◎ 논 문

http://dx.doi.org/10.22680/kasa2021.13.1.031

한국 V2X 보안인증체계 분석 및 개선방향 연구

엄성욱* · 김동환** · 김성섭*** · 조성우****

A Study on KOREA SCMS Analysis and Improvement Method

Sungwook Eom*, Donghwan Kim**, Sungsub Kim***, Sungwoo Cho****

Key Words: V2X, SCMS(보안인증체계), V2X Certification(V2X 인증서), OBU(차량 단말기), CRL(인증서 폐기 목록)

ABSTRACT

SCMS is a security credential management system for V2X communication, which performs generation/provision/validation of device's security certificates. In this paper, we will explain about the main functions of SCMS and the role of each institution, and propose the following improvement measures in the process of establishing the Korean V2X security certification system. First, connection scheme of ERA (Enrollment certificate RA) between SCMS and Vehicle Manager Information System (VIMS) will be proposed. Second part is the problem of certificate revocation and proposal of improvements.

1. 서 론

4차 산업혁명의 핵심 분야인 자율주행기술은 주변 자동차 및 도로 인프라와의 통신을 통해 다양한 정보를 수집하는 자율협력기술[1~6]로 발전하고 있다. 하지만 자동차의 지능화 및 연결성 확대는 해킹 등의 사이버공격을 통해 국민의 생명과 안전을 위협할 수 있을 것으로 우려된다. 이에 도로의 노변 기지국과 차량에서 생성하는 V2X 메시지의 신뢰성과 사용자의 익명성을 보장하고 자율주행 자동차의 안전한 운행기반을 조성하기 위해 V2X 보안인증체계(SCMS, Security Credentional Management System)[7]가 필요하다.

V2X 통신 보안을 위해 미국, 유럽, 중국 등은 인증서 기반의 V2X 보안인증체계를 채택하고 있다. 이는 공인된 기관에서 인증 및 등록된 기기(차량, 도로 인프라)만 V2X 보안 통신환경에 참여하도록 허용할 수 있게 해주며 해킹 등을 방지하기 위한 V2X 보안 통신 프로토콜을 제공한다.

우리나라도 V2X 보안인증체계 실증사업을 통해 인증서기반의 V2X 보안체계를 개발 중에 있으며 서울,제주, 고속도로 C-ITS 등과 연계하여 실증 중이다.

V2X 보안인증체계에서는 실제 차량의 V2X 인증서를 발급/폐지하는 절차에 관한 내용이 정의되어 있지 않아, 자동차를 V2X 보안인증체계에 등록하고 말소하는 절차를 제안한다. 제안한 절차는 V2X 보안인증체계와 자동차 관리 전산망을 연계하여 인증서 발급 및 폐지 업무를 간소화하고 사용자가 편리하게 이용할 수 있는 절차를 제안하고 있으며 크게 아래 3가지 장점을 제공한다. 첫째, 이용 절차의 간소화 및 접근성 확보를 통해 사용자 편의성 확보한다. 둘째, 기존 자동차 관리체계와 연계하여 차량의 등록인증서정보를 관리를 쉽게 한다. 셋째, 기존 자동차 관리 전산망 시스템을 활용하여 V2X 보안인증체계 구축 비용을 절감한다.

등록인증서는 익명인증서 발급을 요청할 때만 사용하는 것이고, 익명인증서는 차량에 설치되어 있는 단말이 송신하고자 하는 메시지에 서명을 하거나, 서명된 메시지를 검증 하는데 사용되어 진다. 등록인증서의 경우 좀 더 안전하게 만들기 위해 발급과정에 수동 작업들이 포

* 한국교통안전공단 자동차안전연구원, 선임연구원
** 한국교통안전공단 자동차안전연구원, 연구원
*** 한국교통안전공단 자동차안전연구원, 처장
**** 한국교통안전공단 자동차안전연구원, 실장
E-mail: sweom@kotsa.or.kr

자동차안전학회지: 제13권, 제1호, pp. 31~37, 2021
논문접수일: 2020.11.13, 논문수정일: 2020.12.7, 게재확정일: 2021.1.29

함 되어 있다. 등록인증서를 이용하여 익명인증서를 온라인으로 요청하고 다운로드 받을 수 있으며, 발급된 익명인증서는 차량에서 BSM 메시지를 생성할 때 사용된다. 현재 등록인증서는 유효기간은 6년이며, 익명인증서의 유효기간은 1주일이다, 익명인증서의 경우 1주일에 20개씩 무작위로 사용할 수 있으며, 3년치 3120장을 모두 발급한다.

