디지털산업정보학회 논문지 제14권 제1호-2018년 3월
http://dx.doi.org/10.17662/ksdim.2018.14.1.027

차량인터넷을 포함한 V2X 환경에서 안전한 차량 통신 서비스 제공을 위한 해시 트리 기반 통신 프로토콜*

진 병 욱** · 차 시 호***

Hash Tree based Communication Protocol in V2X Environments Including Internet of Vehicles for Providing Secure Vehicular Communication Services

Jin Byungwook · Cha Siho

〈Abstract〉

Various messages generated in vehicles are transmitted based on the wireless telecommunication which is a core technology of vehicle to everything (V2X). However, the hackers attack them upon penetration to the system and network to cause the generation of users' inconveniences for vehicular communication. Moreover, huge damage could be occurred in terms of physical and materialistic areas if the users in the vehicles were attacked in the communication environment. Therefore, this study was to design the safe communication protocol using hash tree technique in the V2X environments. Using hash tree technique, processes of issuing certificate and registration and communication protocol were designed, and safety analysis was performed on the attacking technique which is occurred in the existing vehicles. Approximately 62% of decrease in the capacity analysis was found upon comparative analysis of telecommunication processes with the system to issue the certificate which is used in the existing vehicles.

Key Words : Hash Tree, Vehicular Communication, Internet of Vehicles, V2X

Ⅰ. 서론

차량 통신환경은 차량과 무선통신망이 결합된 대표적인 통신기술로 텔레매틱스, ITS(Intelligent Transport Systems) 등 다양한 서비스를 제공하며 산업적인 파급효과가 높아지고 있다. 차량 통신은 크게 차량 내 네트워크, 차량 간 통신 네트워크, 차량과 인프라 간 통신 네트워크로 구분되고 있으며 이들을 통합적으로 활용하여 사용자들로부터 편의성 높은 효율적인 서비스를 제공하고 있다[1-2]. 특

* 이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (NRF-2016R1D1A1A09917662).
** 한국지식재산보호원 전임연구원
*** 청운대학교 멀티미디어학과 교수(교신저자)

히 차량 인터넷(IoV, Internet of Vehicles)은 스마트카의 핵심적인 요소로 언제, 어디서든 모바일 인터넷을 통해 다양한 정보를 받을 수 있고 안전한 차량 운행에 필요한 전후방 정보를 지원받을 수 있는 자동차 사물인터넷이다[3].

이러한 차량 통신환경에서 제공되는 운전자의 안전과 관련된 서비스들은 신뢰성을 보장해야 하며, 사용자의 프라이버시를 보호할 수 있어야 한다. 만일 차량 통신환경에서 어떠한 보안위협이 발생한다면 물질적인 피해뿐만 아니라, 그 피해가 운전자의 생명과 직결되기 때문에 안전한 통신 프로토콜은 스마트카 서비스의 핵심 요소이다[4].

그러므로 본 논문에서는 V2X(Vehicle to Everything) 기반 차량 통신환경에서 안전한 메시지를 전송하기 위한 프로토콜을 해시 트리(hash tree) 기반으로 설계한다. 또한, 본 논문에서 설계한 해시 트리 기반 통신 프로토콜의 안전성을 검증하기 위하여 기존의 시스템들에서 발생하는 공격기법에 대해서 안전성을 분석하였으며, 이를 통해 기존에 사용되는 인증체계와의 비교분석을 수행하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 차량 통신 기술 동향, 차량 통신환경에서의 위협 및 보안 요구사항에 대해서 다룬다. 3장에서는 논문의 제안 부분으로 V2X 기반 차량 통신환경에서 해시 트리 기법을 활용한 안전한 통신 메시지 설계한다. 4장에서는 제안한 프로토콜의 성능분석을 위하여 수행한 안전성 분석과 보안성 평가 결과를 보인다. 5장은 본 논문에 대한 결론과 향후 연구에 관하여 기술한다.

