망하였으며, 365만 명이 부상을 당하였다. 또한 자동차 사고가 전체 교통사고 발생건수의 99.6%와 부상자 수의 99.9%이상을, 사망자 수의 95.1% 이상을 차지하고 있다[2].

이로 인해 지능형 교통시스템의 연구가 활발히 진행되고 있으며, 미국의 IntelliDrive 프로젝트와 캘리포니아 PATH(Partners for Advanced Transit and Highways), 유럽의 CVIS(Cooperative Vehicle-Infrastructure Systems)프로젝트와 Coopers(Co-operative Systems for Intelligent Road Safety) 프로젝트가 진행 중이다[3][4][5][6][7]. 또한 일본에서는 우리나라에서는 흔히 하이패스로 알려져 있는 ETC(Electronic Toll Collection) 시스템이 개발되었으며 Internet ITS기술이 연구 중이다[3][8].

우리나라에서는 2001년 "국가 ITS 기본계획 21"이 수립되어 ITS가 제공하는 서비스를 ①교통

관리 최적화 서비스 분야, ②전자지불처리 서비스 분야, ③교통정보유통 활성화 서비스 분야, ④여행자정보 고급화 서비스 분야, ⑤대중교통 서비스 분야, ⑥화물운송 효율화 서비스 분야, ⑦차량·도로 첨단화 서비스 분야 등의 7개 서비스 분야, 18개 서비스, 62개 단위 서비스로 구분하여 규정하고 있으며, 2020년까지 3단계 ITS 사업 추진계획을 세워 2010년 현재 2단계 성장·확산의 마무리 단계로써 고속도로의 하이패스 서비스, 대중교통 통합정보를 제공 하는 TAGO(Transport Advice on GOing Anywhere)서비스, 실시간 도로 교통정보 서비스 동이 제공되고 있다[9][10].

또한, 교차로의 교통지체를 줄이고 이에 따른 교통흐름을 원활히 하는 교통신호제어를 위한 교통신호 개선방안이 활발히 진행되고 있다. Hummer et al.(1991)은 lagging left-turn이 안전측면에서 큰 효과가 있고 비보호좌회전이 보호좌회전에 비하여 운영측면에서 효율적임을 증명하였다. 그리하여 일본은 간선도로급 이하의 위계에서 비보호 좌회전을 시행하여 2~3현시의 짧은 주기로 신호운영을 하고 있고, 교차로 내에 회전차량이 기다릴 수 있는 Extended-bay가 그려져 있어 all-red 신호시 1~2대정도가 회전을 할 수 있도록 되어 있으며, 영국에서는 직진 차량을 우선적으로 처리하고, 안전도가 높은 roundabout을 일반화하여 보행우선 교통전략을 취하고 있다. 미국은 교통량이 많거나 간선도로를 제외하고 일반적으로 비보호좌회전을 사용하고 있고, 신호운영은 반감응 신호체계가 잘 운영되고 있어 차량유무에 따라 신호현시를 탄력적으로 운영해서 차량이 적은 곳에서는 교차로에서 정지하는 경우가 거의 없다[1].

국내에선 신호선진화 방안으로써 국가경쟁력강화위원회에서 2009년 4월 29일 '기초 법질서 확립을 위한 교통 운영체계 선진화 방안'을 발표하여 ①직진우선 신호원칙 확립, ②좌회전 처리방식 개선을 통한 소통제고, ③적색 신호시 우회전 허용 선별제한, ④신호운영 탄력화 및 교통안전시설 정비·확충, ⑤도로운영 합리화, ⑥보행자·자전거 안전강화 등의 세부사항을 정하고 추진하고 있다[1].

실시간 교통신호제어(RATC: Real time Adaptive Traffic Control)는 미국, 영국, 호주 등 해외 교통 선진국들은 약 20여전부터 꾸준히 연구되었으며 우리나라에서도 1991년에 개발된 실시간신호제어기(COSMOS, Cycle Offset Split Model of Seoul)시스템 개발이 되어 실시간 대응제어와 좌회전 감응제어, 앞막힘 예방제어 등의 주요 기능을 가진다[11].

본 논문에서는 위와 같이 실시간으로 카메라와 각종 센서를 이용하여 교통상황을 모니터하고 이를 바탕으로 각 교차로의 신호제어기를 제어하여 교통흐름을 원활하게 하는 교통감시·제어 시스템에 센서게이트웨이를 개발, TCP/IP 및 Internet 망을 이용하여 중앙서버와 원격으로 감시·제어정보를 중앙서버로 송수신 하게 되고 그에 필요한 데이터의 인증과 암호화를 실시하였다.