본 논문에서는 SCMS의 주요 기능과 각 기관의 역할을 설명하고, 한국형 V2X 보안인증체계를 수립하는 과정에서 고려되어야 하는 문제점과 및 개선사항들을 제시하였다. 자동자의 출고, 등록, 소유권 이전, 말소등에 따른 등록인증서와 익명인증서의 단계별 처리 환경 및 절차를 검증하여 실증시스템에서 추후 개선해야 할 점을 논의하고자 한다. 첫째, V2X 보안인증체계를 기존 자동차 관리체계와 연계하는 방안. 둘째, 인증서 폐지목록 거대화 문제점 및 해결 방향을 제시하였다.

2. V2X 보안인증체계(SCMS)

2.1. SCMS의 개요

자율협력주행(V2X) 통신환경에서 메시지 해킹, 개인정보 침해 등을 방지하기 위해서는 인증서기반의 V2X 보안 통신환경의 구축이 필요하다. V2X 보안인증체계는 V2X 통신에 활용되는 V2X 인증서의 생성·발급·유효성 검증 등을 수행하는 인증서 관리 시스템과 인증서를 활용한 V2X 보안프로토콜 등을 정의한다. 한국형 V2X 보안인증체계 경우 인증서에 기반한 PKI 시스템[8]으로, 미국 규격[9]을 바탕으로 개발된 KISA 규격[10]을 준수하며 인증서 구조 및 보안프로토콜은 IEEE 1609.2[11]를 준수한다. 국외의 경우, 미국, 유럽, 캐나다, 중국 등도 V2X 공인인증서 기반 V2X 통신환경을 구축 중이다. 미국의 경우 미연방교통부(US DOT)와 CAMP(Crash Avoidance Metrics Partners)가 설계한 SCMS를 채택하여 실증을 진행 중이며 유럽은 유럽연합 집행위원회에서 EURO C-ITS Trust Model을 구축하고 있다.

2.2. SCMS 구성기관의 역할

Fig. 1과 같이, SCMS에는 최상위 인증기관, 기관 인증기관, 등록인증서 발급기관, 익명 인증서 발급기관, 기기 등록소, 인증서 등록기관, 이상행위 관리기관의 기관들이 신뢰 체인 형태로 상호 보증하는 형태이며, 내·외부 공격

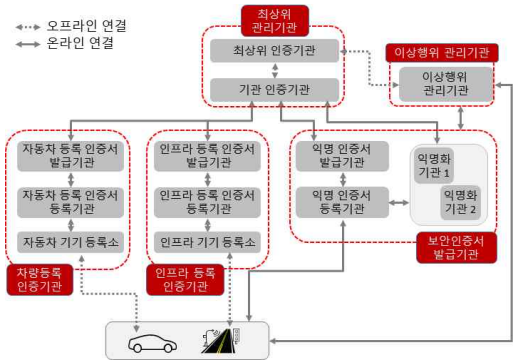

Fig. 1 V2X SCMS structure

방지를 위해 기관 간의 분리가 이루어져 있다.

- 최상위 인증기관(Root): SCMS의 최상위 인증기관이며, 신뢰 기준점(Trust anchor)이다. 하위 기관에 대한 인증서를 발급 및 감사를 담당한다.
- 기관 인증기관(ICA): 최상위 인증기관을 보호하기 위한 보조 인증기관이다. 단말기 인증서 발급 기관(등록인증서, 익명인증서 발급기관)을 인증한다.
- 등록인증서 발급기관(ECA): 단말기(OBU, RSU)에서 인증서를 발급받는데 필요한 자격 증명용 등록 인증서(Enrollment Certificate)를 발급한다.
- 익명 인증서 등록기관(PRA): 단말기로부터 오는 인증서 요청의 유효성을 확인하여 처리한다. 단말기에서 SCMS에 접근할 수 있도록 중계 역할을 하는 기관이다.
- 익명 인증서 발급기관(PCA): PRA의 요청에 따라 보안인증서(OBU의 익명인증서와 식별인증서, RSU의 애플리케이션 인증서)를 발급한다.
- 이상행위 관리기관(MA): 단말기로부터 이상행위 보고를 전송받아 판단 후 이상행위 기기에 대한 인증서 폐지를 수행하고, 폐지된 인증서 목록을 관리한다.
- 기기 등록소(DCM): 차량 및 노변 기지국이 부트스트래핑 과정을 통해 단말기가 SCMS와 상호 작용하여 보안 자격 증명을 얻을 수 있게 해준다.

