6

차량통신을 위한 보안 및 프라이버시 보호 기술

목포대학교 ▌김 현 곤

1. 서 론

차량통신 기술은 차량과 무선통신, 컴퓨터, 인터넷, 인공지능과 결합하는 융합기술로 차량 안전 및 진단, 텔레매틱스, ITS 등의 향상된 서비스를 형성하면서 빠르게 진화하고 있다. 차량통신 기술은 운전자에게 교통정보 안내, 긴급구조, 인터넷 서비스를 제공하여 편리함과 안전성을 증대시켜 준다. 그리고 새로운 부가가치를 얻을 수 있을 뿐만 아니라 잠재 시장이 매우 큰 기술로 주목받고 있다. 이와 관련하여 미국의 경우 VII 프로젝트를 통해 국가차원의 교통정보와 차량 안전 서비스를 추진하고 있으며 자동차 회사 중심의 VSCC 컨소시엄은 차량간 통신을 이용한 차량안전 서비스 기술을 개발하고 있다. 유럽의 경우는 보다 안전하고 지능적이며 고품질의 이동성을 제공하겠다는 비전을 가지고 eSafety 포럼을 구성하고 다수의 프로젝트를 통해 활발한 연구를 진행하고 있다. 국내에서도 한국전자통신연구원 중심의 차량 멀티홉 통신에 관한 연구와 한국정보통신기술협회 주도의 표준화가 진행 중이다[1-2]

차량통신 기술은 deployment 단계에 직면해 있다. 그러나 강력한 보안과 프라이버시 보호 기술이 결합되지 않으면 상대적으로 간단한 공격만으로도 전체 시스템이 무력화되고 치명적인 인명 피해로도 연결될 수 있다. 특히 무선통신을 이용하는 차량 네트워크는 악의적인 공격자에 의해 네트워크가 쉽게 오염되기 쉬운 특징을 가지고 있다. 구체적인 예를 들어보면 공격자가 실제 상황과 무관하게 주변 차량에게 인증되지 않은 교통사고나 긴급 경고를 보낸다고 가정해보자. 급감속을 하는 차량들에 의해 교통사고가 발생하거나 교통 체증이 유발될 수 있다.

공격자는 침해된 노드를 이용해 통신 중인 메시지를 위변조하고, 거짓 정보로 오염시키고, 거짓 메시지를 삽입하고, 수신된 메시지를 공격 목적으로 재전송하고, 다른 차량의 통신 장애를 초래할 목적으로 재밍 신호를 발생시키고, 다수의 수신기를 배치하여 차량을 위치를 추적하거나 정보를 수집할 수 있다. 또한 다수의 차량들이 협업하여 정상적인 차량을 교란하여 교통사고나 교통체증 등을 유발시킬 수도 있다. 다수의 공격 노드들은 서로 다른 위치에 있는 네트워크에 존재할 수도 있다. 공격자들은 독립적으로 또는 공격을 극대화하기 위해 정보 교환을 통해 협업적인 공격을 수행할 수 있다. 시간이 지날수록 공격자들의 수나 위치가 변할 수 있으며 이로 인해 영향을 받는 차량들이 증가할 수 있다.

이와 같은 여러 가지 취약성에도 불구하고 차량통신에서의 보안과 프라이버시 보호는 최근에서야 다루어지고 있는 문제들이다. 본 글에서는 대표적인 차량통신 보안 기술로서 유럽의 SeVeCom 프로젝트에서 제시하고 있는 차량통신 보안 및 프라이버시 보호 기술에 대해 소개한다[3-5]. 기술적인 목표는 프라이버시 보호를 위한 차량의 익명성을 어떻게 제공할 것인지 그리고 보안 기능 탑재로 인한 프로세싱 오버헤드를 최소화하고 통신 대역을 어떻게 효율적으로 사용할 것인지에 두고 있다. 특징으로는 물리적 노출에 안전한 변형 억제성(temper resistant)을 갖는 하드웨어 안전 모듈 장착, 안전성과 무결성 그리고 프라이버시 보호를 위한 익명성 인증 기법 도입, 모든 메시지에 전자서명을 하여 안전한 통신 추구, 차량위치 추적을 어렵게 하는 혼합 존의 도입 등을 들 수 있다. 본 글의 구성은 다음과 같다. 일반적인 차량통신에서의 보안 요구사항을 먼저 제시하고 차량통신 보안 개요와 익명 인증 기법의 개념을 소개한다. 그리고 인증서 관리와 암호학적인 지원 기술과 안전한 통신을 위한 요소 기술들 즉, 안전한 비컨, 안전한 멀티캐스트, 혼합 존 등의 개념을 소개한다. 글 후반에는 구현에 필요한 구조와 차량내 보안 그리고 소프트웨어 시뮬레이션을 통해 도출된 성능 분석 결과의 일부를 제시한다.

2. 보안 요구사항

차량통신 네트워크는 차량 내부망과 외부망으로 구분할 수 있다. 차량 외부망의 통신은 차량과 차량(V2V) 사이의 통신과 차량과 인프라(V2I) 사이의 통신으로 분류된다. 다음은 주로 차량 외부망의 통신에서 필요한 보안 요구사항이다.

- o 메시지 인증 및 무결성
  - 메시지 수신자가 메시지 송신자를 식별할 수 있어야 하고 메시지가 변경되지 않았음을 보장해야 한다.
- o 메시지 부인방지
  - 메시지 송신자가 메시지를 보낸 다음 이를 부인하는 것을 방지해야 한다.
- o 엔티티 인증
  - 통신 상대자인 송신자가 생성한 메시지이고 송신자의 활성(liveness) 상태를 확인할 수 있어야 한다. 다른 표현으로는 수신된 메시지가 일정 시간 구간 [t-δ, t]내에 생성되었음을 확인하는 것이다. 여기서 t는 수신자의 현재 시간이고 δ는 0보다 크고 아주 작은 양의 값이다.
- o 접근 제어
  - 노드들의 역할에 따른 접근 제어와 시스템에서 허용할 수 있는 범위를 제한할 수 있어야 한다.
- o 권한 관리
  - 접근제어의 일부로서 네트워크내의 각 노드들에게 협약에 따른 권한을 부여할 수 있어야 한다.
- o 메시지 기밀성
  - 메시지를 오직 인가된 엔티티에게만 공개하는 것이며 전송되는 메시지의 내용을 완벽하게 보호하여 알아보지 못하게 해야 한다.
- o 추적성
  - 시스템 엔티티들의 보안 관련 이벤트가 관리자에 의해 추적될 수 있어야 한다.
- o 프라이버시 보호
  - 차량통신 사용자들의 민감한 개인 정보 즉, 차량의 시간, 위치, 차량 ID, 이동 정보 등의 차량과 관련된 프라이버시 정보를 안전하게 보호할 수 있어야 한다.
- o 가용성
  - 프로토콜과 서비스가 장애 상태나 침해당하더라도 가용될 수 있는 회복력을 가져야 한다. 자원 고갈 공격에 대한 회복력과 장애를 제거한 후에 정상적인 오퍼레이션을 재기하는 즉, 자체 회복력을 갖는 프로토콜이 적용되어야 한다.

