Journal of Digital Contents Society Vol. 8 No. 3 Sept. 2007(pp. 371-376)

차량 네트워크 통신용 보안 모듈

권병헌*, 박진성**

요 약

차량 내부에서는 컨트롤러, 센서, 텔레매틱스 단말기, 내비게이션, 오디오 및 비디오 등 다양한 모듈들이 CAN이나 MOST와 같은 차량 네트워크를 통해 연결되어 있다. 게다가, 사용자는 이동 중에 무선 모바일 네트워크를 이용하여 ITS나 인터넷에 접속할 수도 있다. 이러한 네트워크의 다양한 활용은 데이터 해킹, 프라이버시 침해, 위치 추적 등과 같은 많은 보안 문제를 야기하게 된다. 또한, 차량 운영 데이터(센서, 제어 데이터)를 해킹함으로써 차량을 고장 내거나 사고를 유발할 수 있는 가능성도 점차 커지고 있다. 본 논문에서는 CAN이나 MOST와 같은 차량 네트워크에 적용할 수 있는 암호화 기능을 가지는 보안 모듈을 제안한다. 이 보안 모듈은 DES, 3-DES, SEED, ECC 및 RSA와 같은 일반적인 암호화 알고리듬과 전자서명 기능을 제공하게 된다.

A Security Module for Vehicle Network Communication

ByeongHeon Kwon*, JinSung Park**

Abstract

Many modules such as controller, sensor, telematics terminal, navigation, audio and video are connected each other via vehicle network (CAN, MOST, etc). Futhermore, users can have ITS or internet services in moving by connecting to wireless mobile network. These network capabilities can cause a lots of security issues such as data hacking, privacy violation, location tracking and so on. Some possibilities which raise a breakdown or accident by hacking vehicle operation data (sensor, control data) are on the increase. In this paper, we propose a security module which has encryption functionalities and can be used for vehicle network system such as CAN, MOST, etc. This security module can provide conventional encryption algorithms and digital signature processing functionality such as DES, 3-DES, SEED, ECC, and RSA.

Keywords : Vehicle Network, Security, Network, 차량 네트워크, 통신용 보안 모듈

1. 서론

차량 내 탑재되는 제어장치, 센서부, 전자기기, 텔레매틱스 단말기, 네비게이션, 편의장치 들이 모듈화 되어 CAN이나 MOST 같은 전용 통신 시스템으로 연결되고, 무선 네트워크를 이용하여 이동 중에도 인터넷을 사용하거나 ITS 서비스를 이용할 수 있게 됨에 따라 데이터의 해킹이나 프라이버시 침해, 위치 추적의 가능성이 그리 먼 미래의 문제만은 아니다. 또, 차량의 각종 센서와 주제어 장치 사이에 교환되는 데이터를 해킹/위변조하여 차량을 고장 내거나 사고를 일으킬 수 있는 가능성도 점차 커지고 있다.

본 논문에서는 이러한 차량 내부/외부 통신 시스템을 이용함에 있어 적용할 수 있는 보안 모듈을 제안하여 향후 발생할 수 있는 차량 정보의 보안 문제를 해결할 수 있는 방향을 제안하고자 한다.