2.3. SCMS의 주요 기능

2.3.1. V2X 통신채널 보안을 위한 보안규격 제공

Fig. 2와 같이, 차량 및 도로 인프라에 V2X 통신채널 보안을 위한 보안규격을 제공하며 기밀성·무결성·가용성 등 보안의 주요 요소들을 목적에 따라 제공한다.

Fig. 2 Security for V2X communication channel

2.3.2. 내부공격자에의한 개인정보 침해 방지 보장

SCMS의 기관들로부터 차량 위치정보 등의 개인정보 침해 방지를 보장하기 위해 보안(익명)인증서 비밀 값을 관련 기관들이 나눠서 생성하고, 각 기관을 다른 운영 주체가 책임지는 기관 분리 원칙을 제시하고 있다. Fig. 3과 같이, 약속이나 정책이 아닌 기술적 개인정보 보호를 통해 사용자의 거부감을 줄여준다. 단, 악의적 행동을 하는 사용자는 기관들의 협력을 통해 추적할 수 있다.

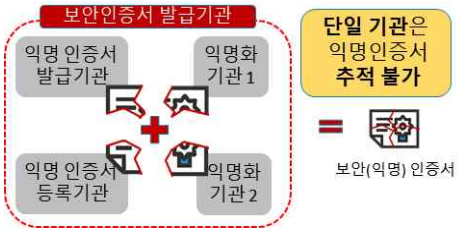

Fig. 3 Privacy protection from inside attacker

2.3.3. 외부공격자에 의한 개인정보 침해 방지 보장

각 자동차는 일주일에 20장의 익명인증서를 돌려가며 사용하도록 설계되어 있다. Fig. 4와 같이, 외부공격자들은 익명인증서로부터 운전자의 정보를 식별할 수 없을 뿐만 아니라, 익명인증서를 돌려가면서 쓰기 때문에 임의의 운전자의 운전경로도 쉽게 식별할 수 없다.

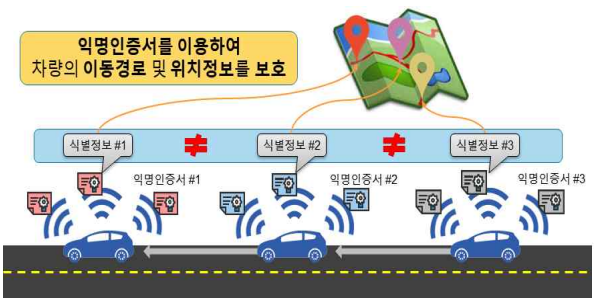

Fig. 4 Use of pseudonym certificate to prevent location tracking

2.3.4. V2X 이상행위 관리

자율협력주행 차는 V2X 통신 메시지를 이용하여 주변 자동차 및 도로 인프라로부터 다양한 정보를 수신하여 제어 등에 활용하기 때문에, 메시지의 신뢰성이 중요하다. SCMS는 고장이나 사이버공격으로 인해 잘못된 정보를 공유하는 차량을 감지하고, 이에 해당 인증서를 폐지하여 신뢰성 있는 V2X 통신환경을 확보한다. Fig. 5와 같이, 통신채널에 대한 보안 뿐만아니라 수신된 메시지가 잘못된 경우를 감지함으로써 신뢰성 있는 V2X 통신환경 구축한다.

Fig. 5 Misbehavior detection

이를 위해 Fig. 6과 같이, 자동차들은 수신된 V2X 메시지들의 이상행위 여부를 탐지하여 이상행위 관리기관에 보고하고, 이상행위 관리기관은 이를 판단하여 최종적으로 인증서를 폐지한다.

