차량 통신 보안 기술 동향

이상우
ETRI 융합보안연구팀 선임연구원
ttomlee@etri.re.kr
이병길
ETRI 융합보안연구팀 팀장

1. 개요

오늘날 차량 교통시스템은 교통 시설에 전자, 제어 및 통신 첨단 교통 기술과 교통정보를 개발/활용함으로써 교통 체계의 운영 및 관리를 과학화, 자동화하고, 교통의 효율성과 안전성을 향상시키는 교통 체계를 의미하는 지능형 교통시스템(Information Transportation System: ITS)의 형태로 진화하고 있다. 특히, 차량 통신 기술은 지능형 교통시스템을 구축하기 위한 필수 요소 기술이다. 즉, 지능형 교통시스템은 차량 간 통신 및 차량과 노변 장치 간의 통신을 이용하여 차량 주행의 안전성을 높이고, 운전자에게 편리한 서비스를 제공하며, 궁극적으로는 교통 사고 경감 및 교통 효율성을 증대시키는 효과를 얻기 위한 방향으로 발전하고 있다.

그러나, 지능형 교통시스템의 구축을 위해서는 반드시 보안 기술의 확보가 선행되어야 한다[1],[2]. 차량 네트워크 환경은 기존의 인터넷 등의 네트워크 환경과 달리 네트워크의 보안성 확보 여부가 운전자의 생명과 직결되는 위험 상황을 유발할 수 있기 때문이다. 본고에서는 차량 통신 기술을 소개하고, 보안 요구 사항 및 보안 위협, 그리고 보안 기술 연구 동향에 대해 기술한다.

* 본 내용과 관련된 사항은 ETRI 융합보안연구팀 이상우 선임연구원 (☎ 042-860-1097)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 NIPA 의 공식적인 입장이 아님을 밝힙니다.

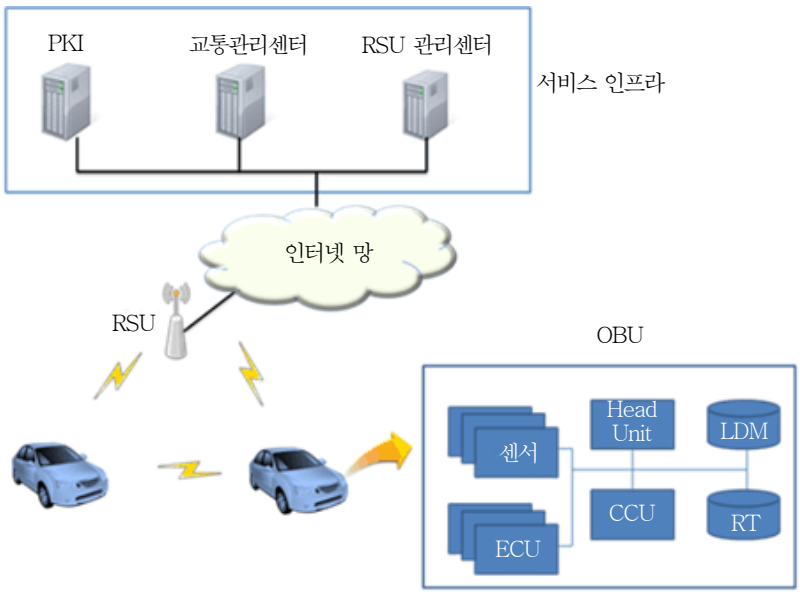
2. 차량 통신 및 보안 요구 사항

가. 차량 통신시스템 개요

(그림 1)에 차량 통신시스템의 개념도를 나타내었다. 차량 통신시스템을 구성하는 개체는 다음과 같다[3].

