제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

ITS를 위한 교통감시·제어시스템의 암호화 연구

임일권*, 김영혁*, ,Li Qi Gui*, 이재광*, 이수경**
*한남대학교 컴퓨터공학과
**NAS(주)
e-mail:{iklim, yhkim, qgli, jklee}@netwk.hannam.ac.kr*, ijsong@nas21.com**

The encryption research of traffic surveillance and control system for the ITS

Lim Il Kwon*, Kim young Hyuk*, Li Qi Gui*, Lee Jae Kwang* Lee Soo Kyoung**
*Dept of Computer Science, Hannam University
**Nas Inc.

요 약

본 논문은 현재 국내·외에서 활발히 연구개발이 진행되고 있는 지능형 교통시스템(ITS: Intelligent Transportation System)의 중요한 역할을 하게 되는 원격감시망의 교통감시·제어시스템을 Internet을 이용하여 개발하고 그에 따라 데이터 송·수신 시 발생할 수 있는 정보 보안의 취약점을 해소하기 위해 대칭암호 알고리즘인 AES(Advanced Encryption Standard) 알고리즘을 적용하였다.

1. 서론

현대사회는 네트워크 기술과 함께 자동차와 그에 따른 환경이 많은 발전을 이루어졌고 그와 함께 차량의 증가로 인한 심한 교통체증으로 인한 차량이동성이 급격히 떨어지고 있다. 그리고 그로 인한 교통 안전성 역시 매우 심각한 문제가 되고 있으며, 그에 따른 국내에서는 2007년에 211,622건의 교통사고가 발생되고 6,166명이 사망, 335,906명이 부상당하였다[1]

그로 인해 첨단 네트워크 기술을 활용하여 기존의 교통체계를 더 효율적으로 사용하거나 새로운 교통서비스를 제공함으로써 교통문제를 해결하는 데 목적을 두고 있는 지능형 교통시스템(ITS: Intelligent Transportation System)의 연구개발이 활발히 진행되고 있고 있으며, 미국에서는 US DOT(United States Department of Transportation:미국 교통부)에서 IntelliDrive 프로젝트를 추진하여 국가차원의 교통정보와 차량 안전 서비스를 제공하려하며, 캘리포니아 대학과 교통연구학회(ITS-Institute of Transportation Studies)에서 관리하는 California PATH(Partners for Advanced Transit and Highways)라는 교통연구단체가 연구 활동 중이다[2][3]

유럽에서는 ITS에 활용하기 위한 차량통신기술로써 COMeSafety라는 참조 모델을 표준화하였고, 노변장치와 차량 통신 시스템과의 통신을 위한 프로젝트로 CVIS(Cooperative Vehicle-Infrastructure Systems) 프로젝트가 진행 중이며, V2I(Vehicle to Infrastructure)통신을 이용한 안전관리 서비스 개발을 위한 Coopers(Co-operative Systems for Intelligent Road Safety)프로젝트가 진행 중이다[5][6] 또한 일본에서는 Smart Way 프로젝트를 통해 DSRC(Dedicated Short Range Communication)통신을 이용하여 ETC(Electronic Toll Collection), 교통정보, 차량 간 충돌 경고 서비스를 제공하는 기술을 개발하였으며, 셀룰러, 무선 랜과 연동되어 차량에서 인터넷 서비스를 개발하는 Internet ITS 기술을 개발하였다[2][7]

우리나라에서는 국가 ITS 기본 계획을 수립, 우리 여건에 맞는 ITS 사업을 위해 2000년 12월 '지능형교통체계 기본계획 21'을 수립하여 진행 중이다. 또한 지방자치단체별 ITS 시스템을 구축(수원, 울산, 광주, 부산, 군산, 부천, 충주 등)하고 있으며, 또한 지식경제부와 공조하여 움직이는 사무실이라 불리는 텔레매틱스 사업을 추진하고 있다[8][9] 또한 한국전자통신연구소를 중심으로 2007년부터 V2V(Vehicle to Vehicle)를 활용한 VMC(Vehicle Multi-hop Communication) 기술을 연구하고 있다[2]

지능형 교통시스템에서의 중요한 역할을 하게 되는 원격감시망을 통한 교통 감시·제어 시스템은 도로의 신호기와 카메라 등의 교통시설물의 상태정보를 실시간으로 수집/관리하고, 이를 통제/제어하여 교통흐름을 최적화하는 시스템이다. Internet망을 이용하여 원격 감시/제어 정보를 중앙 서버로 송수신하게 되며, 이때 TCP/IP 및 Internet 망의 사용은 인가되지 않은 사용자의 접근으로 인한 피해가 발생할 수 있음을 의미한다. 그러므로 그에 따른 데이터의 인증과 암호화는 필수적이다.