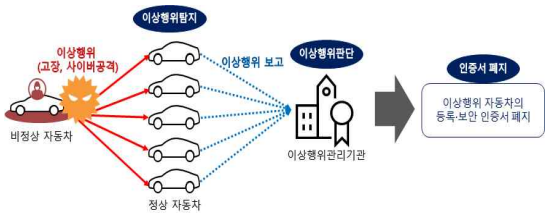

Fig. 6 Misbehavior management system

3. 등록인증서 등록/폐지 절차 제안

3.1. 배경

한국형 V2X 보안인증체계에서는 실제 차량의 V2X 인증서를 등록/폐지하는 절차에 관한 내용이 정의되어 있지 않다. 본 절에서는 자동차를 V2X 보안인증체계에 등록하고 말소하는 절차를 제안한다.

제안한 절차는 V2X 보안인증체계와 자동차 관리 전산망을 연계하여 인증서 발급 및 폐지 업무를 간소화하고 사용자가 편리하게 이용할 수 있는 절차를 제안하고 있으며 크게 아래 3가지 장점을 제공한다. 첫째, 이용 절차의

간소화 및 접근성 확보를 통해 사용자 편의성 확보한다. 둘째, 기존 자동차 관리체계와 연계하여 차량의 등록인증서정보를 관리를 쉽게 한다. 셋째, 기존 자동차 관리 전산망 시스템을 활용하여 V2X 보안인증체계 구축 비용을 절감한다.

3.2. 등록인증서 발급 절차

V2X 보안인증체계와 기존 자동차 관리체계를 연계하는 ERA(등록인증서 등록기관) 개념을 도입. 자동차관리전산망에서 차량 정보(차대번호, V2X 단말 정보 등), 사용자 정보, 등록인증서 정보를 통합 관리한다.

3.2.1. 비포마켓 등록인증서 발급 절차

Fig. 7과 같이, 제작사에서 출고 시 등록인증서 발급 및 관련 정보를 차량 제원정보와 함께 자동차관리전산망 등록한다. 이때 자동차관리전산망에는 차량의 제원정보와 등록인증서 발급정보가 함께 들어가며, 아직 사용자에게 인도되지 않은 상태이기 때문에, 등록인증서를 이용한 익명인증서 발급을 막기 위해 등록인증서를 비활성화시킨다. Fig. 8과 같이 사용자가 차량 등록 시 등록인증서 정보와 사용자 정보를 연계시켜 자동차관리전산망에 저장하며 등록인증서를 이용하여 익명인증서를 발급받을 수 있도록 활성화시킨다.

Fig. 7 Procedure for before-market enroll certificate registration

Fig. 8 Procedure for before-market enroll certificate activation

제안한 방법은 V2X 보안인증체계를 이용하고자 하는 사용자가 기존에 자동차를 구매하고 등록하던 절차에서 추가적인 업무 없이 자연스럽게 보안인증체계를 이용할 수 있게 해준다.

3.2.2. 에프터마켓 등록인증서 발급 절차

Fig. 9와 같이, 에프터마켓 용 V2X 단말기를 구매하여 차량에 장착하기 위한 사용자를 위해서 접근성이 좋고 신뢰성이 확보된 자동차검사소, 차량등록소 등을 기기 등록소로 지정하여 V2X 단말기 정보와 등록인증서 발급정보를 기존에 자동차관리전산망에 연계하여 등록한다.

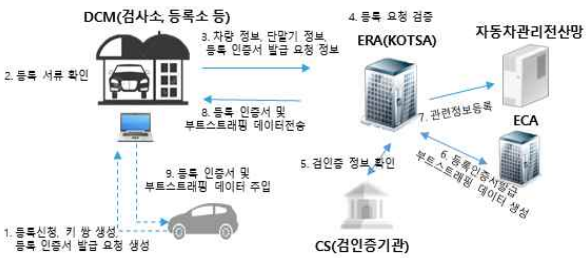

Fig. 9 Procedure for after-market enroll certificate registration

3.3. 자동차 말소에 따른 인증서 폐지 절차

사용자가 자동차 말소 신청을 하면 자동차관리 전산망에 인증서 폐지정보가 저장되고 이상행위관리기관(MA)에게 폐지될 인증서 정보를 전달한다. Fig. 10과 같이, MA는 폐지할 인증서 정보(등록인증서, 보안인증서)를 수집/확인하여 CRL(인증서 폐지정보)로 공유한다.