- 차량 단말 장치(On-Board Unit: OBU)
- 노변 장치(Road-Side Unit: RSU)
- 서비스 인프라

OBU 는 차량 통신을 지원하기 위해 차량 내부에 설치되는 시스템을 의미한다. 라우팅 테이블(Routing Table: RT)은 이웃 차량의 위치 정보 및 타임스탬프 정보를 저장한다. 테이블 정보는 이웃 차량들로부터 수신되는 메시지로부터 구성된다. 지역적인 동적 지도(Local Dynamic Map: LDM)는 고정된 지도 정보에 차량 주위의 도로 교통 정보 및 상태 정보가 반영된 지도 데이터베이스이다. 차량으로 수신되는 메시지가 중복되었는지, 최신의 정보인지를 필터링 하는 역할을 수행한다. 통신 제어 유니트(Communication and Control Unit: CCU)은 차량 내부 및 차량 외부의 통신을 연결하는 모듈이다. 전자 제어 유니트



(그림 1) 차량 통신 시스템

(Electronic Control Unit: ECU)는 차량의 엔진, 자동 변속기 등의 상태를 컴퓨터로 제어하는 장치로서 차량 내부의 센서들을 관리하는 역할을 수행한다. 센서는 차량 주행에 관련된 정보를 감지하는 장치이다.

RSU는 도로 주변에 설치되어 차량과의 통신, RSU 간의 통신을 지원하는 장비로 OBU와 동일하게 라우팅 테이블, 지역적인 동적 지도 등으로 구성된다. 그러나, OBU는 차량 주행과 관련된 센서와 이를 제어하는 ECU로 구성되지만, RSU는 도로 주변에 설치되는 센서 및 이를 제어하는 ECU로 구성된다는 차이점이 있다. 또한, 유선망을 통해 서비스 인프라와의 네트워크를 구성한다.

서비스 인프라는 공개키 기반 구조(Public Key Infrastructure: PKI), 교통 관리 센터, RSU 관리 센터 등으로 구성된다.

차량 통신은 특수한 형태의 이동 애드 혹 네트워크로서 다음과 같은 특징을 가진다.

첫째, 차량 통신은 근거리의 애드 혹 네트워크이므로, 네트워크 노드가 정보를 교환하기 위해 직접 다른 노드와의 연결을 설정한다. 차량 통신 상의 노드는 정보를 요구하는 호스트의 역할 및 다른 노드의 정보를 전달하기 위한 라우터의 역할을 동시에 수행하게 된다. 그리고, 차량 통신 환경에서는 각각의 노드가 서로 다른 방향 및 속도를 가지고 이동하기 때문에 노드의 위치가 급격하게 변하는 특성을 가진다. 특히, 특정 그룹을 형성함에 있어서 노드의 진입 및 탈퇴가 빈번하게 발생한다. 또한, 차량 통신은 노드의 고속 이동 및 네트워크 그룹의 잦은 변화에 대응하기 위해 메시지 처리 및 송수신 과정에서 실시간성이 요구된다.

나. 차량 통신 보안 요구 사항

차량 통신 보안 요구 사항은 다음과 같다[1]-[3].

① 인증 및 데이터 무결성: 차량 통신에서 통신 개체(예: OBU 또는 RSU)는 자신의 ID 및 자신이 그 ID 의 정당한 소유자임을 밝혀야 한다. 이를 개체 인증(Entity Authentication)이라고 한다. 따라서, 통신 개체는 서로 다른 유일한 ID를 가져야 한다. 여기서 주목할 점은 차량 통신은 개체 인증이 반드시 필수적이지 않다는 것이다. 즉, 특정 그룹의 차량 간 통신에 있어서 그룹의 구성원인 차량은 자신이 현재 그룹의 구성원인 것만을 증명하면 된다. 이를 속성 인증(Attribute authentication)이라고 한다. 또한, 통신 개체 간 송수신 되는 메시지는 위/변조되지 않아야 한다.

② 기밀성: 차량 통신에서 통신 개체 간 송수신되는 메시지는 인가되지 않은 개체에 대해 비밀성이 유지되어야 한다.