Ⅱ. 관련 연구

2.1 PKI

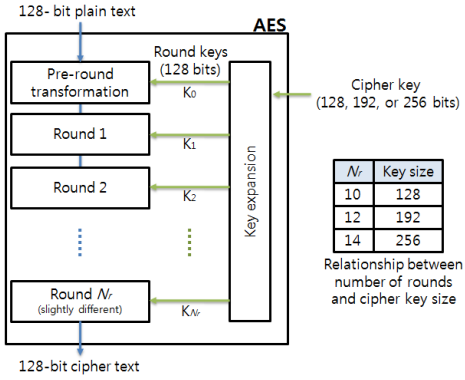
IETF(Internet Engineering Task Force)의 표준안을 중심으로 공개 키 기반구조(PKI: public-key infrastructure)는 비대칭 암호시스템에 기초해서 디지털 인증서를 생성하고, 관리하고, 저장하고, 배분하며 취소하는 데 필요한 하드웨어, 소프트웨어, 사람, 정책 및 절차라고 정의하며, 공개키를 효과적으로 운용하기 위해 정해진 많은 규격이나 선택사항의 총칭이다. PKI의 구성 요소는 주로 다음의 3가지로써, ①이용자, ②인증기관, ③저장소 이며, 이용자는 PKI를 이용하려는 객체, 인증기관은 인증서를 발행, 관리, 폐지하는 역할을 하며, 저장소는 인증서를 보존해 두고, PKI의 이용자가 인증서를 입수할 수 있도록 한 데이터베이스를 말한다. 이러한 효과적인 전자서명 기술을 위해서는 RSA, DSA등과 같은 전자서명 암호화 알고리즘이 필요하다. 본 논문에서의 교통 감시·제어 시스템은 시스템 제작 시 암호화에 필요한 키와 ID를 시스템에 입력하여 제공함으로써 공개키 배포 시의 노출을 최소화 할 수 있다[12][13].

2.2 CRL

인증기관에서는 인증서의 유효성을 검사하기 위한 방법 중 하나로 CRL(Certificate Revocation List: 인증서폐지목록)을 사용하며 PKI 이용 시 키를 분실하거나, 시스템의 폐기, 키를 도난당하거나 했을 경우 인증서의 유효기간 전에 인증서의 효력을 상실하기 위해 만드는 목록을 말한다. CRL은 인증서의 유효성 목록을 갱신하는 시간이 정해져 있고, 목록 전체를 다운 받아야 한다. 이것은 인증서의 폐지 목록의 크기가 커질수록 다운 받는 양이 커지고 목록 갱신을 위한 시간이 증가하게 되며, 결과적으로 통신량의 증가로 인한 과도한 트래픽을 유발하게 된다[14]. 따라서 CRL은 실시간 인증 시 다양한 문제가 발생할 수 있다.

2.3 AES 알고리즘

AES 알고리즘은 2000년 10월 미국의 표준화 기구 NIST(National Institute of Standard and Technology)에 의해 FIST의 새로운 규격으로 선정되었으며, 128비트의 평문을 128비트 암호문으로 출력하는 대칭암호 알고리즘으로써 non-Feistel 알고리즘에 속한다. 라운드 키의 길이는 128비트로써 다음 [그림 1] 같은 구조를 가지고 있다[12]. 2006년까지 공개적으로 알려진 암호화 공격이 없었다[13]. 그리하여 본 논문에서는 보안을 위하여 암호화에 AES 알고리즘을 적용하였다.

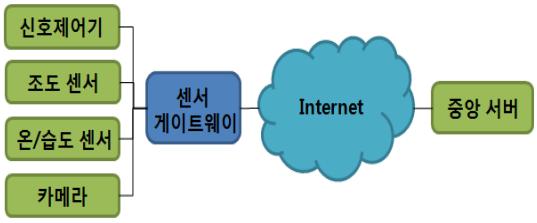


[그림 1] AES 구조

Ⅲ. 시스템 구조

3.1 신호제어 시스템 구조

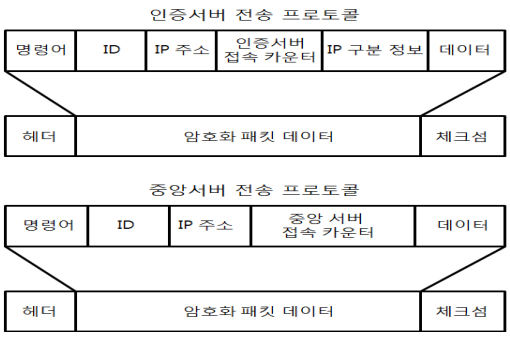
교통 감시·제어 시스템은 다음 [그림 2]와 같은 구조로 구성되어 있으며, 신호제어기와 카메라, 센서 등의 정보는 센서게이트웨이에서 암복호화를 거쳐 Internet 망을 이용하여 중앙서버에서 암복호화를 거쳐 송수신 된다.