2. 관련 연구

2.1 PKI

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 3가지이며, ①이용자, ②인증기관(CA: certification authority) 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. 본 논문에서의 교통 감시·제어 시스템은 시스템 제작 시 암호화에 필요한 키와 ID를 시스템에 입력하여 제공함으로써 공개키 배포 시의 노출을 최소화 할 수 있다.

2.2 CRL

이용자가 PKI 이용 시 키를 잃어버렸거나, 권한이 변경되었거나, 시스템의 폐기, 키를 도난당하거나 했을 경우 인증서의 유효기간의 만기일이 도래하기 전에 인증기관은 인증서의 효력이 상실되어 폐지해야 하는 경우가 발생하는데 이때 인증서를 폐지하거나 무효로 만드는 목록이 인증서폐지목록(CRL: Certificate Revocation List)이다. 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[9] 따라서 CRL은 실시간 인증 시 다양한 문제가 발생할 수 있다.

2.3 3중 DES 알고리즘

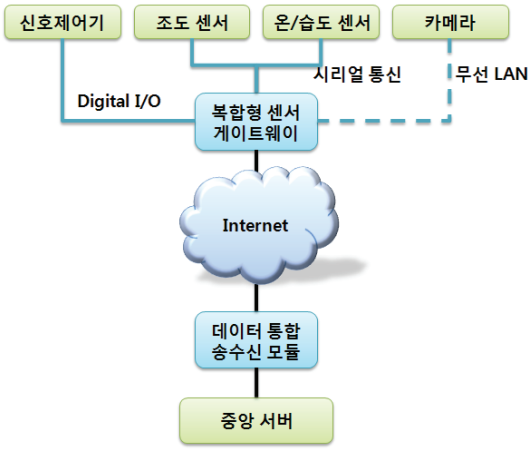
DES(Data Encryption Standard) 알고리즘은 54비트 키를 이용하는 대칭형 블록 암호로써 1977년 미국의 연방정보처리표준규격(FIPS :Federal Information Processing Standards)으로 채택되어 널리 이용되어 왔으나 1999년에 하루 만에 DES키가 해독됨으로써 그에 따른 대안으로 3중 DES를 IBM사에 의해 고안되었다. 이는 3개의 키를 가지고 암호화, 복호화, 암호화를 하는 방식으로써 기존 DES 알고리즘과 호환이 가능하며, 전사적 공격 외에 유효한 암호해독 공격이 발견되지 않았다는 장점을 가지고 있지만, 상대적으로 속도가 느리고 비록 이론적이기는 하지만 전사적 공격에 해독될 수 있다는 단점을 가지고 있다[11][12]

2.4 AES 알고리즘

AES 알고리즘은 2000년 10월 미국의 표준화 기구 NIST(National Institute of Standard and Technology)에 의해 FIST의 새로운 규격으로 선정된 AES는 3중 DES에 비해 속도도 빠르며, 128비트의 키를 가진 대칭 암호 알고리즘으로써 2006년까지 공개적으로 알려진 암호화 공격이 없었다[11][12] 그리하여 본 논문에서는 보안을 위하여 암호화에 AES 알고리즘을 적용하였다.

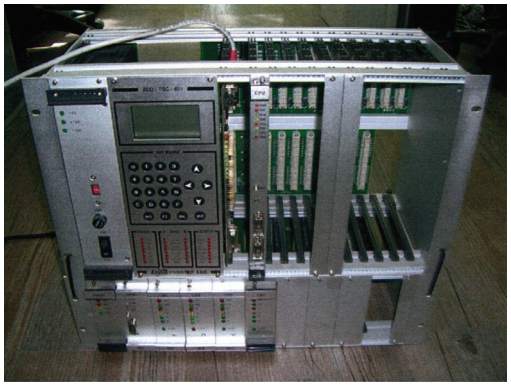
2. 시스템 구조

교통 감시·제어 시스템은 다음과 같은 구조로 구성되어 있다. 신호제어기와 센서에서 취득한 정보 또는 서버에서 전송한 제어 명령은 센서게이트웨이를 거쳐 암·복호화 거쳐 송수신한다. 이러한 정보들은 Internet 망을 이용하여 중앙서버와 송수신되며 그 구성은 다음 [그림 1]과 같다.



[그림 1] 교통 감시·제어 시스템의 구성

다음 [그림 2]는 교통신호 제어기에 센서게이트웨이를 적용한 교통 감시·제어 시스템의 모습이다.