③ 프라이버시 보호: 프라이버시 보호는 차량 통신에 있어서 매우 중요한 보안 요구 사항이다. 운전자는 자신이 소유한 차량에 대한 정보(운전자 식별 정보, 주행 정보 및 위치 정보)를 다른 차량으로부터 보호할 수 있어야 한다. 차량 통신에서 프라이버시 보호 방안이 제공되지 않는다면, 임의의 공격자는 특정 차량의 주행 정보 등을 쉽게 추적할 수 있다. 한편, 주행 안전과 관련해서 차량 간의 신뢰가 형성되어야 하므로, 완전한 프라이버시 보호가 아닌, 특정 조건에서는 차량을 추적할 수 있는 조건부 프라이버시 보호 방안이 제공되어야 한다. 특히, 특정 차량의 주행 위치를 알 수 없도록 하는 위치 정보 프라이버시 보호 방안이 제공되어야 한다. 또한, 비인가된 개체는 동일한 차량이 전송한 두 개 또는 그 이상의 메시지 간에 연결성을 확인할 수 없어야 한다.

④ 부인 봉쇄: 메시지를 송신한 개체는 메시지 전송 사실을 부인할 수 없어야 한다. 차량 통신시스템에서는 디지털 서명을 사용함으로써 부인 봉쇄 기능을 제공한다.

⑤ 가용성: 가용성은 각각의 노드는 항상 메시지를 전송할 수 있어야 하고, 전송되는 메시지는 수신 노드에게 적절한 시간 안에 도착해야 한다는 요구사항이다. 차량 통신 보안은 운전자의 생명과 직결된다는 점에서 가용성에 대한 요구 사항이 강조된다. 예를 들어, 사고 발생 경고 메시지는 사고 지점에 도착되는 차량들에게 신속하게 전달되어야 한다. 즉, 사고 발생 경고 메시지가 채널 전파 방해와 같은 공격에 의해 신속하게 메시지가 전달되지 못하고, 후방 차량이 사고 발생 지점까지 도착하게 된다면 차량 통신을 통한 지능형 교통 서비스 시스템이 무의미하게 된다.

다. 차량 통신 공격자 형태 및 위협 분석

차량 통신에서의 공격 형태는 공격자의 위치를 기준으로 외부 공격자 및 내부 공격자로 분류할 수 있다. 외부 공격자는 인터넷 통신망을 통해 RSU를 공격하는 형태, RSU 주변에서 무선망을 통해 공격하는 형태, OBU 주변에서 무선망을 통해 공격하는 형태가 있으며, 내부 공격자는 외부 공격자보다 상위의 접근 권한을 가지고 OBU, RSU, 서비스 인프라에 침입하는 형태이다. 특히, 내부 공격자는 특정 차량의 비밀 정보(개인키 등)을 알고 있고, 이를 활용하여 차량 통신 프로토콜에 참여할 수 있는 공격자를 의미한다.

또한, 공격자의 데이터 위/변조 가능 유무에 따라 능동적인 공격자 및 수동적인 공격자로 분류할 수 있다. 능동적인 공격자는 자신이 라우팅 하는 메시지를 위조 또는 변조할 수 있으며, 일정 범위의 거리에 있는 차량들이 메시지 송수신이 불가능하도록 전파 방해 공격도 가능한 공격자를 의미한다. 수동적인 공격자는 전송되는 메시지의 위/변조는 불가능하고, 도청을 통해 불법적인 정보를 습득하는 공격자를 의미한다.

차량 통신시스템에서 보안 요구 사항에 따른 위협은 다음과 같다[1]-[3].