II. 관련 연구

3.1 차량 통신 기술 동향

차량 통신의 서비스 형태는 크게 V2V(Vehicle to Vehicle) 경고 전파 서비스, V2V 그룹 통신 서비스, V2V 경계서비스, V2I(Vehicle to Infrastructure) 경고 서비스로 4가지 형태로 구분할 수 있다[5].

V2V 경고 전파 서비스는 안전한 차량 운행을 위하여 특정 차량 또는 차량 그룹으로 차량 주행과 관련한 사고 발생에 대한 경고메시지를 전송하는 서비스이다. 예를 들어 응급 차량이 지나갈 수 있도록 메시지를 전송하여 먼저 긴급차량이 진행할 수 있도록 하는 서비스이다[5-6].

V2V 그룹 통신 서비스는 각 그룹에 포함된 차량 간의 통신을 수행할 수 있는 서비스로 특정 지역을 주행하는 차량으로부터 제공하는 서비스로 특정한 정보를 모든 그룹에 공지하기 위해 주로 사용된다.

V2V 경계서비스는 차량이 주기적으로 속도, 방향, 브레이크 등에 대한 사용 명세를 관리하여 이들에 대한 임계 여부에 대한 정보를 제공함으로써 차량의 안전성을 높이기 위해 사용하는 서비스이다.

V2I 경고 서비스로 차량 간의 주행 시 발생하는 위험에 대해서 차량이 아닌 도로 주변의 다양한 인프라가 경고메시지나 사고 위험 메시지를 발송하는 서비스이다[5-7].

3.2 차량 통신환경에서의 위협 및 보안 요구사항

일반적인 통신환경과 같이 차량 통신환경에서도 다양한 공격이 발생할 수 있다. 차량 통신환경에서 발생할 수 있는 공격으로는 차량 및 RSU(Road Side Unit)에 대한 공격, 메시지 무결성에 대한 공격, 기밀성에 대한 공격, 사용자 정보의 공격, 부인봉쇄에

대한 공격, 가용성에 대한 공격 등이 있다. 이러한 공격 이외에도 차량 통신환경에서는 다음과 같은 보안 요구사항이 필요하다.

- **차량 및 RSU 인증 :** 통신 주체에 대해서 자신의 ID와 그 자신에 대한 정당한 소유자를 밝히며, 개체 인증을 수행하여야 한다. 차량의 소유자가 통신을 수행할 때 현재의 구성원을 밝히며 메시지의 무결성을 입증하도록 해야 한다[4,8].
- **메시지 무결성 :** 차량 간 송수신하는 메시지는 위·변조되지 않아야 한다[4].
- **기밀성 :** 통신 개체 간의 메시지는 인가되지 않은 사용자, 그리고 공격자에 대해서 메시지가 보호되어야 한다[5].
- **사용자 정보에 대한 프라이버시 보호 :** 차량의 소유자는 다른 차량으로부터(운전자 식별번호, 주행번호, 차대번호 등) 식별 값이 보호되어야 한다. 만약 보호 방안이 제공되지 않으면 쉽게 위치추적이 될 수 있으며, 메시지의 신뢰성을 잃어버릴 수 있다. 그러므로 차량이 발생한 메시지 사용자에 대한 정보는 보호되어야 하며, 해킹 및 유출에 대한 보안성 강화가 요구된다[6].