표 1 차량통신 응용의 특징과 보안 요구사항의 중요도

	특징			요구사항		
응용	안전응용	V2V/V2I	멀티홉	인증	무결성	프라이버시
교차로 혼잡 경고	o	V2V		2	2	2
위험 차량 신호	o	V2I	o	2	2	0
작업구간 경고	o	V2I	o	1	2	0
전방 혼잡 경고	o	V2V	o	2	2	2
상호협력 적응형 크루즈 제어		V2V	o	2	2	2

대표적인 차량통신 응용에 대한 특징과 보안 요구사항을 표 1에 나타내었다. 여기서 값이 크면 요구사항의 중요도가 높다는 의미이다[6].

3. 차량통신 보안 개요

보안 관점에서 도식한 차량통신 보안의 개요를 그림 1에 나타내었다. 기존의 차량통신 네트워크와 비교해 보면 추가적으로 인프라측에 인증서 관리를 위한 인증기관(CA)이 연결된다. 차량에는 하드웨어 보안 모듈이 탑재되어 암호 키와 인증서가 관리되고 암호 오퍼레이션이 수행된다. 이를 기반으로 비컨 메시지를 포함하여 V2V와 V2I간 안전한 통신을 이루며 차량들간에는 안전한 싱글 홉 또는 멀티 홉 라우팅이 이루어진다. 차량통신에서 차량의 위치는 안전하게 관리되어져야 할 매우 중요한 데이터 중의 하나이다. 각 차량은 자신의 위치나 자신의 이웃에 위치한 다른 차량의 위치를 알아야 한다. GPS 신호는 약하고 스푸핑될 수 있고 재밍에 취약하다. 또한 차량들은 그들의 위치를 고의적으로 속일 수도 있다. 따라서 차량의 위치와 관련한 추적 기능과 권한 제어를 할 수 있는 안전한 포지셔닝 기술이 요구된다.

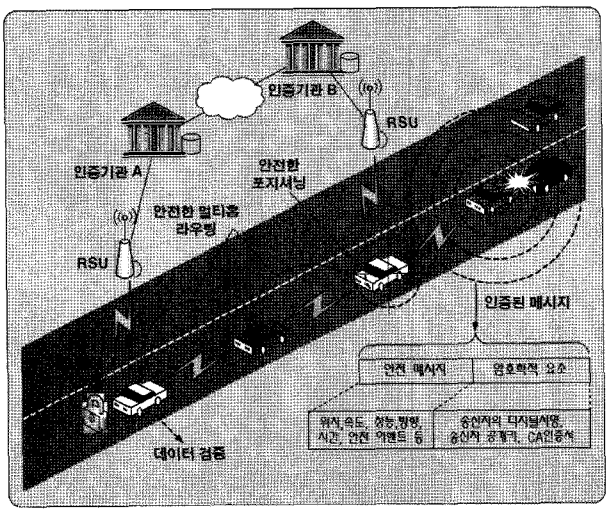

그림 1 차량통신 보안 개요

인증기관은 기존의 전자서명 및 암호화를 위한 디지털 인증서를 발급하고 관리하는 역할을 수행하며 계층적인 인프라를 사용한다. 인증기관은 차량과 관련하여 기본적으로 개체 식별과 자신의 영역에 등록된 차량 노드의 인증서를 관리한다. 인증기관들은 서로 다른 지역의 노드들간에 인터렉션을 가능하게 하기 위해서 교차 인증서(cross certificate)를 제공하거나 또는 관리 지역을 벗어날 경우에는 외부 인증기관을 통해 방문자 인증서(foreigner certificate)를 발급한다.

각 노드는 오직 하나의 인증기관에 등록하며 유일한 장기 식별자(long-term identity)와 공개키와 개인키 쌍 그리고 장기 인증서를 차량에 장착한다. 인증서에는 차량의 특성을 나타내는 속성과 유효기간이 포함된다. 인증기관은 노드의 제거 또는 침해된 암호키를 철회하기 위해 인증서를 폐기하는 역할을 수행한다. 차량 노드의 보안 구조를 그림 2에 나타내었다. 안전한 통신에서 V2CA는 V2I의 일부이며 차량과 인증기관과의 인터렉션을 의미한다. 차량통신 보안에서는 위치 정보를 보호하고 차량의 익명성을 보장하기 위해 장기 인증서와 단기 인증서 그리고 장기 공개키와 단기 공개키를 별도로 두고 오퍼레이션을 수행한다.

하드웨어 보안 모듈(HSM)은 서명 생성을 위한 개인키를 저장하며 차량과 RSU(Road Side Unit)를 위한 안전한 기준시간을 제공한다. 그리고 암호학적 오퍼레이션을 제공하는 중요한 장치이며 물리적 노출에 안전한 변형 억제성을 갖는다. HSM이 물리적으로 해체되어 개인키가 노출되면 모듈은 자체적으로 민감한 중요 개인키를 모두 지운다. 이를 통해 중요한 비밀키가 공격자에 의해 노출 및 탈취되는 것을 막는 것이다. 그리고 민감한 정보가 물리적으로 안전한 HSM 환경을 벗어나지 않음을 보장하기 위해서 저장된 키를 이용해 모든 개인키 암호 오퍼레이션을 실행한다. HSM

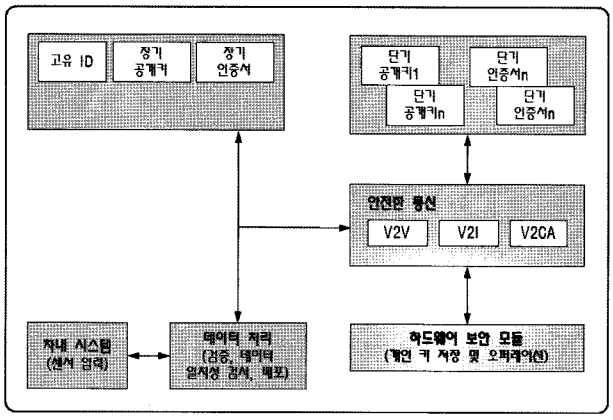

그림 2 차량 노드의 보안 구조

이 없으면 비밀 키는 쉽게 훼손될 수 있기 때문에 차량통신 보안의 핵심적인 요소라 할 수 있다.

차량통신 보안에서는 기본적으로 암호학적인 안전성과 무결성을 동시에 보장하기 위해 익명성 인증(pseudonymous authentication) 기법을 도입하였다. 그리고 모든 메시지에 대해 디지털 서명을 한다. 익명성 인증이란 장기 개인키/공개키를 사용하는 정적인 기존 방식과는 다르게, 다수의 단기 개인키/공개키 쌍과 단기 익명 인증서를 이용하고 짧은 기간마다 변경하는 방식을 말한다. 단기 인증서와 장기 식별자의 매핑은 신뢰할 수 있는 제 3자인 인증기관에 의해 이루어진다. 익명 인증서 형식을 그림 3에 나타내었다. 여기서 익명 인증서 제공자는 인증기관에 해당하며 차량 익명성을 제공하기 위해 차량의 식별자는 포함되지 않는다.