① 인증 및 데이터 무결성에 대한 공격

- 라우팅 테이블, LDM의 변조 공격: 차량의 위치 정보를 거짓으로 조작하여 전송하거나, GPS(Global Positioning System) 위치 정보를 스푸핑(spoofing)하거나, GPS의 신호 정보를 조작하는 공격을 의미한다.
- 위장(Impersonation) 공격: 공격자는 네트워크 상의 다른 노드로 위장할 수 있다. 이것은 공격자가 위장하고자 하는 노드의 비밀 정보를 획득함으로써 가능하다. 위장 공격에 의해 특정 노드에게 전달될 정보가 공격자에 의해 수신되거나, 특정 노드가 전송해야만 하는 정보를 공격자가 거짓으로 전송하는 것이 가능하다. 예를 들어, 공격자는 응급 차량 ID를 도용하여 전방 차량으로 하여금 응급 차량이 접근한다는 거짓 정보를 전송 할 수 있다.
- Sybil 공격: Sybil 공격은 임의의 공격자가 다수의 ID를 가지고 네트워크를 공격하는 방법을 의미한다. 차량 통신 환경에서는 하나의 차량이 다수의 차량 ID를 이용하는 것을 의미한다. 예를 들면, 공격자(하나의 차량)가 다수의 차량 ID를 도용하여 도로가 병목 상태에 있다는 거짓 정보를 전파할 수 있다.
- 라우팅 메시지의 위/변조 공격: 중간 노드가 자신이 전달하게 되는 메시지를 위/변조 함으로써 다른 차량으로 하여금 거짓 정보를 수신하게 하는 공격이다.
- 센서 위/변조 공격: 차량 내 통신망에서 물리적인 주소를 위/변조 하거나, ECU의 센서 제어 정보를 위/변조하는 공격이다.
- 차량 비밀 정보 유출 공격: 차량의 개인키 및 고유 정보(예: 차량 ID)에 대한 위/변조 및 비인가된 사용을 의미한다.
- 서비스 인프라에 대한 공격: PKI 인증 센터에게 OBU의 거짓 침해 정보를 전달하여 잘못된 인증서 취소 목록을 생성하게 하는 공격이다.

② 기밀성에 대한 공격

- 차량 통신 메시지의 도청 공격: 차량 통신 메시지의 도청은 차량 간 통신 메시지 및 차량과 인프라 간의 통신 메시지에 대한 도청을 의미한다. 공격자는 차량 내 또는 근접 거리에서 OBU 의 통신 메시지를 도청하거나 도로 상에서 RSU 의 통신 메시지를 도청할 수 있다. 또한, 도청된 메시지를 이용하여 교통 상황 정보를 분석할 수 있다.
- OBU 또는 RSU 의 비밀 소프트웨어의 도청 공격: OBU 또는 RSU 의 원거리 업데이트 중에 소프트웨어를 가로채거나, 가로챈 소프트웨어로부터 차량의 비밀 정보를 유출하는 공격을 의미한다.

③ 프라이버시에 대한 공격

- 개인정보의 수집 공격: 차량 통신 메시지를 수집 및 분석하여 차량의 소유자를 분석하고, 그 차량의 출발지, 경유지 및 목적지 등의 위치 정보를 수집하는 공격을 의미한다.
- 가명(Pseudonym) 분석 공격: 가명 분배 과정의 메시지를 획득하여 차량의 고유 ID 와 가명의 연결 관계를 획득하거나 서로 다른 가명들이 동일한 차량임을 분석하는 공격을 의미한다.

④ 부인 봉쇄에 대한 공격

차량 통신에서 부인 봉쇄를 제공하는 보안 메커니즘은 디지털 서명이다. 따라서, 부인 봉쇄에 대한 공격은 디지털 서명에 연관된 공격 행위가 된다. 즉, CA(Certificate Authority)에 저장된 가명 DB 를 위조하거나, 장기 인증서(Long Term Certificate)와 가명 인증서(Short Term Pseudonym Certificate) 간의 관계를 조작하는 형태의 공격이 가능하다. 또한, 디지털 서명 생성을 위한 개인키 및 인증서에 대한 비인가된 접근도 부인 봉쇄 요구 사항을 위배하는 공격이 된다. 특히, 차량 통신에서 부인 봉쇄에 관한 공격은 두 개 이상의 노드가 비밀 정보를 공유할 때 발생할 수 있다.

⑤ 가용성에 대한 공격

가용성에 대한 공격은 통신 채널을 점유하여 정상적인 메시지 송수신이 불가능하게 하는 것을 의미한다. 이것은 다수의 OBU 또는 RSU 를 해킹하거나, 하나의 차량으로 하여금 무한대의 메시지를 전송함으로써 가능하다. 또한, 메시지를 라우팅하는 차량이 라우팅하지 않거나, 특정 메시지만 라우팅하는 것도 가용성에 대한 공격의 일종이다.