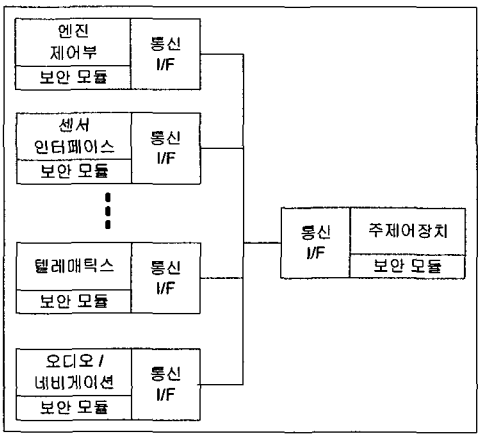
2. 차량통신에서의 보안

2.1 차량 내부의 통신 보안

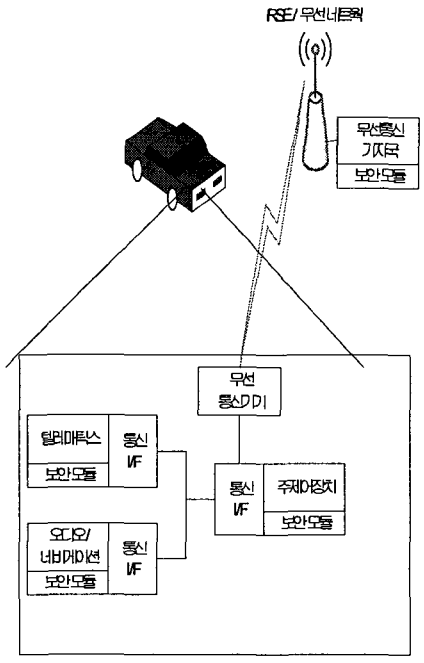
현재의 차량의 주제어장치와 엔진 제어부, 각종 센서, 텔레매틱스 장치, 오디오, 네비게이션

※ 제일저자(First Author) : 권병헌
접수일자:2007년01월27일, 심사완료:2007년06월20일
* 유한대학 정보통신학과
bhkwon@yuhan.ac.kr
** 유한대학 정보통신학과

간의 데이터 교환은 암호화 등의 보안 장치 없이 이루어지는 것이 대부분이다. 교환되는 데이터가 차량의 운행에 중요한 정보가 아닌 경우에는 보안 모듈이 필요 없지만, 데이터가 해킹되는 경우 차량의 운행에 심각한 영향을 끼치는 경우에는 모안 모듈을 필요한 유닛에 부착하여 전송할 데이터를 실시간으로 암호화하여 전송하도록 한다.



(그림 1) 차량 네트워크에서의 보안 모듈



(그림 2) 외부 통신을 위한 보안 모듈

2.2 차량 외부의 통신 보안

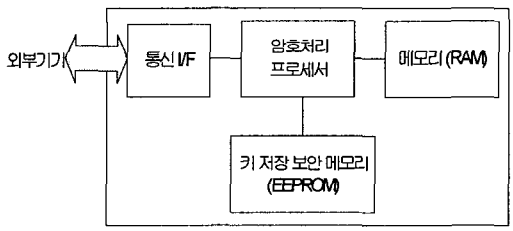
현재 차량과 차량 외부와의 통신은 DSRC, CALM, Wibro 등의 무선 네트워크가 사용되거나 제안되고 있다.

어떠한 네트워크를 사용하건 차량에서는 주제어장치가 그 통신을 제어하게 되며 주제어장치에 연결된 보안 모듈이 외부로 전송되는 데이터의 보안을 수행한다. 차량 외부에서는 무선 통신 기지국이나 RSE, 혹은 무선 통신 게이트웨이에서 모안 모듈을 연결하여 차량과 교환되는 데이터의 보안을 책임진다.

3. 보안 모듈

3.1 보안 모듈의 구조

보안 모듈은 연결된 장치와 Master-Slave 구조로 동작하며, 장치에서 보안 모듈로 암호화, 복호화 등의 명령을 내리고 보안 모듈이 이를 수행한 후 그 결과를 장치로 응답하는 방식이다. 따라서 보안 모듈은 연결 장치와의 통신을 담당하는 인터페이스와 암호화, 복호화, 데이터 검증 등을 수행하는 암호처리 프로세서, 운용을 위한 메모리(RAM), 암호화 키들을 저장하고 있는 보안 메모리 등으로 구성된다.