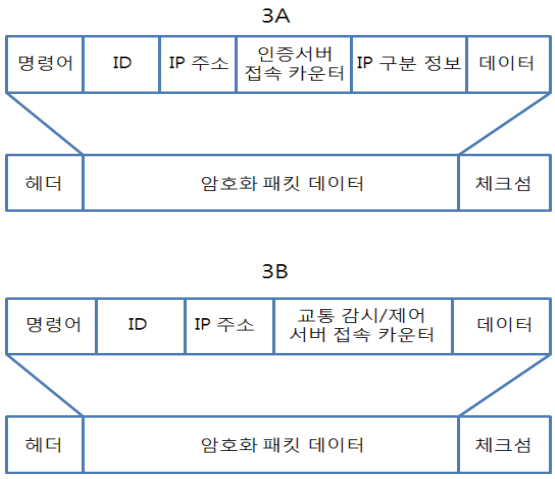


[그림 2] 교통 감시·제어 시스템의 모습

3. 통신 패킷 설계

교통 감시·제어 시스템은 Internet 망을 이용함으로써 보안의 취약점이 발생하게 된다. 본 시스템은 교통의 감시/제어 서비스를 지원하는 만큼 높은 수준의 보안이 요구되며, 인터넷 상에서 사용되는 다양한 프로토콜을 지원할 필요 없이 교통 감시/제어에 필요한 제한된 종류의 프로토콜에만 적용하면 된다는 특징이 있다. 이러한 시스템의 특성을 고려하여 본 교통 감시/제어 시스템은 특화된 프로토콜로 구성되어 있다. 먼저 통신 패킷의 형태는 다음

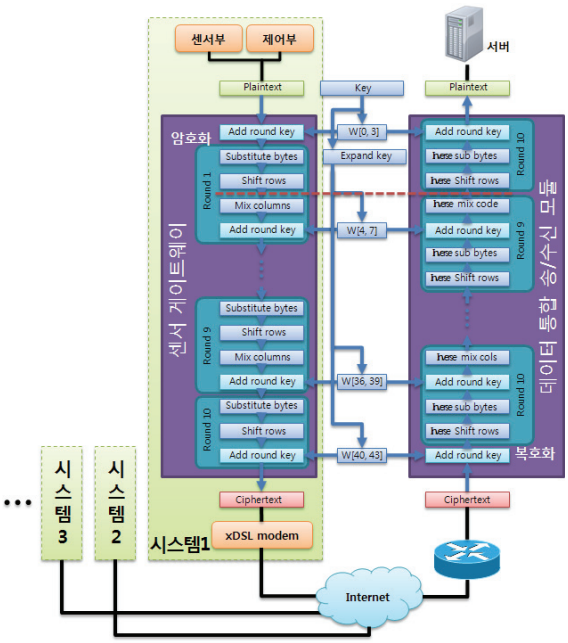
[그림 3]과 같이 구성된다. 이는 센서/제어부에서 수신한 데이터를 최대한 특별한 형태의 분석 또는 가공 없이 서버로 전송하는 투명한 구조로써, 암·복호화 시 암·복호화 및 송수신 목표에 대한 정보만 헤더에 추가하여 encapsulation을 수행한다.



[그림 3] 교통 감시/제어 시스템의 패킷 구조

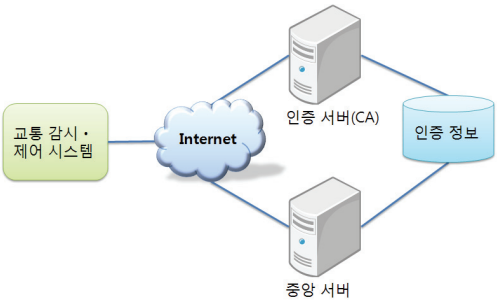
4. 암호화 및 인증 과정

다음 [그림 4]는 교통 감시·제어 시스템에 AES 알고리즘을 적용한 데이터의 암·복호화 과정이다. 이는 각 제어기에 설치된 센서 게이트웨이에서 암호화가 수행하여 서버 측에서는 데이터 통합 송수신 모듈을 통해서 복호화가 수행되는 모습을 도식화하고 있다.



[그림 4] AES 알고리즘을 적용한 교통 감시·제어 시스템의 암·복호화 과정

인증의 기본적인 구성은 다음과 같다. 교통 감시·제어 시스템에 ID, 인증용 키를 저장하고, 이 두 가지 정보와 IP 주소를 이용하여 인증을 받고, 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. 교통 감시·제어 시스템에 적용할 때의 인증 서버 및 중앙서버와의 연결은 다음 [그림 4]와 같다.



[그림 5] 인증 서버 및 중앙서버와의 연결

최초 접속 또는 인증, 일반 동작 과정은 다음과 같다.

4.1 시스템 출하 및 설치 전

기기별로 Serial ID와 인증용 키를 부여하고, 최초 인증 서버의 주소와 통신, 동작방법을 내장하며, 서버관리자가 기기별로 부여된 Serial ID와 인증용 키를 DB에 입력한다.