차량은 짧은 기간 동안에 다수의 익명 인증서 중 하나를 사용하며 정해진 유효기간이 만료되면 이전에 사용하지 않은 새로운 익명 인증서로 교체한다. 단기 익명 인증서를 이용하여 메시지를 서명함으로써 얻을 수 있는 장점은 메시지들이 서로 다른 공개키로 서명되기 때문에 메시지간 연관성을 찾기 힘들고 메시지들을 서로 링크하기가 어려워진다는 것이다. 서명은 메시지 페이로드, 타임스탬프, 송신자 정보를 포함하여 생성되며 프로토콜 기능에 따라 메시지 생성자 외에도 중간 노드들에 의해 생성될 수 있다. 이 외에 차량통신 보안에서는 주기적으로 송신되는 비컨 메시지의 안전성, 송신자로부터 정해진 홉간 거리 또는 특정 영역내에서의 한정된 메시지 플러딩의 안전성 그리고 중계 노드들이 하나의 루트를 통해 메시지를 전송할 수 있는 위치 기반 라우팅 등의 안전성도 제공한다.

4. 인증서 관리와 암호학적인 지원

인증기관은 단기 인증서와 장기 인증서를 관리하며 장애나 인증서 취소 사유가 발생할 경우 특정 노드에 대한 인증서를 폐기한다. 그리고 장기 식별자와 노드들의 통신 내용을 매핑하여 노드 추적이 가능하도록 한다. 시스템의 안전성을 담보하기 위해서 공개키 오퍼레이션은 온보드유닛(OBU)에 의해 수행되지만 모든 개인키 오퍼레이션은 HSM에 의해 수행된다.

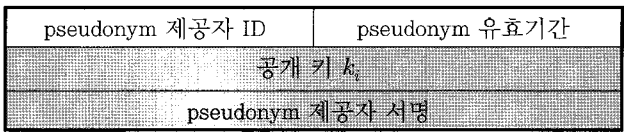

그림 3 익명 인증서 형식

4.1 장기 식별자

하나의 노드 X는 유일한 장기 식별자 ID_X를 갖는다. 이 식별자는 차량의 식별자 번호(VIN)와 유사하게 차량 제작사와 인증기관과의 상호 동의에 의해 생성된다. 차량뿐만 아니라 RSU도 동일한 형식의 식별자를 사용한다. ID_X는 하나의 암호키 쌍인 개인키와 공개키 (SK_X, PK_X) 그리고 노드 X의 속성들과 매핑된다. 속성으로는 노드 장비의 기술적인 특성들 즉, 노드 형태, 크기, 센서, 컴퓨터 플랫폼, 전체 시스템 내에서 노드의 역할 등이 포함된다. 노드 형태로는 개인용 차량, 공용 차량, RSU 그리고 경찰차와 같은 특수 목적의 차량 등으로 구분된다. 장기 식별자의 할당, 각 노드의 특성을 반영한 속성의 선택 그리고 인증서 발행은 노드가 인증기관에 등록하는 시점에서 오프라인으로 수행된다. 인증서의 유효기간은 차량의 수명을 반영하여 장기간으로 지정되어야 한다.

4.2 단기 식별자

차량 보안에서는 단기 식별자로서 익명 인증서를 사용한다. 단기적인 익명 인증서를 얻기 위해서 차량 V의 HSM은 암호키 쌍 $\{(SK_V^1, PK_V^1), \ldots\ldots (SK_V^n, PK_V^n)\}$의 셋을 생성하고 안전한 통신채널을 통해 공개키들을 자신이 등록한 인증기관에게 전송한다. 차량 V는 인증기관이 자신을 인증할 수 있도록 장기 식별자 ID_V를 제공한다. 인증기관은 공개키들 PK_V^i를 서명하고 차량 V를 위한 단기적인 익명 인증서 셋을 생성한다. 익명 인증서에는 그림 3에 나타낸 바와 같이 인증기관 식별자, 익명 인증서의 유효기간, 공개키 그리고 인증기관의 서명을 포함한다. 여기서 차량의 식별자를 포함시키지 않는 이유는 공격자가 차량을 식별할 수 없도록 하여 차량 익명성을 보장하기 위해서이다.

익명 인증서들은 보드내 익명 인증서 풀에 저장되어 관리되며 HSM에 저장되어 있는 단기 개인키와 매핑된다. 이를 통해 각각의 차량은 정확하게 하나의 키 쌍인 공개키와 개인키를 특정 시간 동안 활성화 시킨다. j키 쌍 (SK_V^j, PK_V^j)가 $j+1$번째 키 쌍 (SK_V^{j+1}, PK_V^{j+1})으로 변경되면 PK_V^j가 아직 만료되지 않았더라도 SK_V^j로 메시지 서명을 더 이상 하지 않는다. 즉 불법 차량이 짧은 시간 동안에 서로 다른 SK_V^j를 가지고 다수의 비컨에 서명을 할 수 없게 함으로써 익명성을 보장받을 수 있다. 한편 차량은 새로운 익명 인증서 셋을 얻기 위해서 주기적으로 인증기관과 인터렉션 한다. 예를 들어 현재 익명 인증서 셋 i를 사용하고 있다면 $i+1$번째 셋을 획득한다. 이후 i번째 셋에 있는 익명 인증서를 다 사용하였다면 사전에 얻은 $i+1$번째 셋을 사용한다. 이런 절차를 익명 인증서 재충전이라 한다. 인증기관은 차량의 장기 식별자와 생성한 익명 인증서들을 저장하여 추적이 가능하도록 한다. 따라서 나중에 필요 시 익명 인증서 리스트를 통해 차량의 장기 식별자와 익명 인증서들의 링크를 찾아낼 수 있다.

한편 짧은 시간내에 동일한 익명 인증서가 사용되기 때문에 공격자는 그 시간 동안 차량의 활성화 상태를 링크할 수 있다는 문제점이 존재한다. 이를 차단하기 위해 익명 인증서를 자주 변경하여 공격자가 차량 및 그 차량의 이동경로 그리고 메시지를 링크하는 것을 어렵게 만든다. 또한 익명 인증서내에 해당 공개키를 생성한 인증기관 A의 식별자가 포함된다는 것은 그 차량이 인증기관 A에 등록한 모든 차량 셋의 하나라는 것을 알 수 있다는 문제가 존재한다. 이를 차량 V의 익명성이라 한다. 예를 들어 스위스 차량은 모든 스위스 차량들의 셋내에 포함된 익명성이 된다는 것이다. 이러한 추론을 막기 위해 외부 영역을 가로질러 움직이는 차량들은 현지의 인증기관 B로부터 단기간 인증서를 획득한다. 예를 들어 차량 V는 인증기관 A에 등록했지만 인증기관 B에게 검증을 받을 수 있다. 또한 인증기관 B로부터 익명 인증서를 획득한 다음 영역 B에서만 사용할 수 있다. 이러한 방법들을 통해 차량 V가 영역 B에서 임의의 관측자에 의해 쉽게 추적되는 것을 차단할 수 있다.