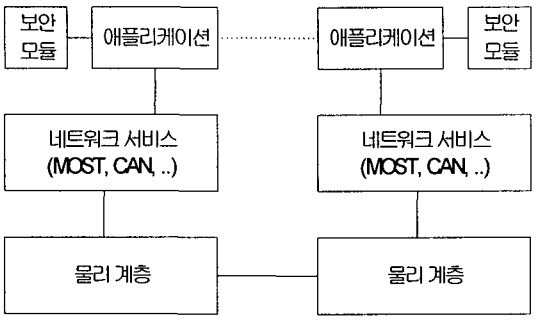


(그림 3) 보안 모듈의 구조

암호처리 프로세서는 DES, 3-DES, SEED, ECC, RSA 등의 암호화 알고리듬을 고속으로 처리할 수 있는 전용 로직을 내장하고 있으며, 암호화/복호화 연산 수행시 키 저장 메모리에 저장된 여러 개의 키 중에서 알맞은 키를 가져와 연산을 수행한다.

보안 모듈에 의해 암호화 되는 데이터는 이미 구축된 차량 내외부 통신 네트워크 시스템 상에서 교환되는 애플리케이션 데이터에 해당하는

부분이다. (그림 4)에 나타나 있듯이 보안 모듈을 이용한 데이터 보안 처리는 애플리케이션 레벨에서 이루어지며, 이는 통신 인프라의 형태나 사용 주파수, 통신 프로토콜과는 독립적으로 보안 처리가 이루어짐을 의미한다.



(그림 4) 통신에서의 보안 모듈 적용

3.2 보안 처리 절차

보안 모듈은 여러 가지 방식으로 동작이 가능하지만, 본 논문에서는 세 가지 처리 절차를 제안한다. 하나는 상호간의 전처리 없이 일방적으로 한 모듈이 다른 모듈에게 암호화된 데이터를 전달하는 방식이고, 다른 하나는 상호간에 인증 절차를 거쳐 세션키(session key)를 생성하여 공유한 후에 보안 처리를 수행하는 방식, 그리고 전자서명을 사용하는 경우에 필요한 방식이다.

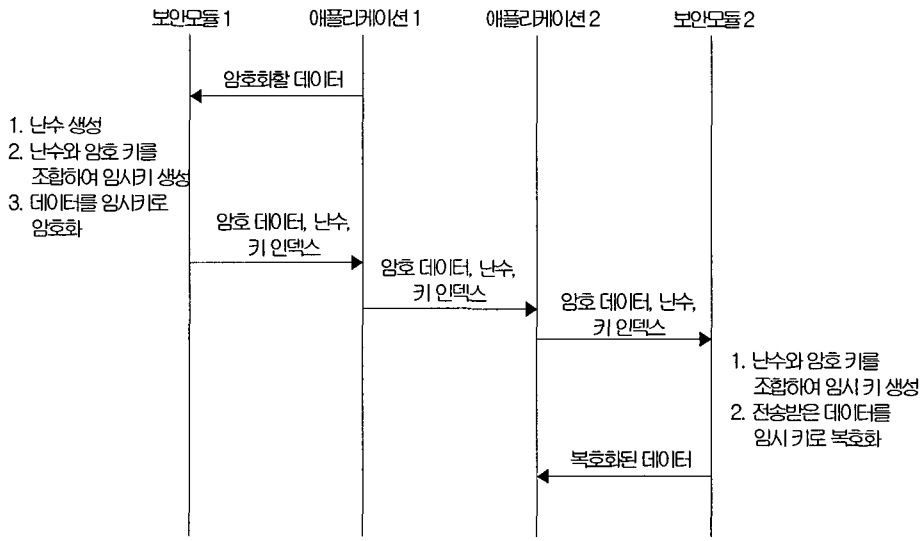
3.2.1 일반 보안 처리

이 방식은 차량 내/외부 애플리케이션 간에 데이터가 고속으로 전송되어야 하거나, 약한 보안 강도를 가져도 되는 데이터에 적용되는 처리 방법이다.

