JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 9 : 2114~2120 Sep. 2015

차량 클라우드 환경에서 안전한 통신을 위한 프레임워크 설계

박중오[1] · 최도현[2*]

A Design of Framework for Secure Communication in Vehicular Cloud Environment

Jung-oh Park[1] · Do-hyeon Choi[2*]

[1]Information & Communication Engineering, Dongyang Mirae University, Seoul 152-714, Korea
[2*]Computer Science, Soongsil University, Seoul 156-030, Korea

요 약

차량 클라우드 기술은 차량 통신 환경기술과 유무선 인터넷에서 활용되고 있는 클라우드 컴퓨팅을 융합한 기술로서 새로운 IT 패러다임으로 부각 받고 있다. 차량 환경에서 효율적인 통신을 사용자로부터 컴퓨터, 센서, 통신, Device, 리소스 등을 제공하여 도로 교통 환경에서 크게 기여할 수 있을 것으로 예상하고 있다. 하지만 차량 클라우드 환경을 적용하기 위해서는 보안문제가 해결되어야 하며, 차량환경의 보안위협과 유・무선환경에서 발생하는 공격기법에 대하여 안전하게 해결되어야 한다. 그러므로 본 논문에서는 차량 클라우드 환경에서 차량과 차량, 차량과 노변과의 안전한 통신을 수행하도록 보안 프레임 워크를 설계하였다. 차량환경의 안전성과 보안성은 차량기반 및 클라우드 환경의 보안요구사항을 만족하였으며, 기존의 차량네트워크의 통신 프로토콜보다 효율성을 높였다.

ABSTRACT

Vehicle cloud technology is a fusion technology of vehicle communication technology and cloud computing used in wired and wireless Internet, and has attracted attention as a new IT paradigm. It is expected that it would contribute to resolve the road traffic problem with effective communication by providing computer, sensor, communication, device, and resource. but security is necessary to apply vehicle cloud environment and it have to resolve security threats and various attacks occurred in wired and wireless vehicle environment. Therefore, in this paper, we designed security framework to provide secure communication between vehicle and vehicle, and vehicle and the Road side in the vehicle cloud environment. Safety and security of the vehicle environment was satisfied with the security requirements of the vehicle and cloud-based environment, and increased efficiency than the conventional vehicle network communication protocols.

키워드 : 차량 네트워크. 차량기반 클라우드, 보안 프레임 워크, 프라이버시 보호

Key word : VANET, Vehicle based Cloud, Secure Framework, Privacy Protect

Received 27 July 2015, **Revised** 05 August 2015, **Accepted** 17 August 2015

*** Corresponding Author** Do-hyeon Choi(E-mail:cdhgod0@ssu.ac.kr, Tel:+82-2-2610-5169)
Computer Science, Soongsil University, Seoul 156-030, Korea

Open Access **http://dx.doi.org/10.6109/jkiice.2015.19.9.2114** print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

클라우드 컴퓨팅 보급으로 인하여 자동차 클라우드 기능을 탑재하여 원격시동, 음성인식, 도어락 등 다양한 기술을 사용자로부터 제공하고 있다. 이를 차량 클라우드(Vehicular Cloud Networking)라 정의하고 있으며 클라우드 컴퓨팅을 차량환경에 제공한 기술이라 하고 있다. 차량네트워크 기반으로 발전하고 있으며 운전자와 승객으로 하여금 안전한 서비스와 편의성을 제공하고 있다[1].

이러한 서비스와 편의성을 제공하기 위해서는 기존의 차량네트워크기반에서 발생하던 보안 위협과 클라우드 컴퓨팅 환경과 접목되어 인터넷기반의 다양한 공격기법이 존재할 수 있다. 그리고 차량통신환경이 위협을 받는다면 사고로 인해서 인명피해가 발생할 수 있으므로 이에 대한 보안 기술이 요구된다[1, 5].

본 논문에서는 차량 클라우드 환경에서 안전한 통신을 위한 보안 프레임워크를 설계하며, 기존의 차량 통신에서 메시지 통신의 효율성을 높인다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구 항목을 다루며 차량 클라우드 구조 및 유형, 차량 환경의 보안요구사항, 차량 통신간의 메시지 규격을 기술한다. 3장에서는 제안된 통신 프레임을 설계하며 차량 인증 및 등록, V2I(Vehicle-to-Infrastructure) 통신 프로토콜, V2V(Vehicle-to-Vehicle)통신 프로토콜을 설계한다. 4장에서는 안전성 분석 및 보안성을 평가하며, 5장에서는 결론을 제시한다.

Ⅱ. 관련연구

2.1. 차량 클라우드 구조 및 유형

차량 클라우드의 구조는 차량 클라우드, 노변 클라우드, 중앙 클라우드로 구성되어 있다. 차량 클라우드의 환경을 살펴보면 차량과 차량과의 통신환경 즉 V2V (Vehicle-to-Vehicle)간의 메시지를 통신한다. 클라우드 서버로 접속된 차량은 서비스를 제공받을 수 있으며, 개인차량과 비교해서 많은 자원을 보유하고 있다. 노변 클라우드 환경은 V2I기반의 환경이며 차량과 RSU (Road Side Unit)과 통신한다. RoadSide와 Local Server로 구성되어 있다. 하지만 노변 클라우드는 무선 인터넷 영역 내에 무선 인터페이스를 제공하므로 통신범위가 한정적이다. 차량 및 Road Side Unit이 무선 네트워크를 용하여 중심부로 접속되는데 이를 중앙 클라우드라 정의한다. 중앙 클라우드는 차량 클라우드와 노변 클라우드 보다 많은 리소스를 보유하고 있으며, 데이터 처리 및 연산을 위해 사용된다[2].