4.3 하드웨어 보안 모듈

HSM은 물리적으로 OBU와 분리되어지며 물리적인 공격이 발생했을 때 개인 키 요소들이 노출되지 않도록 변형 억제성을 가진다. HSM은 중앙처리장치, 비휘발성 메모리, 자체 내장형 클럭, 입출력 인터페이스, 변형 탐지 및 변형 방지 기능을 가진다. 주로 디지털 서명 생성과 암호화된 메시지를 복호화하는 암호학적 오퍼레이션과 비밀키 및 디바이스를 관리한다. 모든 메시지를 디지털 서명함으로써 안전한 통신을 보장받는다. HSM은 항상 재생공격을 탐지하기 위해서 자신이 생성한 모든 서명에 타임스탬프를 포함시킨다. 복호화는 익명 인증서 처리 응용에 의해 주로 수행된다. HSM은 차량의 단기 식별을 위해 단기 키를 사용하며 장기 식별을 위해 장기 키를 사용한다. 이 키들은 HSM에 의해 생성되며 장치의 외부로는 오직 공개키만 공개된다. 단기 키의 생성은 OBU에서 실행되는 모든 응용에 의해 시작될 수 있다. 이와는 달리

장기 키는 차량 제작시점에 생성된다. 그러나 필요에 따라 신뢰할 수 있는 인증기관을 통해 추후에 갱신될 수도 있다.

인증기관에 의해 서명된 명령어를 통해 장치 관리가 이루어지며 장기 키가 갱신된다. 서명된 명령어를 검증하기 위하여 HSM은 신뢰할 수 있는 루트 공개키를 저장하며 안전한 환경에서 초기화 절차를 통해 장치로 로딩한다. 인증기관에 의해 만들어진 개인키와 일치시켜 두 개의 루트 공개키 K_1과 K_2를 둔다. 만약 인증기관의 비밀키 중 하나가 침해되었다면 이와 일치하는 공개키 K_1은 폐기시킨다. 취소 명령은 K_1과 일치하는 개인키에 의해 반드시 서명되어야 한다. 한 때 K_1이 폐기되면 새로운 키 K_1'이 K_2와 일치하는 개인키로 서명된 명령어에 의해 HSM에 로딩된다. 그리고 K_1이 폐기되었을 때 HSM은 더 이상 K_2를 취소하는 명령어를 수행하지 않는다. 이러한 기법을 통해 두 개의 루트 키가 동시에 침해되지만 않는다면 루트 키 갱신이 안전하게 이루어질 수 있다. 한편 차량은 암호 키와 인증서를 보유한다. 그러나 차량 노드가 인증서를 소유했다는 사실만으로 노드의 정확한 오퍼레이션을 보장할 수 없다. 예를 들어 HSM이 장착된 OBU가 위조되고 내부 기능이 변조될 수 있다. 또한 차량이나 RSU의 암호 키가 물리적인 공격으로 인해 노출될 수 있고 공격 장치에 의해 불법으로 사용될 수 있다. 이 경우 다수의 동일한 키가 다수의 노드에서 나타날 수 있다.

4.4 인증서 취소 목록 배포 및 폐기

비정상적인 동작을 하는 노드의 인증서나 공격에 오염된 인증서들은 차량통신 네트워크에 악영향을 줄 수 있으므로 반드시 폐기되어야 한다. 이 외에도 관리적인 목적이나 기술적인 이유로 인증기관에 의해 폐기가 결정될 수 있다. 인증서 폐기를 위한 기본적인 메커니즘은 인증기관이 생성하고 인증할 수 있는 인증서 취소 목록(CRL)을 활용한다. CRL이란 해지되었거나 더 이상 유효하지 않은 인증서의 리스트를 말한다. 차량통신에서 CRL을 효율적으로 배포하는 방법을 그림 4에 나타내었다.

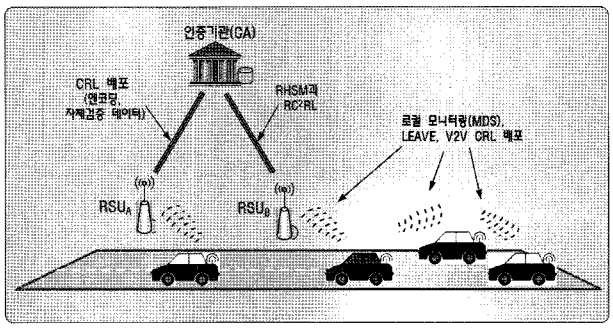

그림 4 인증서 취소 목록(CRL) 배포

CRL을 배포하기 위해서 도로측 인프라나 사전에 CRL을 획득한 이웃 차량들을 이용한다. 실험에 의하면 평균 수 Km 떨어진 곳에 RSU를 위치시키고 각 RSU에 초당 수 킬로비트로 CRL을 분배하는 환경에서 차량들은 통근 시간 동안에 대략 수백 킬로바이트의 CRL을 얻을 수 있다[7]. 여기서 CRL은 암호학적으로 자체 검증할 수 있는 작은 조각 단위로 엔코딩되고 이 조각들은 저속의 브로드캐스트 통신을 통해 전달된다. RSU가 없는 지역에서는 RSU와 이전에 접촉한 차량이나 또는 이동통신과 같은 다른 통신 기술을 사용하여 V2V로 CRL을 배포한다. CRL의 데이터 크기와 분배되어야 할 전체 정보의 양에 대해서는 분석이 더 필요하다. CRL에는 단지 지역적인 인증서 폐기 정보를 포함시키고 CA들간에 상호 연동을 통해 CRL 데이터 크기를 줄이는 방법도 제시되었다[7].

인증서 폐기는 인증기관이 주도하여 HSM 폐기 프로토콜(RHSM)을 이용하는 방법이 제시되었다[7]. 인증기관이 루트 공개키와 연관된 비밀키를 사용하여 *Kill* 명령어를 서명하고 실행시킨다. 인증기관은 차량의 위치를 확인하고 가장 가까운 RSU를 통해 *Kill* 명령어를 보낸다. HSM은 장기 서명 생성키 SK_X를 지우기 이전에 ACK 명령어로 응답하여 *Kill* 명령어를 정상적으로 수신했음을 알린다. HSM이 명령어를 수신하면 침해된 모듈의 인증서를 없애고 새로운 키 생성을 막기 위해 자신의 개인키를 포함하여 자신의 메모리에 있는 모든 내용을 삭제한다. 만약 RSU를 통한 통신이 실패하면 즉, 타임아웃 시간내에 ACK를 수신하지 못했다면 인증기관은 명령어를 브로드캐스트로 전달한다. 만약 공격자에 의해 인증기관과 HSM 간 통신이 제어되는 환경을 고려한다면 압축된 CRL을 이용한 폐기 프로토콜(RC^2RL)을 이용하여 인증서를 안전하게 폐기할 수 있다[8]. 이 프로토콜은 손실이 있는 압축 기법 즉, 블룸필터를 이용하여 CRL의 데이터 사이즈를 줄인다.