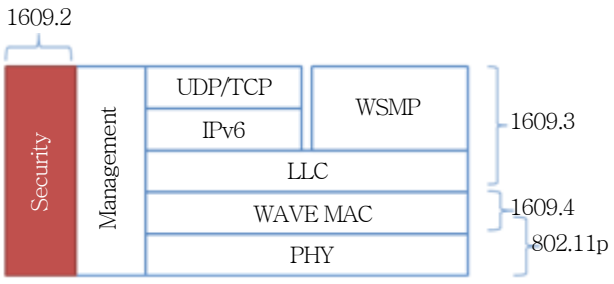
- 전파 방해(Jamming) 공격: 전파 방해 공격은 일정 구역에서 차량 통신에 장애를 일으키는 신호를 발생시키는 공격으로서 네트워크 계층 또는 물리 계층에서의 공격을 의미한다.
- V2X 통신에 대한 DDoS 공격: 플러딩(Flooding)은 단일 홉 또는 멀티 홉 통신 구간에 다량의 무의미한 메시지를 전파하는 공격이며, 블랙홀(Black-hole attack)은 다음 홉으로 라우팅 해야 할 메시지를 전송하지 않는 공격이다. 라우팅 노드가 특정 메시지만을 재전송하는 공격도 포함된다.
- OBU 및 차량 내부 통신망에 대한 DDoS 공격: 차량 내부 통신망에 악성 코드를 삽입하는 공격 및 특정 차량에게 아주 많은 연산이 필요한 메시지를 다량으로 전송하거나, 저장하기에 너무 큰 메시지를 다량으로 전송하는 공격을 의미한다. 특히, 비인가된 OBU 소프트웨어의 빈번한 업데이트도 치명적인 공격이 될 수 있다.

3. IEEE 1609 WAVE 및 보안 기술

가. WAVE 개요

IEEE 1609 에서는 차량 간 통신에 적합한 프로토콜인 WAVE(Wireless Access in Vehicular Environment)의 표준화를 진행중이다[4]. (그림 2)는 WAVE 프로토콜의 계층 구조를 나타낸 것으로 IEEE 802.11p 를 물리 계층으로 활용하며, 5.85~5.925GHz 의 전용 주파수 대역을 사용한다. IEEE 802.11p 상위의 MAC 및 응용 계층은 IEEE 1609 에 정의되어 있다.

물리계층인 IEEE 802.11p 의 특성은 차량의 고속 이동 환경에 적합하도록 기존의 무선랜 규격에 비해 좁아진 채널 대역폭(10MHz), 높은 RF 출력(최대 44.8dBM)을 가진다. 또한, 교통 안전 메시지의 빠른 전송을 위한 제어 채널과 트래픽 메시지 전송을 위한 서비스 채널로 채널을 구분하여 사용하는 멀티 채널 스위칭 방식을 채택하고 있다. 또한, IEEE 802.11p 에서는 무선 링크 접속 시간을 단축하기 위해 기존 무선랜에서의 링크 접속을 위한 인증 및 협상 단계를 생략한 것이 특징이다.



(그림 2) WAVE 프로토콜 스택

물리 계층 위에서 정의되는 WAVE 표준의 종류 및 현재 표준화 제정 상태는 <표 1>과 같으며, 그 주요내용은 다음과 같다.

- IEEE 1609.1 Resource Manager: IEEE 1609.1 에서는 WAVE 자원 관리 애플리케이션의 서비스 및 인터페이스에 대해 정의한다. WAVE 구조에서 제공되는 데이터 및 관리 서비스에 대해 기술하고, 명령어 메시지 및 그에 대응되는 응답 메시지의 포맷을 정의하고, WAVE 규격 상의 개체 간 통신을 위한 애플리케이션의 데이터 저장 포맷에 대해 정의한다.
- IEEE 1609.2 Security Services for Applications and Management Messages: IEEE 1609.2 에서는 보안 메시지 규격과 보안 통신을 위한 처리 절차를 기술한다.
- IEEE 1609.3 Networking Services: IEEE 1609.3 에서는 WAVE 데이터 교환을 위한 주소 체계 및 라우팅 방법을 포함하는 네트워크/전송 계층 서비스를 정의한다. WAVE Short Message 프로토콜과 WAVE 프로토콜 스택을 위한 관리 정보(Management Information Base: MIB)를 기술한다.
- IEEE 1609.4 Multi-Channel Operation: IEEE 1609.4 에서는 제어 채널 및 서비스 채널로 구성되는 다중 채널을 지원하기 위한 MAC 계층을 정의한다.