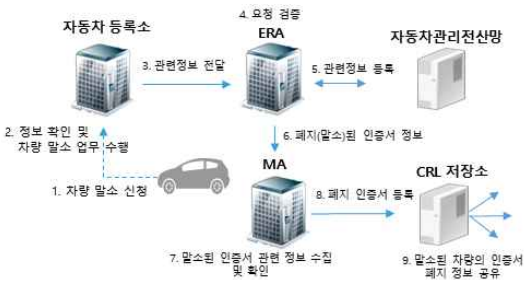

Fig. 10 Procedure for revocation of certificate following vehicle deregistration

4. 인증서 폐지 문제점 및 개선 방향

4.1. 배경

한국 보안인증체계에서 각 자동차들은 개인정보 보호를 위해 일주일 동안 20개의 익명인증서를 돌려가며 V2X 보안통신에 사용한다. 이때 사용되는 익명인증서의 발급 과정은 다음과 같다. 각 자동차가 등록인증서를 이용하여 익명인증서 발급을 신청하고, 익명인증서 발급기관에서를 이를 확인한 후 한번에 3년치 인증서들을 자동차에 발급하도록 설계 되어있다. 한번의 3년치의 인증서를 발급하는 이유는 자동차가 인증서가 없어서 V2X 통신 메시지를 전송하지 못하는 경우를 줄이기 위해서다.[12] V2X 통신을 기반으로 한 다양한 안전 어플리케이션들이 실제로 효과가 있으려면 많은 수의 자동차들이 실제로 V2X 안전 메시지(BSM, Basic Safety Message)를 이용하여 자신의 정보를 알려야 이를 수신하고 정보로 조합하여 자신 주변의 상황을 파악하고 활용할 수 있게 되는 것이다. V2X 통신이 가능한 차량이 익명인증서를 발급받으려면, RSU를 통해 보안인증체계에 신청을 할 수 있다. 아직은 미국 전역이 RSU의 구역에 들어올 수 없는 상황이기 때문에 미리 3년 치 익명인증서를 발급하여, 인증서가 없어서 V2X 안전 메시지를 못 보내는 경우를 최소화하고자 하는 의도가 있다. 하지만 인증서를 한 번에 많이 발급하면 발급 및 배포 관리 측면에서는 장점이 있지만, 인증서 폐지 측면에서는 문제가 발생한다.

4.2. 차량 이전·말소에 따른 인증서 폐지

2019년 국토부 통계에 의하면 1년에 약 500만대가 이전·말소된다. 즉 해당 차들은 등록인증서를 발급받고 운행기록을 남긴 운전자가 다른 사람으로 바뀌거나 폐차되기 때문에 해당 인증서는 폐지되는 것이 보안 측면에서 제일 좋다.

차량이 한꺼번에 3년 치의 인증서를 받기 때문에, 최악의 경우 인증서 폐기목록(CRL)에 해당 인증서가 3년간 포함되어야 한다. 이를 계산을 용이하기 하게위해 한 차의 폐지 인증서 정보가 1년동안 CRL에 포함된다고 가정한다면, 이전·말소에 의한 CRL의 아이템수가 약 500만개로 계산된다.

한국 V2X 보안인증체계 실증시스템의 인증서 폐지리스트는 연결정보와 등록인증서 정보를 포함하여 한 개당 약 47Byte를 차지하고 있으며, 이전·말소에 의한 CRL만 평균 235MB, 최악의 경우 627MB(47Byte/item×5,000,000item/year×3years)될 것으로 예상된다. 이는 차량 이상행위에 의한 폐지목록을 추가를 고려하지 않은 수치이며, 이 경우까지 고려한다면 CRL의 크기는 더 커진다.

IEEE 1609.2[7]에는 각 단말기에 최소한 460KB의 CRL을 저장할 수 있는 공간을 최소 요구조건으로 제시하고 있다. 이는 10,000개의 아이템만 CRL에 저장하는 수치이기 때문에 앞서 도출한 500만개의 아이템을 저장해야 하는 상황을 수용할 수 없게 된다.

또한 2019년 국토부 통계에 의하면 대한민국 운행차는 약 2400만대이며, 차량 들에게 정해진 시간에 인증서 폐지목록을 배포하기 위해 CRL 저장소에서 매주 564TB(627MB×2400만대)를 배포해야 한다. CRL 저장소와 각 OBU 사이의 전송데이터를 줄이기 위해서는 현재 CRL과 직전 주 CRL의 변경 점만 배포하는 Incremental CRL 방식이 고려되야 하지만, 아직 정해진 규격이 없는 실정이다.