CRL에 인증서를 포함한다는 것은 그 노드를 폐기하기 위해 인증기관과의 설정이 필요하다는 의미이다. 만약 폐기가 장애 때문이라면 탐지가 더 어려워진다. 또한 CRL이 하루에 한번 정도 밖에 이슈화되지 않으므로 고장 노드가 폐기되기 전까지 잠재적인 취약점을 가지고 있다. 이를 위해 이상 행위 차량을 검출하여 그 차량을 제외시킬 수 있는 MDS(Misbehavior Detection

System)와 LEAVE(Local Eviction of Attackers by Voting Evaluators) 기법이 제시되었다[8]. 전자는 이상행위 노드의 근처 노드들이 이상행위를 검출하며 로컬 차량통신 오퍼레이션을 통해 그 노드를 제거한다. 후자는 이상행위 평가자들이 인증기관에게 이상행위 노드를 보고하며 그 노드는 인증기관에 의해 폐기된다.

5. 안전한 통신

5.1 안전한 비컨

비컨은 주기적으로 원 홉 브로드캐스트를 하는데 사용된다. 비컨 패킷은 근처에 있는 이웃 차량들이 네트워크 토폴로지를 잘 인식할 수 있도록 차량의 위치, 속도, 그리고 방향과 같은 송신자의 상태 정보를 포함한다. 비컨 패킷의 브로드캐스팅 횟수는 대부분의 경우에 1Hz에서 10Hz 범위이다. 차량통신 보안에서 비컨 메시지들은 디지털 서명되며 송신자의 인증서가 첨부된다. 송신 노드 V는 비컨 메시지를 어셈블리한 후 현재 사용하고 있는 j번째 인증서 PK_V^j에 해당하는 비밀키 SK_V^j를 이용하여 메시지를 서명(sig(m))한다. 여기에 타임스탬프와 전송하는 시점의 지리적인 위치인 geo-stamp 그리고 인증서 $Cert_A(PK_V^j)$를 첨부한다. 수신측은 첨부된 인증서의 PK_V^j와 SK_V^j를 이용하여 메시지 서명을 검증한다. 이 절차를 그림 5에 도식하였다.

이 절차를 통해 네 가지의 목적을 달성할 수 있다. 첫째로 수신자는 비컨 메시지를 수신하여 차량통신에 적법한 참여 노드 즉, 적법한 차량 또는 RSU가 송신했다는 것을 검증할 수 있다. 둘째로 노드 자신의 HSM이 침해되지 않고서는 다른 노드로 가장할 수 없다. 셋째로 만약에 서명이 유효하지 않다면 조작임을 알 수 있으므로 이를 통해 메시지의 무결성을 보장받을 수 있다. 마지막으로 서명과 함께 geo-stamp를 사용함으로써 재생공격을 검출할 수 있다.

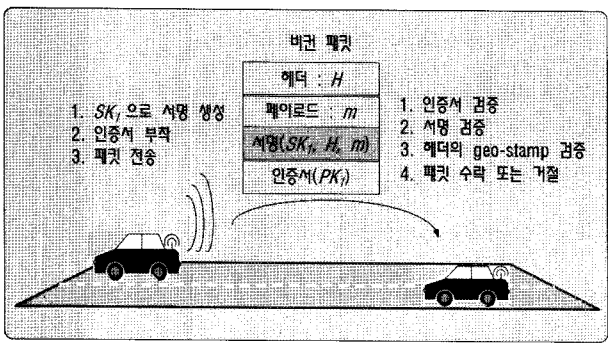

그림 5 차량통신에서의 안전한 비컨

5.2 안전한 통신 이웃 노드 발견

이웃 차량들이나 인프라와 통신을 하기 위해서는 차량들은 직접적으로 근접할 수 있는 차량이나 RSU들 즉, 통신 이웃 노드를 발견하는 것이 기본적으로 필요하다. 다른 노드들과의 협력이나 안전 메시지 전송을 통해 차량은 물리적으로 근접한 다른 차량들의 정보를 수집해 네트워크 토폴로지를 구성한다. 만약 두 개의 노드가 통신 이웃이라면 두 차량은 물리적으로 근접해 있다고 가정한다. 그렇지만 원격 노드들의 메시지를 수신하고 빠르게 재전송하는 재생공격이 이루어질 수 있으므로 이에 대한 고려가 필요하다. 차량통신 보안에서는 인증과 더불어 송신자의 타임스탬프와 위치를 포함시킴으로써 외부 공격에 대한 안전한 이웃 발견을 실행한다[9]. 기본적인 아이디어는 자신의 내부 시간과 수신된 타임스탬프의 시간 차이를 계산하고 수신된 메시지의 위치 그리고 자신의 좌표를 기준으로 하여 송신자와 수신자의 거리를 예측하는 것이다. 수신 노드는 송신자가 인증되고 자신이 예측한 두 노드의 거리가 일치하였을 때 송신 노드를 통신 이웃으로 인정한다. 이 후 차량은 자신의 통신 이웃 테이블에 인증된 송신 노드를 포함시킨다.

5.3 안전한 멀티캐스트

원 홉 비컨 패킷이 도달되는 범위는 가끔 충분하지 않을 수 있고 상대적으로 넓은 영역으로 전파해야 하는 경우 예를 들어 차량사고와 같은 이벤트들이 있다. 이를 해결하기 위해서 다음의 특징을 갖는 멀티캐스트를 이용한다.

- o 지리적인 목적지 영역을 설정
- o 목적지 영역으로 이벤트를 포워딩
- o 목적지 영역내에서 이벤트 패킷을 분배

위치기반 라우팅 즉, 멀티 홉 싱글 패스를 통해 지리적으로 구분된 목적지 영역으로 패킷을 포워딩하는 기법은 동적인 차량통신 네트워크에 매우 적합하다 할 수 있다. 위치기반 라우팅은 GPSR(Greedy Perimeter Stateless Routing) 또는 CGGC(Cached Greedy GeoCast)와 같은 라우팅 프로토콜에 의해 실현한다[10]. 목적지 영역내의 모드 노드들에게 메시지 분배는 간단한 플러딩 또는 멀티 홉 브로트캐스팅과 같은 좀 더 효율적인 방법을 이용할 수 있다. 간단한 플러딩의 경우 목적지 영역내의 모든 노드에게로 메시지를 한번 더 브로드캐스팅하며 동일한 메시지의 재브로드캐스팅을 막기 위해 순서 번호를 이용한다. 안

전한 위치기반 라우팅과 메시지 분배를 위해 송신노드는 생성된 메시지를 서명하고 안전한 비컨 패킷과 유사하게 인증서를 첨부한다. 그리고 중계 노드들은 다음 홉 릴레이에 의해 자신이 인증될 수 있도록 하기 위해 자신이 전송할 패킷에 서명을 한다[5]. 이 방법은 오직 검증된 네트워크 참여자만이 다른 노드들에 의해 수락될 수 있는 메시지들을 생성할 수 있게 해주며 메시지가 목적지로 향하는 경우에 무결성을 보장을 해준다.