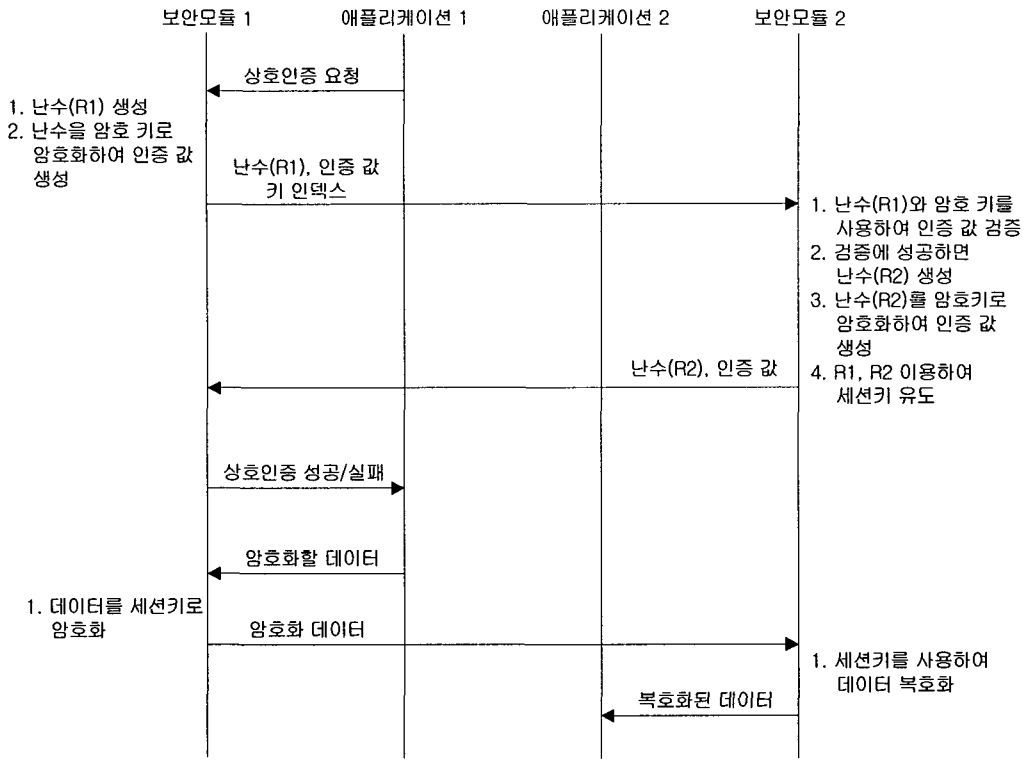
(그림 5)에 나타나 있듯이, 데이터를 전송하는 애플리케이션은 보안 모듈을 통해 데이터를 암호화하고 이 암호화된 데이터를 상대방에게 전송하면, 전송받은 애플리케이션은 자신의 보안 모듈을 통해 이 데이터를 복호화 하는 방식이다. 보안 모듈 간에는 공통된 키를 공유하고 있으며, 상대방 모듈의 고유 번호와 난수를 기반으로 어떤 키를 사용하였는지 계산하게 된다. 이 방식은 두 보안 모듈 간에 사전 데이터 교환 없이 단방향으로의 데이터 전송만 이루어지기 때문에 상호 인증에 비해 빠른 처리 속도를 낼 수 있다.

3.2.2 상호인증 처리

상호인증 처리는 전자지불이나 사용자/차량 고유 정보과 같이 전송되는 데이터가 매우 중요한 경우, 강력한 보안을 적용하기 위한 방법이다. (그림 6)에 나타나 있듯이 상호인증을 시작하고자 하는 보안 모듈이 먼저 자신의 난수(R1)를 생성하고, 다시 난수에 대한 인증 값을 생성하여 상호인증 요청과 함께 상대방 보안 모듈에게 전송하면, 상대방 보안 모듈은 이 난수의 인



(그림 5) 일반 보안 처리 절차



(그림 6) 상호인증 처리 절차

증값을 검증하고 올바른 경우 자신의 난수(R2)를 생성 하고 인증 값을 생성해 응답으로 전송하는 것으로 전처리 과정을 마무리한다.