따라서 익명인증서를 3년치 발급하는 방식을 한국 실정에 맞게 조정하던지, 이전·말소에 따른 인증서 폐지절차를 수정하는 등의 추가 연구가 필요하다.

4.3. 폐지목록에 따른 OBU의 계산량

OBU가 V2X 메시지를 받았을 때 이 메시지가 CRL에 있는 메시지인지 확인하기 위해서는 HASH 및 PRP 연산이 필요하다. 이를 확인하기 위해 OBU용 보드로 널리 사용되고 있는 Hash(SHA-256) 및 PRP(AES-128) 연산을 벤치마크한 결과를 Latency로 환산할 경우, SHA-256는 3.5054us, AES-128는 3.06507us이 나온다.

위 결과를 바탕으로 CAMP에서 제시하고 있는 Fig. 11 알고리즘에 따라 OBU가 CRL의 한 아이템 당 계산해야 하는 계산양과 시간을 도출하면 다음과 같다.

1) ls_1(i), ls_2(i)로부터 lv(i', 0), ..., lv(i', 20)을 구하는 것과 같다.
2) 1년을 대략 50주로 잡을 경우, ls1(i')와 ls2(1')의 계산을 위해 2×hash×3×50 = 300×hash의 연산이 필요하다.
3) 추가적으로 lv(i', 0), ... lv(i', 20)을 계산하기 위한 연산이 필요하다. 이는 20×2×PRP 연산이 필요하다.
4) 1개 아이템의 사전계산에 소요되는 시간은 300hash+40PRP+20XOR 과 같다. 여기서, XOR은 상대적

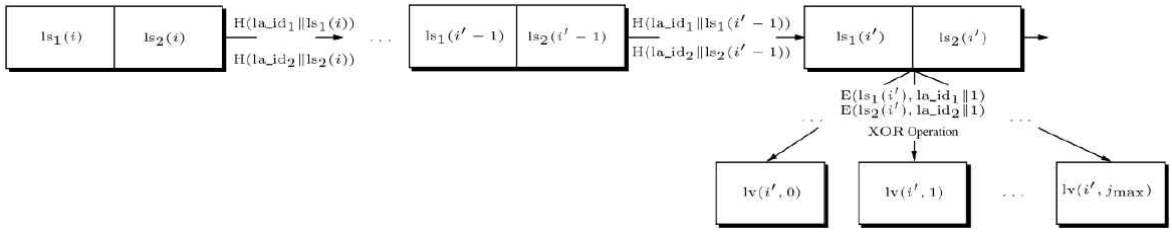

Fig. 11 Procedure for calculating linkage values on all devices

으로 빠르므로 무시할 수 있다. 위에서 적용한 벤치마크 결과를 수식에 적용하면 한 아이템당 1.17ms의 계산이 필요하다. 즉 500만개의 CRL을 처리하기 위해서는 97분30초가 걸린다.

시간을 다투는 V2X 안전 어플리케이션에서 한 메시지를 검증하는데 97분30초의 시간이 걸리는 것은 허용할 수 없는 결과이기 때문에, 각 단말기는 CRL로부터 위 결과를 사전계산해야 하며 사전계산을 한다고 하더라도 CRL 하나를 처리하는데 상당히 많은 시간과 계산량이 걸리기 때문에 실제 운영에 있어 문제가 생길 것으로 판단된다. 따라서 위에 관련된 요구사항도 제도화해야 할 것으로 보인다.

4.4. 해결방안

현 한국 V2X 보안인증 실증시스템은 실증 차량만 처리하기 때문에 문제가 없지만, 협력 주행차가 널리 보급되어 보안인증체계를 이용하는 시점에는 개선이 필요하다. 한 번에 3년 치 인증서를 한꺼번에 발급하는 숫자를 줄이기, CRL 배포 및 다운로드 방식 개선 및 규격화, CRL 검증시간 요구사항 규격화 등이 필요할 것으로 보이며, 근본적으로는 익명 인증서 배포 및 폐지 방식에 대한 SCMS의 고도화가 필요할 것이다.

5. 결 론

본 논문에서는 한국 V2X 보안인증체계의 대해 분석하고, 기존 자동차 관리체계와 연계방안 및 V2X 인증서 폐지 관련 문제점과 개선방향을 제시하였다.