비컨이 위치기반 포워딩을 하는데 결정적인 요소가 되기 때문에 비컨에 포함된 위치는 데이터 전송에 실패하고 공격자에 의해 트래픽에 추출될 경우 또는 라우팅 루프에 의해 네트워크 부하가 증가될 경우에는 거짓 정보로 오염될 수 있다. 차량통신 보안에서는 위치 위조를 검출할 수 있는 위치 검증 방법을 사용한다. 한편 프라이버시 보호를 위해 익명 인증서를 자주 변경하게 되면 노드가 유지하는 이웃 테이블이 안전성과 라우팅 성능을 감소시킨다. 네트워크 부하와 프라이버시 보호에 대한 균형을 맞추기 위해서 MAC 계층의 콜백을 적용할 수 있는 확장된 라우팅 메커니즘을 활용한다. 여기서 콜백은 테이블에 없는 통신 이웃 노드를 라우팅 계층에 알려주는 역할을 한다. 다수의 목적지로 그리고 고속으로 메시지를 분배하는 자원 고갈 공격을 완화시키기 위해서는 전송율을 적절하게 제한할 필요가 있다.

5.4 익명 인증서 처리

익명 인증서에는 공개키와 서명 결과가 첨부되므로 공격자는 충분한 시간을 가지고 분석하면 차량들의 위치를 추적할 수 있다. 이를 막기 위해 차량통신 보안에서는 짧은 시간 동안에만 사용할 수 있는 다수의 검증된 공개키 즉, 익명 인증서를 차량에게 부여한다. 만약 익명 인증서가 적절한 횟수와 위치에 따라 변경된다면 공격자는 서로 다른 익명 인증서를 가지고 서명한 메시지들에 대해 연관성을 링크하기가 어려워진다. 공격자가 차량 추적을 위해 통신 스택의 다른 계층으로부터 정보(예; MAC, IP)를 사용할 수 있으므로 하위 프로토콜에서의 차량 식별자 변경과 익명 인증서 변경이 동시에 이루어져야 한다. 한편 공격자가 메시지에 포함된 위치 정보를 활용하여 차량의 다음 위치를 예측하고 이를 통해 간접적으로 차량을 식별할 가능성이 여전히 존재한다. 이를 고려하여 정해진 영역내에서 차량들의 익명 인증서 변경을 모니터링 할 수 없도록 하는 혼합 존(mix zone)이라는 개념을 도입하였다[11].

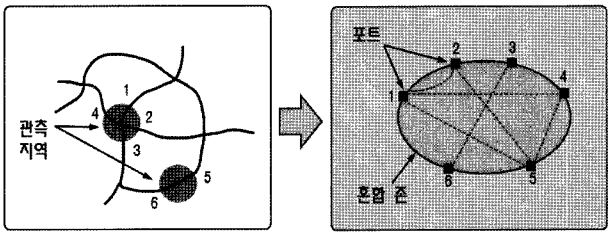

그림 6 혼합 존의 개념

그림 6에서와 같이 공격자가 수신기나 장치를 통해 물리적으로 관측할 수 있는 지역을 관측 지역(observed spot)이라 하고 그 외에 통신 지역을 벗어난 지역을 미관측 지역(unobserved region)이라고 하자. 물리적으로 두 영역은 흩어져 있지만 논리적으로 결합하면 하나의 논리적인 혼합 존을 만들 수 있다. 그림 6의 예에서는 6개의 포트를 하나의 논리적인 혼합 존으로 결합하였다. 만약 한 차량만이 혼합 존에서 자신의 익명 인증서를 변경한다고 가정하면 공격자는 그 영역에서 입차와 출차 되는 차량을 관측함으로써 차량을 추적할 수 있다. 단지 하나의 익명 인증서만이 변경되기 때문이다. 그러나 다수의 차량이 혼합 존에서 그들의 익명 인증서를 변경한다면 공격자는 입차와 출차되는 차량을 매핑하고 차량의 이동을 예측하고 혼합 존을 지나가는 시간을 매핑해야 하므로 차량 추적이 매우 어려워진다. 또한 공격자는 자신의 통신 지역을 벗어난 미관측 지역을 분석하기가 현실적으로 어렵다. 즉, 모니터링되지 않은 미관측 영역에서 차량들이 익명인증서를 변경하게 되면 공격자는 이를 예측할 수가 없다. 공격자가 서로 다른 익명 인증서를 가지고 서명한 메시지를 찾아내 링크하는 것은 시간이 흐를수록 그리고 공간이 커질수록 점점 어려워진다. 차량들이 목적지까지 도착하기 전에 익명 인증서 변경 횟수가 높을수록 공격자는 더욱 많은 불확실성을 예측해야 한다. 다른 의미로 표현하면 혼합 존에서는 이동 노드들이 높은 수준의 위치 프라버시 보호를 받을 수 있다. 혼합 존들은 암호 기법을 사용하여 생성하였을 때 사이즈가 작아지는 경향이 있으며 효율성을 극대화하기 위해서는 최적화된 사이즈가 설계되어야 한다.

6. 구현 구조 및 성능 시뮬레이션

차량통신 보안 기술이 deployment되기 위해서는 구현 구조가 설계되어야 하고 상용화 수준의 HSM과 차량통신 보안 전용 칩이 필요하다. 이 장에서는 구현과 관련된 연구 결과로서 차량통신 보안의 구현 구조, 하드웨어 보안 모듈의 보안 요구사항, 차량내에 필요

한 보안 장치, 소프트웨어 기반의 시뮬레이션을 통한 성능 분석 결과의 일부를 소개한다[4].

6.1 구현 구조

구현 구조는 안전한 통신 프로토콜, 프라이버시 보호, 차량내 보안과 같은 서로 다른 관점이 고려되었다. 현재까지는 설계, 차량통신 프로토콜의 deployment, 시스템 구조, 그리고 보안 메커니즘이 아직 논의 중이고 일부만이 표준화된 상태이기 때문에 고정된 플랫폼을 고려하기가 어렵다. 대안으로서 새롭게 출현할 차량통신 기술이나 새로운 응용들을 수용할 수 있도록 유연성 있는 구현 구조를 고려하였다. 그림 7에 deployment 관점에서 설계한 구현 구조를 나타내었다.

모듈은 각각의 서로 다른 임무를 수행하는 몇 개의 컴퍼넌트로 구성된다. 예를 들어 안전한 통신 모듈은 안전한 통신을 위한 프로토콜을 구현하며 하나의 프로토콜은 다수의 컴퍼넌트로 구성된다. 컴퍼넌트들은 임의의 상위 응용에 의해 호출될 때에만 구동되며 다른 컴퍼넌트와 통신할 수 있는 정의된 인터페이스를 사용한다. 즉, 컴퍼넌트들은 다른 모델에 영향을 주지 않고 새로운 버전으로 변경할 수 있도록 설계하였다. 보안 메니저는 구현 관점에서 제일 중요한 부분이다. 다른 보안 모듈들과 연결되고 설정될 수 있고 구동될 수 있으며 암호 지원 모듈과도 연결된다. 또한 정책을 유지하여 특정 컴퍼넌트를 활성화 및 비활성화 시킬 수 있다.