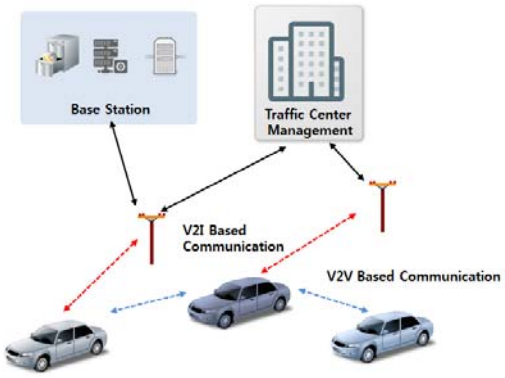
Ⅲ. 해시 트리 기법을 활용한 안전한 통신 메시지 설계

3.1 제안한 차량 통신 프로토콜의 전체 구성도

본 절에서는 V2X 기반 차량 통신환경에서 해시 트리 기법을 활용한 안전한 통신 메시지 프로토콜을 제안한다. 본 논문에서 제안한 차량 통신 프로토콜의 전체 구성도는 <그림 1>과 같이 차량, RSU, Base Station, Traffic Management Center로 구성되며 V2I와 V2V 통신을 기반으로 데이터를 송수신한다. 이들의 통신 절차는 다음과 같다.

1. 차량은 Base Station으로 Vehicle Number, OBU Serial Number, TIMESTAMP 을 Service Provider의 공개키로 암호화하여 등록 요청 메시지를 전송한다.

$$E_{Pub-SP}(OBU \| Time\ Stamp \| VN) \quad (1)$$



<그림 1> 제안한 차량 통신 프로토콜의 전체 구성도

2. Bases Station은 차량으로부터 수신받은 메시지를 Service Provider로 전송하여 식별요청 메시지를 전송한다.

$$E_{Pub-SP}(OBU \| Time\ Stamp \| VN) \quad (2)$$

3. 식별요청 메시지를 받은 Service Provider는 복호화 후 OBU Serial Number를 검증한다.

$$D_{Pub-SP}(OBU \| Time\ Stamp \| VN) \quad (3)$$
$$Verification\ OBU_{SN}$$

4. Service Provider는 차량으로부터 Base Station을 거쳐 식별 값을 요청한다.

5. 차량에서 사용자는 License Number와 Password를 입력 후 해시 함수를 사용하여 Service Provider의 공개키로 암호화를 수행하고 식별 값 응답 메시지를 전송한다.

$$E_{Pub-SP}(Hash(User_{LicenseNumber}||Hash(User_{Pwd}) \quad (4)$$

6. Base Station은 차량으로부터 수신한 식별 값을 Service Provider로 전송한다. Service Provider에서는 메시지를 수신한 후 복호화를 수행한다.

$$D_{Pub-SP}(Hash(User_{LicenseNumber}||Hash(User_{Pwd}) \quad (5)$$

7. Service Provider는 Traffic Management Center로 인증서 발급 요청 메시지를 전송한다. 수신한 License Number를 해시 함수를 수행하고, Service Provider의 인증값을 첨부하여 요청한다.

$$E_{Pub-tms}(SP_{CertValue}||Hash(User_{LicenseNumber}) \quad (6)$$

8. Traffic Management Center는 수신된 메시지를 복호화하며 해시 트리 기법을 활용하여 인증서를 생성한다. 생성된 인증서는 Service Provider로 전송한다.

$$D_{Pub-tms}(SP_{CertValue}||Hash(User_{LicenseNumber}) \quad (7)$$
$$E_{Pub-SP}(User(Certificate\,Issuance)) \quad (8)$$

9-10. Service Provider는 수신된 메시지를 복호화한 후 이를 등록한다. 인증서와 해시 함수를 수행한 후 Password를 XOR를 수행한 값을 차량으로 전송하여 등록 완료 메시지를 송신한다.

3.2 차량 등록 및 인증서 발급 절차

차량 등록 절차는 Base Station을 거쳐 Service Provider에서 등록 요청 메시지를 검증한다. 이후 Service Provider에서 수신된 메시지를 확인하여 등록 메시지를 요청한 차량으로부터 식별 값을 요청한다. 차량은 식별 값과 password를 입력하여 Service Provider로 전송한다. Traffic Management Center는 식별 값을 검증한 후 해시 트리 기반으로 인증서를 생성한다. 해시 트리 인증서는 차량, RSU의 식별 값을 관리할 때도 사용한다. 생성한 메시지를 Service Provider로 전송한 후 등록과정을 수행한다. 마지막으로 등록과정을 마친 후 차량으로부터 인증서를 발송하는 절차를 수행한다. 이러한 차량 등록 및 인증서 발급 절차는 <그림 2>와 같다.