[그림 2] 시스템 구조

3.2 통신 프로토콜 설계

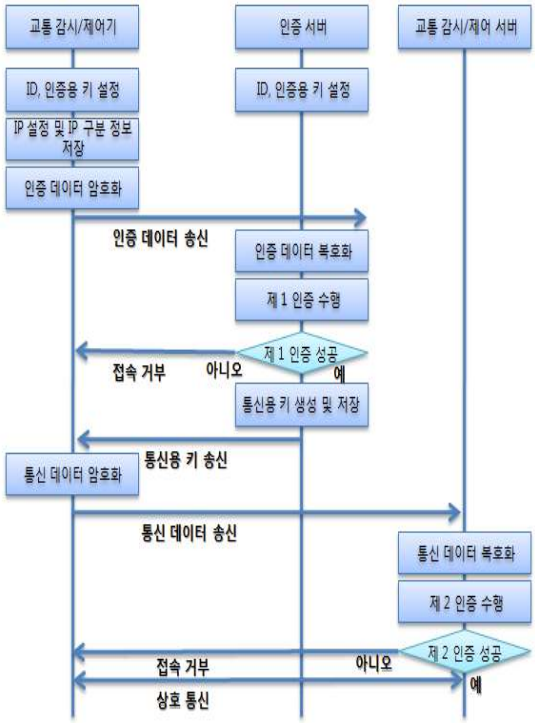
본 시스템은 인터넷 상의 다양한 프로토콜을 지원할 필요 없이 제한된 종류의 프로토콜만 적용하면 되기에 송수신 데이터를 특별한 형태의 분석 또는 가공 없이 서버로 전송하는 투명한 구조로 설계 되었으며 그 구조는 다음 [그림 3]과 같다.



[그림 3] 통신 프로토콜 구조

Ⅳ. 암호화 및 인증과정

교통감시·제어시스템의 센서게이트웨이에 ID, 인증용 키를 저장하고, 이 두 가지 정보와 IP 주소를 이용하여 인증 서버를 통하여 인증을 통해, 데이터 통신용 키를 수신하여 데이터 통신에 사용한다. 인증은 정기적 또는 비정기적으로 수행하여야 하며, ID, 인증용 키, IP 주소, 데이터 통신용 키는 중앙에서 관리한다. 데이터 통신은 감시/제어에 필요한 제한된 프로토콜에 대하여만 적용한다. 인증 시 받은 데이터 통신용 키와 자신의 IP와 목적 IP 등의 기존 정보의 조합으로 생성한 암호와 키를 이용하여 암/복호화 한다. 최초 접속 및 인증, 일반 동작과정은 그림 [그림 4]와 같다.



[그림 4] 암호화 및 인증 과정

Ⅴ. 결 론

국내외 지능형교통체계에 대한 연구개발이 활발히 진행되고 있는 가운데 교통신호제어 및 감시를 위한 교통제어시스템에 센서게이트웨이를 개발하여 Internet 망을 이용하여 중앙서버에서 통제, 관리, 감시가 가능하도록 설계하였으며, 그에 따른 암호화와 인증을 위한 PKI 구조와 AES 알고리즘을 사용하여 보안을 강화하였다. 차후 신호제어를 TRANSYT-7F와 Synchro 등의 신호관련 프로그램을 이용하여 신호제어 및 교통흐름을 시

뮬레이터 할 것이며 그에 따른 교통신호시스템의 최적화를 실시할 것이다.

본 연구는 중소기업청 산학협력실비로 지원을 받아 연구되었습니다.

참고문헌

[1] 이정범, “대전광역시 교통신호체계 개선방안 연구”, 대전발전연구원, 2009.9
[2] “2008년도 교통안전연차보고서”, 국토해양부, 2008.8
[3] 오현서, 박종현, “차량 통신 네트워크 기술 동향”, 전자통신동향분석 제23권 제5호, 2008. 10
[4] 김태홍, “차량통신시스템: 기술, 응용 및 지능형 교통시스템의 전망”, Technical series_KOSEN Report 18.
[5] California PATH, "http://www.path.berkeley.edu/"
[6] IntelliDrive, "http://www.intellidriveusa.org/"
[7] Coopers, "http://www.coopers-ip.eu/"
[8] Internet ITS, "http://www.internetits.org/"
[9] 강연수, “지능형교통체계/텔레매틱스”, 정보과학지 제27권 제9호, 2009.9
[10] ITS KOREA, "http://www.itskorea.or.kr"
[11] 김진태, “실시간 신호제어 개발을 위한 계열 범례 기초검토”,「도로교통」제97호, 2004
[12] Behrouz A. Forouzan, “암호학과 네트워크 보안”, McGraw-Hill Korea, 2008.1
[13] William Stallings, “컴퓨터 통신 보안”, 도서출판 그린, 2005. 8
[14] 채송화, “CRL 분배 및 온라인 인증서 상태 확인 비교”, 전자서명 인증관리 센터, 한국정보보호진흥원, 1999.