통신 스택과 독립적으로 분리하기 위해서 보안 메니저와 프로토콜 스택과의 결합은 후킹 개념을 도입하였다. 통신 스택의 사이에는 계층간 프락시(ILP; InterLayer Proxy)가 삽입된다. 모든 ILP는 임의 이벤트를 통지해주는 콜백 핸들러의 리스트를 유지한다. 초기화 시 컴퍼넌트들은 전송할 메시지의 종류와 방향을 지정하여 ILP에 등록한다. 이를 위해 컴퍼넌트들은 이벤트 리스너 인터페이스(Event Listener Interface)를 제공하며 ILP와 연결시키기 위해 레지스터 핸들러 메서드를 사용한다. 특정 컴퍼넌트들은 서로 다른 종류의 패킷을 지정하여 다수의 ILP에 등록할 수도 있다. 하나의 메시지가 ILP에 도착하면 이 메시지 종류가 사전에 등록되어 있는 모든 컴퍼넌트들에게 이벤트 콜백을 트리거하며 이 때 각 컴퍼넌트들의 이벤트 핸들러가 호출된다.

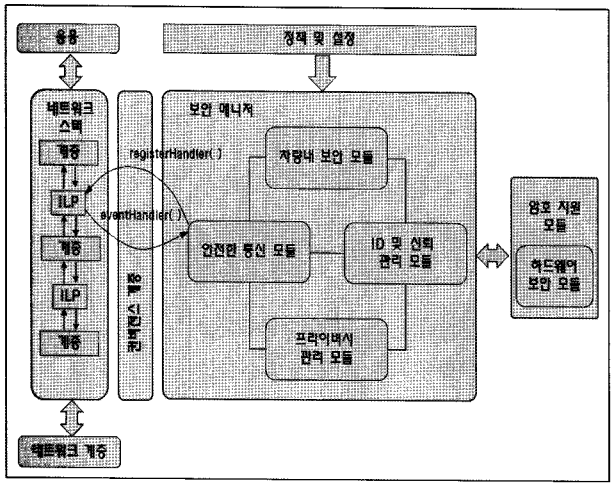

그림 7 Deployment 관점의 구현 구조

콜백은 수신된 메시지에 대한 레퍼런스를 포함하고 있으므로 컴퍼넌트는 이를 검사하거나 수정할 수 있다. 컴퍼넌트는 메시지가 수정되었는지 메시지가 스택에 삽입되어야 하는지 메시지가 ILP에 의해 단순히 드롭되어야 하는지를 리턴값을 이용하여 나타낸다. 예를 들어 안전한 비컨 컴퍼넌트는 MAC 바로 위의 ILP와의 연결되며 모든 입력 비컨 메시지의 서명을 체크한다. 틀린 서명을 갖는 비컨 메시지는 무시되거나 태그된다. 이렇게 후킹 구조를 사용함으로써 최소의 수정만으로도 보안 기능과 기존의 네트워크 스택을 투명하게 결합할 수 있다. 이벤트들은 통신 스택에 의해 트리거되는 반면에 보안 시스템은 잘 정의된 API를 사용하고 명령어 호출방법에 의해 스택을 엑세스할 수 있다. 컨버전스 계층은 다른 통신 플랫폼에 포팅을 가능하게 해준다.

6.2 하드웨어 보안 모듈

하드웨어 보안 모듈은 구현 요구사항과 소프트웨어 구현 예에 대해서만 논의한다. HSM은 물리적인 위조가 방지되어야 한다. 예를 들어 고급 사양의 모듈인 IBM 4758 암호 프로세스를 모든 차량에 장착하기에는 너무 고가이다. 동시에 필요한 일부 기능만을 제공하지만 저가의 물리적인 위조 방지 장치인 스마트 카드를 고려할 수 있다. 그러나 상업용으로 사용가능한 저가 장치들은 자체 배터리를 내장하지 않으므로 신뢰할 수 있는 내부 클럭을 제공하지 않는다. 신뢰할 수 있는 클럭이 없으면 그 장치들은 전체 시스템에서 다른 참여자에 의해 신뢰될 수 있는 타임스탬프를 제공할 수 없다.

따라서 중가의 가격이면서 적정 수준의 하드웨어 위조 방지장치를 갖는 ASIC 형태의 HSM이 필요하다. 장점은 필요한 모든 기능을 설계할 수 있고 대량생산을 통해 가격을 낮출 수 있다. HSM은 OBU상에서 실행되는 모든 모듈들을 서비스 할 수 있는 API를 반

드시 제공해야 한다. API는 디지털 서명, 타임스탬프, 복호화, 키와 디바이스 관리 서비스를 지원해야 한다. 그러나 현재는 적절한 HSM 하드웨어가 없는 상태이므로 여기서는 일반적인 목적의 컴퓨터에서 실행되는 소프트웨어 라이브러리 형태로 API를 구현하였다. 구현 시 디지털 서명을 위해서 ECDSA를 그리고 암호화를 위해 ECIES with HMAC-SHA1과 AES-CBC를 사용하였으며 HSM의 키 관리 서비스를 구현하였다.

6.3 차량내의 보안

차량내 보안 모듈은 차량내 네트워크와 무선통신 시스템간에 인터페이스를 보호한다. 이 모듈은 차량내 네트워크로 외부 접근, OBU, 차량 센서 데이터를 통제하고 그리고 V2V와 V2I 응용들이 정확히 동작하는데 있어서 요구되는 데이터와 서비스를 안전하게 보장해야 한다. 차량내 보안 모듈내에서 제공되는 두 개의 중요한 컴퍼넌트는 방화벽과 침입탐지시스템이다.

- o 방화벽 : 외부 응용으로부터 차량으로 또는 그 반대로 전달되는 데이터 흐름을 제어한다. 방화벽은 패킷 또는 응용 기반의 접근을 하며 규칙 기반의 테이블을 통해 하나의 응용이 어떤 데이터나 어떤 서비스에 접근 가능한지를 나타낸다.
- o 침입탐지시스템 : 지속적으로 차량내 시스템 상태를 모니터링하고 공격을 실시간으로 검출한다. 침입탐지시스템은 특정한 응용 또는 비활성화된 서비스가 접근하는 것을 막기 위하여 동적으로 방화벽 테이블에 규칙을 추가시킬 수 있다.