3.3 V2X 기반 메시지 통신 프로토콜 설계

본 절에서는 V2X 기반 차량 통신환경에서 메시지 통신 프로토콜을 설계한다. 차량은 상황 알림 메시지를 RSU로 전송한다. RSU에서는 발급된 인증서와 차량 메시지의 검증요청 메시지를 Service Provider로 전송한다. Traffic Management Center에서는 차량의 메시지를 검증한 후 차량과 RSU로 메시지를 전송한다. 이들의 통신 절차는 다음과 같다.

1. 차량은 상황 알림 메시지를 Service Provider의 공개키로 암호화를 수행하여 인증서와 같이 전송한다.

$$E_{Pub-Sp}(Message_{Type-i}), \quad E_{Pub-Sp}(Certificate\,Issuance) \quad (1)$$

2. 상황 알림 메시지를 수신받은 RSU는 상황 알림 메시지를 Service Provider로 전달한다.

$E_{Pub-Sp}(Message_{Type-i})$,
$E_{Pub-Sp}(Certificate\ Issuance)$ (2)

3. Service Provider는 수신받은 메시지를 복호화한 후 인증서를 해시 트리 기반의 암호화를 수행하여 검증한다.

$D_{Pub-Sp}(Message_{Type-i})$,
$D_{Pub-Sp}(Certificate\ Issuance)$ (3)

4. Service Provider에서는 인증서 확인 요청 메시지를 Traffic Management Center로 전송한다.

$E_{Pri-sp}((Certificate\ Issuance) \oplus Hash(TimeStamp))$, (4)
$E_{Pub-TMS}(TimeStamp)$

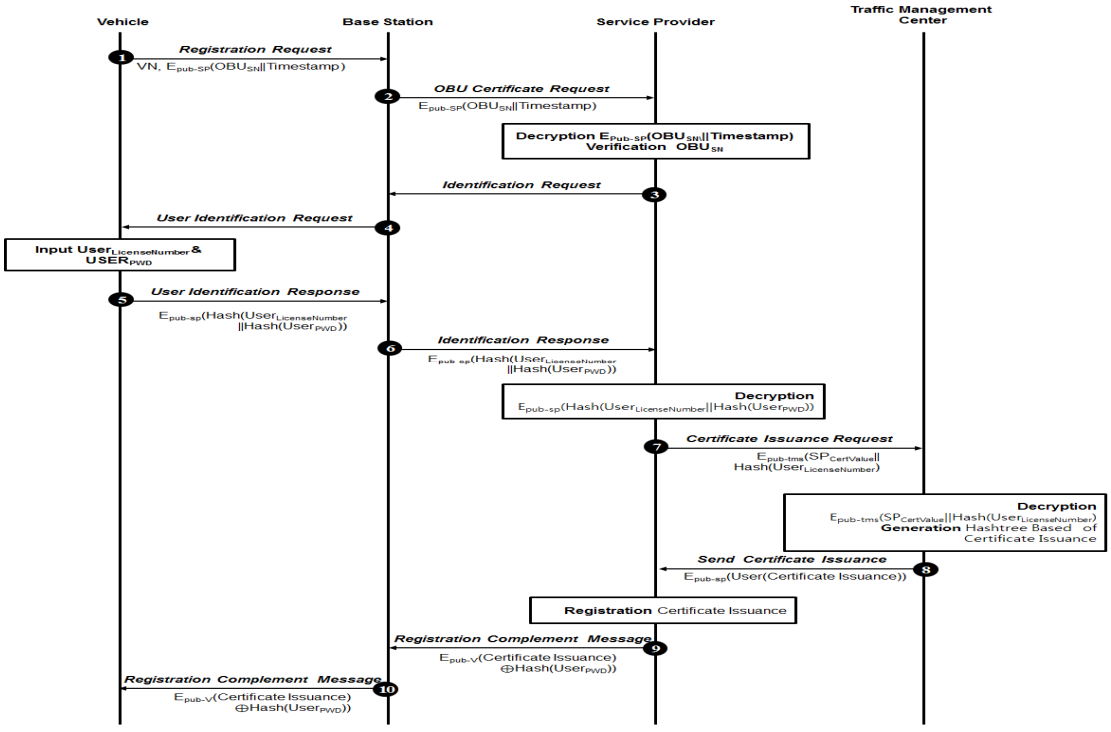
5. Traffic Management Center에서는 수신된 메시지를 복호화한 후 인증서를 XOR 수행하여 Message를 검증한다.