<표 1> WAVE 표준화 현황

표준 번호	제목	비고
IEEE 1609.0	Architecture	진행 중
IEEE 1609.1-2006	Resource Manager	Ver. 1: 2006 년 제정 Ver. 2: 진행 중
IEEE 1609.2-2006	Security Services for Applications and Management Messages	Ver. 1: 2006 년 제정 Ver. 2: 진행 중
IEEE 1609.3-2010	Networking Services	Ver. 1: 2007 년 제정 Ver. 2: 2010 년 제정
IEEE 1609.4-2010	Multi-Channel Operation	Ver. 1: 2006 년 제정 Ver. 2: 2010 년 제정
IEEE 1609.11-2010	Over- the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems(ITS)	Ver. 1: 2011 년 제정

나. WAVE 보안 기술

WAVE 통신 기술을 이용한 애플리케이션은 차량 주행의 안전성과 직결된 문제이므로 도청, 스푸핑, 변조, replay 공격 등으로부터 메시지를 보호하는 것이 필수적이다. 또한,

WAVE 기술은 개인의 차량에 적용되는 기술이므로 운전자의 프라이버시 보장 또한 필수적으로 제공되어야 한다. WAVE 보안 기술의 가장 큰 제약 사항은 보안 기능으로 인한 메시지 전송 시간의 지연을 줄이는 것이다. 즉, WAVE 의 특성 상 고속 이동 중인 차량 간에 전송되는 메시지를 보호하게 되므로 패킷 손실이 발생하지 않도록 보안 기능에 의한 처리 지연 시간이 최소화되어야 한다.

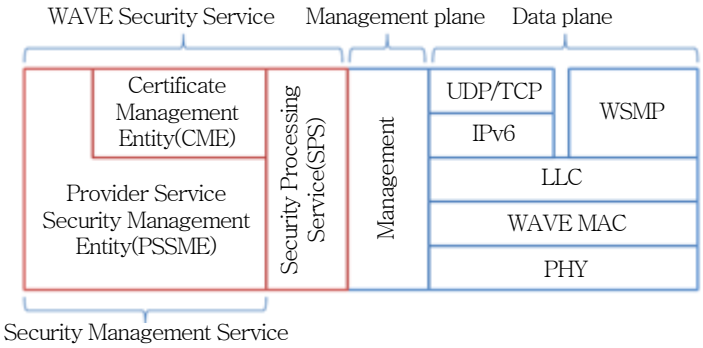
IEEE 1609.2 에서는 WAVE 기술을 위한 보안 서비스를 정의한다[4]. WAVE 메시지에 대한 인증 메커니즘 및 사용자에 대한 인증 메커니즘을 제공한다. 주의할 사항은 사용자 보호를 위한 익명 인증 메커니즘에 관해서는 여전히 표준화가 진행중이며, 현재 버전의 표준에서는 포함하고 있지 않다.

(1) WAVE 보안 구조

WAVE 는 (그림 3)과 같이 데이터 처리부(Data plane), 관리 처리부(Management plane), WAVE 보안 서비스(Security service)로 구분되어 정의된다.

WAVE 보안 서비스는 아래의 두 가지 서비스로 구성된다.

- 보안 처리 서비스(Security processing service): 데이터 및 WSA(Wave Service Advertisement)를 안전하게 전송하기 위한 보안 처리 기능(암호화, 디지털 서명 등)을 담당한다.
- 보안 관리 서비스(Security management service): 보안 관리 서비스는 인증서 관리 기능을 담당하는 인증서 관리 개체(Certificate Management Entity: CME)와 안전한 WSA 전송을 위해서 사용되는 인증서 및 개인키와 연관된 정보의 처리 기능을 제공하는 서비스 제공자 보안 관리 개체(Provider Service Security Management Entity: PSSME)로 구성된다.