4.2 IP 설정

고정 IP의 경우 수동으로 설정하며, 유동 IP의 경우 DHCP(Dynamic Host Configuration Protocol)를 이용하여 IP 설정한다. 고정 IP인지 유동 IP인지를 표시하는 field에 위의 사항을 기록한다.

4.3 최초 인증 서버 접속 및 인증

가) 인증 서버 접속 시 패킷 구조는 [그림 3]과 같이 [헤더 + 암호화된 패킷 + chechsum]이며, 암호화되기 전 패킷은 [헤더 + command + Serial ID + IP 주소 + 고정 IP 여부 + 인증 서버 접속 카운터 + data + checksum]이다. 인증 서버 접속 카운터는 접속 성공 시마다 1씩 증가하는 등 규칙적으로 변화한다. 암호화는 Serial ID, 인증용 키, IP 주소를 XOR하여 암호화 키로 이용하며, 암호화 알고리즘은 AES 알고리즘을 사용한다.

나) 인증 서버에서의 접속기기 확인한다. 복호화는 접속 요구하는 기기의 IP 주소와 DB에 잇는 Serial ID, 인증용 키를 사용하여 복호화하며, 모든 Serial ID, 인증용 키를 이용하여 복호화 해보고 복호화 된

패킷이 정한 규칙에 합당한지 검사한다.

DB에 저장된 모든 Serial ID에 대하여 적합하지 않은 경우 운영자에게 통보 및 관련 기기 접속 거부하고, 유동 IP의 경우에 재인증 시(Serial ID 동일할 경우) 중앙서버에 Warning 메시지 표시한다. 이는 교통 감시・제어 시스템의 경우, 상시 운영 및 상시 접속장비이기에, 유동 IP라고 해도, IP 변동이 생기는 경우가 거의 없기 때문이다. 또한 동일한 기기가 여러 번 인증 받는 경우 중앙서버에 Warning 메시지 표시한다.

다) 인증 서버에서 데이터 통신용 키를 교통 감시・제어 시스템에 전송한다.

라) DB에 데이터 통신용 키를 Serial ID, IP 주소, 고정 IP 여부와 함께 입력한다.

4.4 일반 감시, 제어를 위한 통신

[그림 3]과 같은 패킷 구조를 이용하여 송・수신을 하며 암・복호화는 Serial ID, 통신용 키, IP주소를 이용한다. 이때 암・복호화는 AES 알고리즘을 사용한다. 통신 에러 발생 시 중앙서버에 Warning 메시지를 표시한다.

5. 결론

ITS 시스템은 미국의 IntelliDrive, PATH, 유럽의 CVIS 프로젝트, Coopers 프로젝트 일본의 Smart Way, Internet ITS 등 국내외적으로 많은 연구가 진행되고 있으며, 무선통신의 발달로 텔레매틱스와 V2V, V2I의 개발 또한 활발히 진행되고 있다. ITS 시스템에서 중요한 역할을 하게 되는 교통 감시・제어 시스템을 TCP/IP 및 Internet 망을 이용하여 개발하고 그로 인한 보안상 취약점을 극복하기 위해 암호화를 실시하였다. PKI 구조와 함께 AES 알고리즘을 사용하여 안전성을 높였고, 또한 다른 프로토콜과 호환을 고려하지 않아도 되기 때문에 간단한 구조의 독자적인 프로토콜을 구조를 구성하여 인증 및 암호화를 실시하였다.

본 연구는 중소기업청 산학협력실비로 지원을 받아 연구되었습니다.

참고문헌

[1] “2008년도 교통안전연차보고서”, 국토해양부, 2008.8
[2] 오현서, 박종현, “차량 통신 네트워크 기술 동향”, 전자통신동향분석 제23권 제5호, 2008. 10
[3] California PATH, "http://www.path.berkeley.edu/"
[4] IntelliDrive, "http://www.intellidriveusa.org/"
[5] 김태홍, “차량통신시스템: 기술, 응용 및 지능형 교통 시스템의 전망”, Technical series_KOSEN Report 18.
[6] Coopers, "http://www.coopers-ip.eu/"
[7] Internet ITS, "http://www.internetits.org/"
[8] 강연수 “지능형 교통체계/텔레매틱스”, 정보과학회지 제27권 제9호, 2009. 9
[9] ITS KOREA, "http://www.itskorea.or.kr"
[10] 채송화, “CRL 분배 및 온라인 인증서 상태 확인 비교”, 전자서명 인증관리 센터, 한국정보보호진흥원, 1999.
[11] William Stallings, “컴퓨터 통신 보안”, 도서출판 그린, 2005. 8
[12] 히로시 유키, “정보보호 개론”, Infinity books, 2008. 1