$D_{Pri-sp}((Certificate\ Issuance) \oplus Hash(TimeStamp))$,
$D_{Pub-TMS}(TimeStamp)$

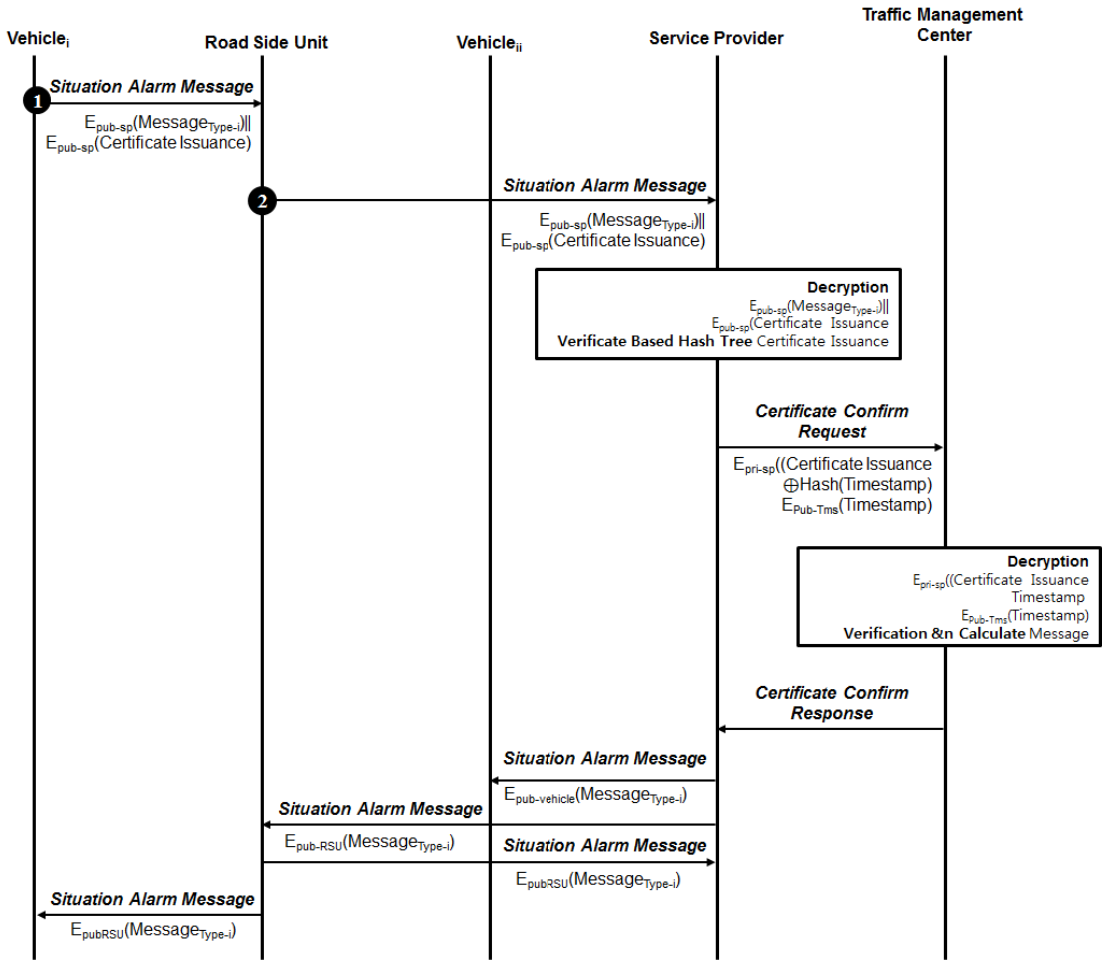
(5)