(그림 3) WAVE 보안 구조

보안 처리 서비스는 안전하지 않은 PDU(Protocol Data Unit)와 안전한 PDU 사이의 데이터 변환 기능을 수행한다. 즉, 메시지에 대한 암호화 또는 디지털 서명을 생성하고, 암호화된 메시지에 대한 복호화, 디지털 서명된 데이터의 검증 기능을 수행한다. 또한, WSA 에 대한 디지털 서명 생성 및 검증 기능을 담당한다. 그리고, 보안 서비스를 제공하기 위한 개인키와 인증서를 저장하는 기능을 제공한다.

보안 관리 서비스의 CME 는 보안 처리 서비스가 저장하고 있는 개인키와 연관된 인증서의 취소 정보, 상대방 개체의 개인키와 연관된 인증서의 취소 정보 및 근원 인증서(Root certificate)를 관리한다. 또한, CME 는 현재 수신한 데이터가 이전에 수신한 데이터와 일치하는 지 비교하는 기능을 수행한다.

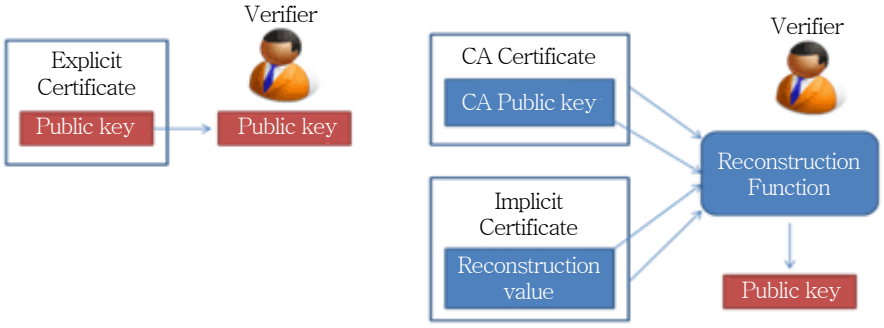
보안 관리 서비스의 PSSME 는 WME(Wave Management Entity)에게 보안 관리 정보를 제공한다. PSSME 는 임의의 보안 관리 서비스의 유일한 ID 인 지역 서비스 보안 인덱스(Local Service Index for Security: LSI-S)를 관리하고, 인증서 관리에 필요한 보안 파라미터를 등록하며, WME 가 WSA 를 서명하기 위해 사용되는 인증서 및 개인키를 보안 처리 서비스에게 전달하는 기능을 담당한다. 또한, 반복되는 WSA 의 빠른 검증을 위해 가장 최근에 수신한 서명된 WSA 를 저장하는 기능을 제공한다.

(2) 인증서의 종류

인증서가 정의하고 있는 정보는 다음과 같다.

- 인증서 소유자(개인키를 사용하는 개체)의 공개키
- 공개키와 연관된 허용 범위 정보
- 인증서 발급자의 ID

인증서는 인증 대상에 따라 차량을 인증하기 위한 개체 인증서와 개체 인증서를 인증하기 위한 CA 인증서로 구분된다. 또한, 공개키 제공 형태에 따라 공개키가 인증서에 명시적으로 제공되는 명시적 인증서와 공개키를 구하기 위해 추가적인 연산이 필요한 암시적 인증서로 구분할 수 있다. (그림 4)는 명시적 인증서와 암시적 인증서의 차이점을 나타낸 것이다. 명시적 인증서인 경우에는 공개키가 인증서에 명시적으로 기술되어 있어서 디지털 서명을 검증할 때 해당 공개키를 인증서로부터 직접적으로 획득이 가능하다. 반면에, 암시적 인증서인 경우에는 CA 인증서의 해시, 개체 인증서의 해시, CA 인증서의 CA 공개키 및 개체 인증서의 재구성 정보를 이용하여 개체의 공개키를 획득하기 위한 추가적인 처리



(그림 4) 명시적 인증서와 암시적 인증서의 개념

가 필요하다.

(3) 암호 메커니즘

IEEE 1609.2 표준에서는 아래의 3 가지 암호 기술이 적용된다.