6.4 성능 시뮬레이션

차량통신에 암호 오퍼레이션을 추가하면 프로세싱 부하 증가와 통신 대역을 비효율적으로 사용하게 된다. 차량들은 자신의 위치나 환경 조건 등의 정보를 보통 100ms당 한 개의 비컨에 실어 전송하며 비컨 사이즈가 커지게 되면 통신방해가 유발된다. 그 지역의 통신 노드의 수, 비컨 전송율, 메시지 오버헤드 등이 많을 경우 복잡한 도로에서는 채널 성능이 현저히 저하된다. 암호 오퍼레이션으로 인한 오버헤드는 주로 패킷 서명과 인증서 첨부로 인해 발생한다. 즉, 100ms마다 비컨이 서명되어야 하고 이를 수신한 차량들은 매번 검증해야 한다. RSA와 DSA 서명 그리고 X.509v3 인증서는 오버헤드가 크므로 EC-DSA 서명과 압축된 인증서를 사용한다. 차량통신 보안에서는 매 비컨마다 인증서 첨부로 인한 오버헤드를 줄이기 위해 모든 비컨에 인증서를 첨부하지 않고 α주기 동안에 하나의 비컨에만 인증서를 첨부하는 기법을 사용한다[12].

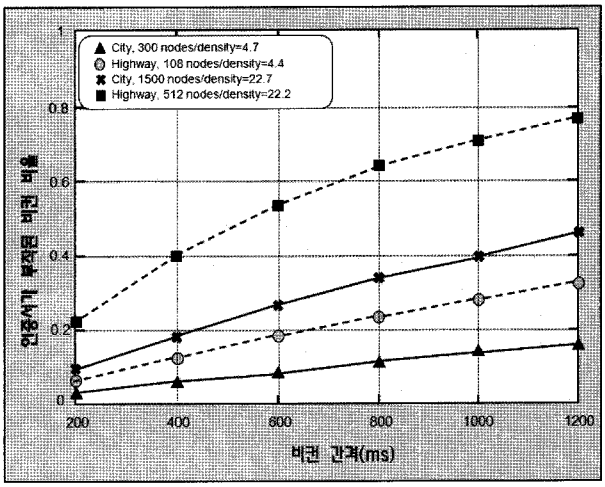

그림 8 인증서 첨부에 따른 비컨의 성능

또한 검증 오버헤드를 줄이기 위해 인증서를 캐싱하는 기법도 제시되었다[13]. 상황을 기반으로 하여 차량의 이웃들이 변하지 않는 경우에는 인증서 첨부와 검증을 적절하게 생략한다.

위에서 언급한 최적화를 기반으로 프로세싱 오버헤드가 제일 높고 비효율적인 통신대역을 사용하는 주기적인 비컨에 대해 성능 시뮬레이션을 실시하였다[4]. 비컨을 전송하는 간격과 인증서를 첨부한 비컨의 비율을 변화시킨 다음 상관관계를 그림 8에 나타내었다. 인증서는 단지 새로운 이웃들이 발견될 때에만 비컨에 첨부된다. 결과에 의하면 짧은 비컨 간격과 중간정도의 노드 밀도를 고려했을 때 전송되는 전체 비컨의 90%이상에서 인증서가 생략될 수 있다. 이와 같은 방법을 통해 차량통신에서 보안 기능을 추가함으로 발생할 수 있는 오버헤드를 줄일 수 있다.

7. 결 론

본 글에서는 대표적인 차량통신 보안 기술로서 유럽의 SeVeCom 프로젝트에서 제시하고 있는 차량통신 보안 기술에 대해 분석하였다. 주요 기술적인 특징으로서 물리적 노출에 안전한 변형 억제성을 갖는 하드웨어 안전 모듈, 안전성과 무결성 그리고 프라이버시 보호를 위한 익명성 인증 기법, 모든 메시지에 전자서명을 통한 안전한 통신, 차량위치 추적을 어렵게 하는 혼합 존 등의 개념을 소개하였다. 그러나 제시한 익명성 인증 기법의 단점은 인증서 변경이 잦을 경우 그에 따른 프로세싱 오버헤드가 커지고 통신대역을 효율적으로 사용할 수 없다는 점이다. 또한 주어진 특정 지역에서 트래픽의 통계적 모델링을 통한 차량 추적 가능성이 여전히 존재한다. 이를 극복하기 위해 최근에는 영역내 차량들에 대해 그룹서명을 고려

하고 있다. 현재 연구되고 있는 분야는 차량통신 전용의 보안 프로세서 개발, 데이터 위주의 신뢰 설정, 네비게이터와 같은 주변장치와의 안전한 결합, 다른 무선 통신기술과 결합 등이다. 한편 국내의 경우 차량통신 기술이 개발되고 있으나 특히 보안과 프라이버시 보호를 위한 연구는 미진한 편이다. 두 이슈는 차량통신 관련 산업 활성화를 위해서 반드시 심도 있게 다루어져야 할 문제라고 판단된다.

참고문헌

[1] H.S. Oh, J.H. Park, "Technology Trends of Vehicle Communication Network," ETTRENDS, pp. 49-55, Oct. 2008. (in korea)

[2] IEEE P1609.2, "Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Application and Management Messages," IEEE Standard, June 2006.

[3] P. Papadimitratos, L. Buttyan, et al., "Secure Vehicular Communication Systems: Design and Architecture," IEEE Wireless Communications Magazine, pp.100-109, Nov. 2008.

[4] F. Kargl, P. Papadimitratos, et al., "Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges," IEEE Wireless Communications Magazine, pp.110-118, Nov. 2008.

[5] Antonio Kung, "Security Architecture and Mechanisms for V2V/V2I(Deliverable 2.1)," SeVeCom Technical report, Aug. 2007.

[6] F. Kargl, Z. Ma, and E. Schoch, "Security Engineering for Vanets," Proc. 4th Workshop Embedded Security in Cars, Berlin, Germany, pp.15-22, Nov. 2006.

[7] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems," ACM VANET, San Francisco, CA, 2008.

[8] Raya et al., "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE JSAC, Special Issue on Vehicular Networks, vol. 25, no. 8, pp. 1557-1568. Oct. 2007.

[9] M. Poturalksi, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," ACM ASIACCS, Tokyo, Japan, pp.189-200, Mar. 2008.

[10] C. Harsch, A. Festag, and Papadimitratos, "Secure Position-based Routing for VANETs," Proc. IEEE VTC07-Fall, pp.26-30, Oct. 2007.

[11] J. Freudiger et al., "Mix-Zones for Location Privacy in Vehicular Networks," Proc. 1st Int'l. Workshop Wireless Networking for Intelligent Transportation Systems(Win-ITS), Vancouver, BC, Canada, Aug. 2007.

[12] G. Calandriello et al., "Efficient and Robust Pseudonymous Authentication in VANET," ACM VANET '07, pp.19-28, 2007.

[13] P. Papadimitratos et al., "Impact of Vehicular Communication Security on Transportation Safety," Proc. IEEE INFOCOM Workshop. Mobile Networking for Vehic. Environments, pp.1-6, Apr. 2008.

김 현 곤

1992 금오공과대학교 전자공학과 학사
1994 금오공과대학교 전자공학과 공학석사
2003 충남대학교 전자공학과 공학박사
1994~2005 한국전자통신연구원 정보보호연구단 팀장
2005~현재 목포대학교 정보보호학과 조교수
관심분야 : RFID/USN 보안, 이동통신 보안, 차량통신 보안
E-mail : hyungon@mokpo.ac.kr