6. 인증서의 메시지를 검증한 후 Service Provider로 인증서 확인 응답 메시지를 전송한다.

7. Service Provider에서는 수신된 확인 응답 메시지를 검증한 후 RSU와 차량으로부터 수신자의 공개키로 암호화하여 메시지를 전송한다.



<그림 2> 차량 등록 및 인증 절차



<그림 3> 안전한 메시지를 전송하기 위한 차량 통신 프로토콜 설계

Ⅳ. 성능평가

4.1 안전성 분석

본 절에서는 논문에서 설계한 해시 트리 기법을 활용한 안전한 통신 메시지 프로토콜에 대한 안전성 분석을 위장 공격, 중간자 공격, 메시지 무결성의 위협, 사용자 정보 해킹 및 유출의 측면에서 분석한다.

위장 공격 : 차량을 탈취하여 인가되지 않은 사용자가 차량 통신을 수행하여 데이터를 탈취하는 행위이다. 그러나 차량 등록 및 인증과정에서 차대번호, 사용자의 License를 전송하여 인증함으로써 위장 공격을 수행할 수 없다.

중간자 공격 : 차량 통신환경에서 발생하는 중간자 공격은 차량으로 메시지 전송 과정에서 악의적인 사용자가 메시지를 탈취하여 메시지를 변조하는 공격이다. 본 논문에서는 해시 트리 기반으로 생성된 인증서를 활용하여 메시지를 검증함으로써 중간자 공

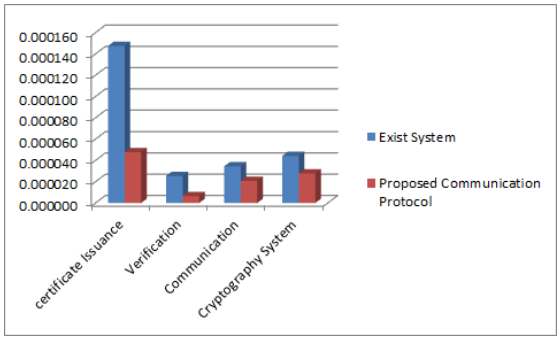
격에 대해서 안전하다.

메시지 무결성의 위협 : 차량 통신과정에서 메시지의 무결성을 위협하는 상황이 발생할 수 있다. 본 논문에서는 메시지의 무결성 위협을 보완하기 위해 인증과정에서 Traffic Management Center에서 Service Provider의 메시지도 같이 검증함으로써 메시지의 보안성을 강화한다.

사용자 정보 해킹 및 유출 : 공격자가 사용자의 정보를 위협하는 해킹 사건이 꾸준히 증가하고 있다. 또한, 원치 않는 과정에서 메시지의 유출사례가 빈번히 발생한다. 이를 보완하기 위해서 차량의 등록과정에서 생성된 인증서와 TIMESTAMP 을 활용하여 메시지를 전송하며, 이를 검증함으로써 사용자의 정보 관리적인 측면을 보완할 수 있다.

4.2 효율성 분석

본 논문에서 제안한 통신 프로토콜의 효율성을 분석하기 위한 시스템 환경은 Inter(R) Core(TM) i5-4590 CPU @ 3.30Ghz 3.30Ghz, 4.00Gb이며 JCA 기반의 암호화와 복호화의 수행 성능을 분석하였다. 기존의 PKI 기반의 인증서 발급, 검증방식, 통신 프로토콜의 수행방식과 제안한 시스템의 수행속도는 <그림 4>와 같다.