- 타원 곡선 전자 서명: ECDSA(Elliptic Curve Digital Signature Algorithm)
- 타원 곡선 암호를 이용한 비대칭 암호화: ECIES(Elliptic Curve Integrated Encryption Scheme)
- 대칭키 기반의 인증 및 암호화: AES-CCM(Advanced Encryption Standard Counter with cipher block chaining message authentication code)

<표 2>는 요구되는 기능에 적용되는 암호 알고리즘의 명칭 및 참조 표준을 나타낸 것이다. 디지털 서명 알고리즘은 FIPS 186-3 의 ECDSA 를 적용하며, P-224, P-256 타원곡선을 이용한다. 공개키 암호화 알고리즘은 IEEE 1363a 에 정의된 ECIES 를 이용하며, P-256 타원곡선과 내부 해쉬 알고리즘은 SHA-256 을 이용한다. 데이터를 암호화하기위한 대칭키 알고리즘은 NIST FPS-197 에 정의된 AES 를 이용하며, 블록암호 운영모드는 NIST SP-800-38C 에 정의된 CCM 모드를 적용한다. ECDSA 또는 ECIES 에 사용되는

<표 2> IEEE 1609.2 에 적용되는 암호 알고리즘

명칭	기능	참조 표준	비고
ECDSA	디지털 서명	FIPS 186-3	P-224, P-256
ECIES	공개키 암호화	IEEE 1363a	P-256, SHA-256
AES-CCM	대칭키 암호화	FIPS 197 NIST SP 800-38C	
SHA-256	해쉬	FIPS 180-3	

키 쌍의 생성은 FIPS 196-3 Annex B.4 를 따르며, 키 쌍의 검증은 IEEE 1363-2000 을 따른다

4. 결론

본 고에서는 차량 통신시스템의 개요 및 차량 통신 보안 요구 사항에 대해 분석하였고, 또한, 현재 차량 통신 보안 기술로서 표준화가 진행중인 IEEE WAVE 보안 기술에 대해 살펴 보았다.

오늘날 차량에서 전자 부품이 차지하는 비중이 급속도로 증가하고 있다. 즉, 차량은 더 이상 기계적인 부품의 집합체가 아니라, PC 같은 컴퓨팅 디바이스의 일종으로 간주할 필요가 있다. 따라서, 지능형 차량은 정보화의 역기능을 방지하기 위한 정보 보호 기술이 필수적으로 요구된다. 특히, 차량 네트워크 환경은 기존의 인터넷 등의 네트워크 환경과 달리 네트워크의 보안성 확보 여부가 운전자의 생명과 직결되는 위험 상황을 유발할 수 있으므로, 지능형 교통시스템을 위해서는 반드시 보안 인프라 기술의 확보가 선행되어야 한다. 또한, 차량 네트워크 환경에서 하나의 차량에 발생한 보안 사고가 타 차량에 미치는 파급 효과가 크다는 것을 고려할 때, 차량 간 통신 보안 인프라 뿐만 아니라 단일 차량의 임베디드 보안 연구의 중요성도 부각되고 있다. 그러나, 차량 네트워크는 차량의 고속 이동성 및 네트워크 토폴로지의 잦은 변화 등의 특성으로 인해 기존의 네트워크 보안 기술로는 한계가 있다. 따라서, 안전한 지능형 교통시스템의 구축을 위해서는 차량 네트워크에 특화된 보안 기술 개발의 중요성을 인식하고, 이에 대한 연구가 진행되어야 할 것이다.

<참 고 문 헌>

[1] X. Lin et. al., “Security in Vehicular Ad Hoc Networks,” IEEE Communications Magazine, April 2008 pp.88-95.

[2] P. Papadimitratos et. al., “Secure Vehicular Communication Systems: Design and Architecture,” IEEE Communications Magazine, Nov. 2008 pp.100-109.

[3] PRESERVE(PREeparing SEcuRe VEhicle-to-X Communication Systems) Deliverable 1.1, “Security Requirements of Vehicle Security Architecture,” June 2011.

[4] IEEE 1609.2/D.12, “Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages,” Jan. 2012.