이 전처리 과정을 통해 두 보안 모듈은 자신과 상대방이 생성한 난수 R1, R2를 공유하게 되며, 인증 값을 통해 서로 동일한 암호 키를 가지고 있는 믿을 수 있는 상대방이라는 것을 검증하게 된다. 검증이 완료되면 각 보안 모듈은 이 두 난수를 기반으로 암호 키에서 세션 키를 유도하게 된다. 만일 한 쪽 상대방이 같은 키를 공유하고 있지 않으면 인증 값 검증에 실패하기 때문에 상호간의 데이터 교환이 이루어지지 않는다.

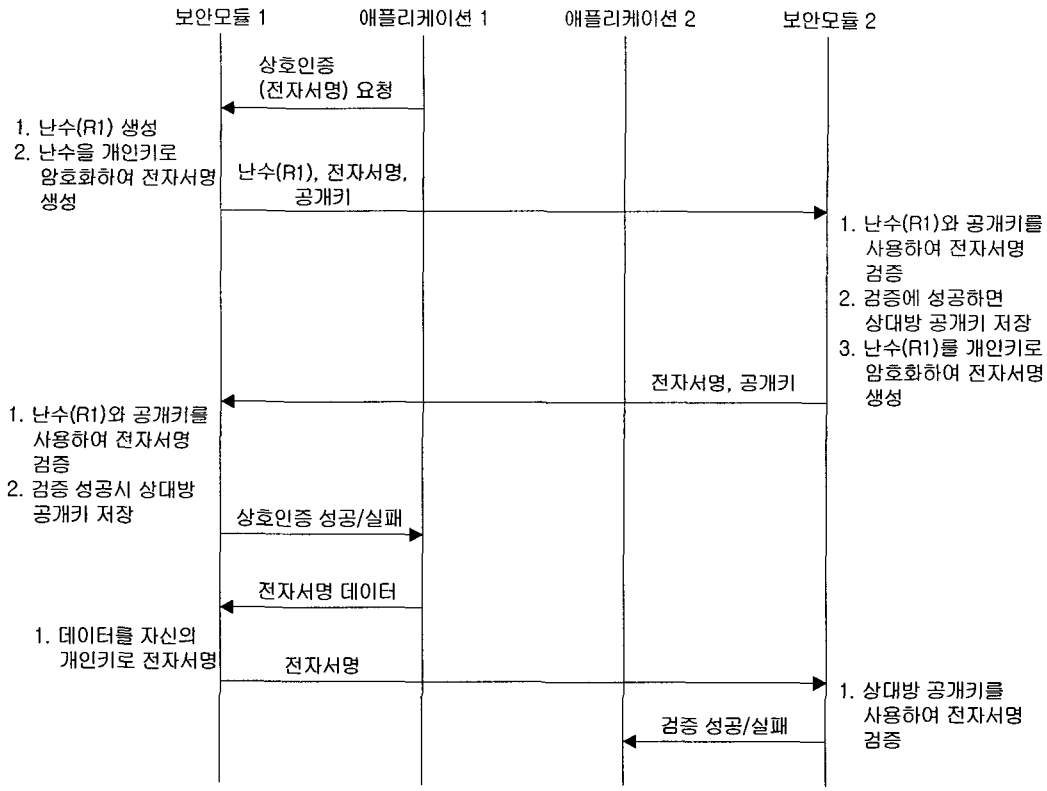
3.2.3 전자서명 처리

두 보안 모듈 간에 RSA 기반의 전자서명을 이용하고자 하는 경우에는 다음과 같이 처리된다(그림 7). 먼저 애플리케이션이 전자서명에 기반한 인증을 보안 모듈에 요청하면, 보안 모듈1은 난수(R1)를 생성하고 이 난수를 자신의 개인키로 전자서명 한다. 이 전자서명을 난수와 자신의 공개키와 함께 상대방 보안 모듈2에 전달하면, 보안 모듈2는 함께 온 공개키로 전자서명을 검증하고, 올바른 경우 이 공개키를 저장한다. 그 다음, 전달된 난수(R1)을 자신의 개인키로 전자서명하고 자신의 공개키와 함께 응답하게 된다. 보안 모듈2의 전자서명과 공개키를 받은 보안 모듈1은 전자서명을 검증하고 보안 모듈2의 공개키를 저장하면 전처리 과정이 끝난다.