<그림 4> 기존시스템과 제안한 시스템의 비교분석

또한, 차량 통신환경을 비교분석 수행하기 위해서 TTAK KO-06.017 TTA 표준문서를 기반으로 기존에 사용되는 통신시스템과 제안한 통신 프로토콜의 비교분석을 수행하였다. 기존의 통신시스템은 PKI 기반의 인증서 발급 검증방식을 수행한 차량 통신 프로토콜을 사용하였고, 제안한 통신 프로토콜의 방식은 MD5 해시 트리 암호화를 사용하였다. 시뮬레이션 수행 결과 본 논문에서 제안한 통신 프로토콜이 차량 통신환경에서 기존 통신 기법 대비 인증서 수행방식은 약 32% 감소하였으며, 검증방식은 약 25% 감소하였다. 또한, 통신 방식에서는 약 60% 감소하여 높은 효율성을 보였으며, 암호화 방식에서도 약 62% 감소하여 경량화성 속도향상을 확인할 수 있었다.

Ⅴ. 결론

본 논문에서 V2X 기반 차량 통신환경에서 해시 트리 기법을 활용한 안전한 통신 프로토콜을 설계하였다. 제안한 통신 프로토콜은 V2X 기반에서 안전한 메시지를 전송하고 효율성에서 기존의 시스템보다 경량화하도록 연구하였다. 기존의 암호 시스템에서 발생하는 위장 공격, 중간자 공격, 메시지 무결성의 위협, 사용자 정보 해킹 및 유출에 관하여 분석하였으며, 기존의 통신시스템과의 보안성을 평가하여 통신 수행 측면에서 약 62%의 높은 효율성을 확인할 수 있었다.

현재 자율주행 차량 통신에 관한 기술적인 연구는 활발히 진행되고 있으나, 차량 통신의 보안성에 관한 연구는 미비하다. 신규 및 변종공격에 대한 대응책이 필요하며, 통신환경에서 사용자들로부터 안전한 통신을 수행할 수 있는 보안정책이 요구된다.

참고문헌

[1] TTAK.KO-12.0208, Security Requirements for Vehicle-to-Vehicle Communication, TTA, 2012. 12. 21.

[2] 이상우 외, "차량 통신 보안 기술 동향," 주간기술동향, 2012. 07.

[3] Say to U, HTC – 폭스바겐과 협력하에 Internet of Vehicles 개발 중, 2015. 12. 15., http://say2you.tistory.com/6245.

[4] TTAK.KO-06.0174, Requirements for Wide-Area Wireless Communication for ITS/Teleics, TTA, 2008. 6. 26

[5] TTAK.K0-12.121241, Security Requirements for Vehicle-to-Vehicle Communication, TTA, 2012. 8. 12.

[6] IEEE 1609.2-2013, "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," April 2013.

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

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

■ 저자소개 ■

진 병 욱
(Jin Byungwook)

2017년 8월~현재
한국지식재산보호원 전임연구원
2017년 8월 숭실대학교 컴퓨터학과(공학박사)
2011년 2월 숭실대학교 컴퓨터학과(공학석사)
2010년 2월 청운대학교 멀티미디어학과(문학사)

관심분야 : IoT, 인증 시스템, 접근제어
E-mail : wlsquddnr@koipa.re.kr

차 시 호
(Cha Siho)

2009년 3월~현재
청운대학교 멀티미디어학과 교수
1997년 7월~2000년 2월
대우통신 종합연구소 선임연구원
2004년 2월 광운대학교 컴퓨터과학과(공학박사)

관심분야 : 네트워크 관리, 차량 통신 네트워크, Semantic Web, Web of Things
E-mail : shcha@chungwoon.ac.kr

논문접수일 : 2018년 01월 19일
수 정 일:
게재확정일 : 2018년 02월 13일