제안된 자동차의 V2X 보안인증체계 등록절차는 자동차관리 전산망을 연계하여 V2X 인증서 발급 및 폐지 업무를 간소화하고 사용자가 편리하게 이용할 수 있는 절차를 제안하고 있으며 크게 3가지 장점을 가진다. 첫째 이용 절차의 간소화 및 접근성 확보를 통해 사용자 편의성 확보하고 둘째, 기존 자동차관리 체계와 연계하여 차량의 등록인증서정보를 관리를 용이하게 하며 셋째, 기존 자동차 관리 전산망 시스템을 활용하여 V2X 보안인증체계 구축비용을 절감할 수 있다.

V2X 보안인증체계 인증서 폐지 절차의 문제점과 개선방향을 제시하였다. 3년 치 익명인증서를 한꺼번에 발행하는 경우, 등록인증서 발급의 절차 및 관리는 쉬워지지만, 인증서 폐지에 문제가 생길 수 있음을 보였다. 국토부 통계에 따르면 차량 이전, 말소에 따른 인증서 폐지가 1년에 500만건에 다를 것으로 예측되며 이에 따른 인증서 폐지목록(CRL)의 거대화가 예상된다. CRL이 거대화되면 크게 3가지 문제점이 생기는데 첫째, 1609.2에서 제시한 CRL 용량 기준을 만족하는 OBU도 CRL 저장공간이 부족해질 정도로 CRL이 거대해진다. 둘째, CRL 저장소가 주기적으로 배포해야 하는 CRL의 데이터양도 지나치게 많아져 문제가 생길 것으로 예상된다. 셋째, CRL의 거대화로인해 각 OBU가 CRL 처리를 위한 계산양이 너무 커진다. 이를 해결하기 위해 한 번에 발급하는 익명 인증서 양을 줄이고, 관련 규격들을 정의할 필요가 있다.

향후 연구로, 현 V2X 보안인증체계를 유지하면서 현재 3년치를 발급하는 익명인증서의 양을 얼마까지 줄이는 것이 효율성과 안정성을 만족할 수 있는지 연구가 필요하다. 나아가 미국 등에서 추진하고 있는 인증서 폐지목록 관리를 위해 사용되는 Certificate Access Manager 등을 고려하여 보안인증체계 시스템 고도화를 위한 다양한 연구가 필요하다.

후 기

본 연구는 국토교통부 도심도로 자율협력주행 안전·인프라 연구 사업의 연구비 지원에 의해 수행되었다(No. 19PQOW-B152473-01).

참고문헌

(1) 권병헌, 이선봉, 2019, “AEB의 V2V 안전성 평가 방법에 관한 연구”, 자동차안전학회지 제11권 제1호, pp. 7~16.

(2) Sangdo Lee, Jun-Ho Huh, 2018, “An effective security measures for nuclear power plant using big data analysis approach”, The Journal of Supercomputing 75, 4267~4294(2019).

(3) Jun-Ho Huh, Yeong-Seok Seo, 2019, “Understanding Edge Computing: Engineering Evolution With Artificial Intelligence”, IEEE Access (Volume: 7), 164229~164245.

(4) 정임영, 2020, “자율주행자동차 위험 및 대응방안에 대한 고찰”. 한국콘텐츠학회논문지, 20(6), 90~98.

(5) 백종현, 김민정, 이진주, 2017, “지능형 교통시스템 보안 아키텍처 및 PKI 인증체계 연구”, 정보과학회지, 35(1), 32~36.

(6) 이유식, 심상규, 김덕수, 2014, “V2X 통신을 위한 보안기술”, 정보보호학회지, 24(2), 28~34.

(7) Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy, 2018, “A Security Credential Management System for V2X Communications”.

(8) Standard Specifications for Public-Key Cryptography, 2000, IEEE Std 1363-2000.

(9) U.S. Department of Transportation (USDOT), 2019, Connected Vehicle Deployment Technical Assistance: Security Credential Management System(SCMS) Technical Primer.

(10) 한국인터넷진흥원(KISA), 2019, V2X 보안인증체계 세부기술규격, c-its.kr/board/getBoardDetail.do?seq=1063.

(11) IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages. IEEE Std 1609.2-2016.

(12) U.S National Highway Traffic Safety Administration (NHTSA), 2016, Preliminary regulatory impact analysis: “FMVSS No.150 Vehicle-To-Vehicle Communication Technology For Light Vehicles”.