그 후 전달하고자 하는 데이터에 전자서명을 생성하여 상대방에게 전달하면, 이를 받은 보안 모듈은 전처리 단계에서 공유한 상대방의 공개키를 이용하여 전자서명을 검증할 수 있게 된다.

4. 결론

차량 내부는 물론 차량 외부와의 데이터 교환에 있어 데이터의 해킹이나 프라이버시 침해, 위치 추적의 가능성이 점차 대두되고 있으며, 차량의 각종 센서와 주제어 장치 사이에 교환되는



(그림 7) 전자서명 처리 절차

데이터를 해킹/위변조하여 차량을 고장 내거나 사고를 일으킬 수 있는 가능성도 점차 커지고 있다.

따라서 본 논문에서는 차량 내부 네트워크는 물론 차량과 ITS, 인터넷 등의 외부 네트워크 연결에 적용할 수 있는 통신 보안 모듈을 제안하였다.

이 보안 모듈은 다양한 보안 알고리듬과 암호키를 내장하고 있어 고속, 대량의 데이터 전송에는 대칭형 암호화 알고리듬을 적용하고, 높은 보안 수준을 요구하는 데이터 전송의 경우에는 상호인증이나 전자서명을 적용할 수 있는 기능을 갖추고 있다. 또, 이러한 보안 모듈은 단순한 통신 보안에만 사용하는 것이 아니라 향후 차량 내 블랙박스 같은 운행기록 장치의 데이터 저장에도 전자서명이나 인증 값을 함께 생성하여 저장하게 함으로써 운행기록의 위변조를 막는데 활용할 수 있다.

참고문헌

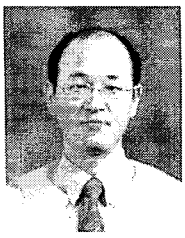
[1] 최창희, 텔레매틱스 기술과 차량 네트워크 기술동향, 오토저널, 27권 6호, pp.9 - 16, 2005년 12월

[2] 곽수진, 이상선, 차량 간 통신을 위한 IEEE 802.11 Ad-hoc 네트워크 성능분석, 자동차공학회 학술대회 논문집, 2006년 춘계학술대회 논문집 3호, pp.1697 - 1702

[3] 박진성, 최명렬, 고기능 RFID 태그를 위한 동적 ID 할당 프로토콜, 한국정보보호학회 논문지, 제15권 제6호, pp. 49-58, 2005.

권 병 헌

1987년 : 한국항공대학교 항공전자공학과 공학사
1989년 : 한국항공대학교 대학원 항공전자공학과 공학석사
1995년 : 한국항공대학교 대학원 전자공학과 공학박사
1997년 : (주)LG전자 선임연구원
현 재 : 유학대학 정보통신학과 부교수
관심분야 : 영상신호처리, 통신, 3D displays.



박 진 성

1995년 : 한양대학교 제어계측공학과 (공학사)
1997년 : 한양대학교 제어계측공학과 (공학석사)
2006년 : 한양대학교 제어계측공학과 (공학박사)
2000년~2002년 : (주)마니네트웍 개발팀장
2003년~2004년 : 노틸러스효성(주) 개발팀 과장
2005년~2007년 : (주)씨이엔 연구소장
2007년~현 재 : 유한대학 정보통신과 강의전담교수
관심분야 : 스마트카드, RFID, 정보보호