그리고 차량 클라우드의 유형은 위에서 언급된 구성형태로 살펴보면 VANET Based Cloud와 Vehicle-to-Cloud로 구성되어 있다. 차량 클라우드 컴퓨팅 환경의 구성 및 유형은 [그림 1]과 같다[1, 7, 8].

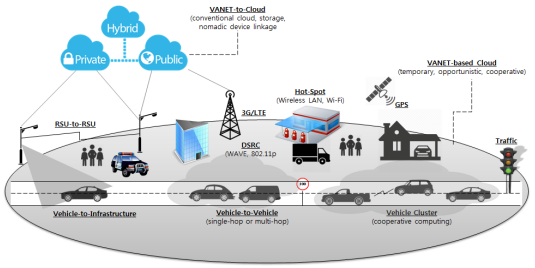

그림 1. 차량 클라우드 컴퓨팅 환경의 구성 및 유형
Fig. 1 Vehicular Cloud Computing Environment of Configuration And Type

VANET-based Cloud는 차량이 보유한 컴퓨터, 센서, Communication, Device 등을 통합 후 플랫폼을 구현하여 인가된 사용들로부터 서비스를 제공하는 모델이다. 도로 및 일상생활 환경에서 발생할 수 있는 위험요소를 감지하여 이를 사전이 예방하고 사후 해결할 수 있으며, 차량 클라우드 서버에서 데이터를 실시간으로 주고받으며 지연시간을 줄일 수 있는 특징이 있다.

Vehicle-to-Cloud의 유형은 클라우드 컴퓨팅 환경과 연계하여 Vanet-Based Cloud에서 수집된 데이터를 바탕으로 중앙 클라우드로 전송 후 상황에 알맞은 결과를 유출한다. 모바일 클라우드의 확대된 개념이라 할 수 있으며 기관 및 업체에서는 Car Cloud라 정의하고 있다. 멀티미디어 콘텐츠 저장 및 차량 관리에 필요한 정보, 내비게이션, Device을 통해 다양한 서비스를 제공하고 있다[3, 6, 7].

2.2. 차량환경의 보안 요구 사항

차량 통신 환경에서는 V2I, V2V로 나누어 질 수 있으며 대표적으로 변조, 위장, Sybil, 서비스 인프라, 도

청, 개인정보 수집, 가명등과 같은 위협요소들이 존재한다. 이를 보완하기 위해서 차량환경에서는 차량 및 RSU(Road Side Unit) 인증, 메시지 무결성, 기밀성, 프라이버시 보호, 부인 봉쇄, 가용성이 있으며 보안 요구사항은 [표 1]와 같다[3].

표 1. 차량 환경 보안 요구 사항
Table. 1 Vehicular Environment of Security Requirement

Division	Described
Vehicle and RSU certification	Vehicle of the vehicle environment, must be unique, which also elements that reveal the identity and Shi must say their identity. In the inter-group vehicle communication environment, it is necessary to prove the members of his current group.
Message Integrity	Message sent to each other should not be above modulation.
Confidentiality	Messages that are sent and received in the vehicle-to-vehicle communication environment must safety there by an attacker.
Privacy Protection	The owner of the vehicle, information from other vehicles must be safe, you need to prepare protection measures from the travel and safety information
Repudiation	Vehicle that sent the message should not be able to deny the corresponding message.
Availability	Each node and cars should always send a message, it should be routed in a quick time.

2.3. 차량 통신간의 메시지 암호화 규격

차량 통신 환경에서 송수신되는 메시지의 암호화를 규격의 대표적인 형태는 'SAE J2735'에 정의된 BSM (Basic Safety Message)이다. BSM은 차량으로부터 번번이 수신되는 브로드 캐스팅 메시지를 의미하며 안전성을 높이기 위해 설계되었다. 100msec 주기로 차량들로부터 메시지를 송신하고 수신된 차량은 안전성에 대하여 판별을 한다[2-4].

BSM은 전송되는 정보와 부가적인 정보로 구분되며 이를 Part 1, Part2라 정의된다. 정보의 내용은 차량의 위치, 이동방향, 현재 시간, 차량의 상태정보를 포함하고 있다.

차량의 메시지 ID는 msgID, msgCnt, id, secMark 를 지정되어 있으며 8바이트가 할당되어 있다. 차량의 위치 값은 lat, long, elev, accuriacy을 지정되어 있고 14 바이트가 할당되어 있다. 필드 값의 상세 값은 'SAE J235'를 참조한다.

Ⅲ. 차량 클라우드 환경의 통신 프레임 워크 설계

3.1. 제안 프레임 워크 구성도

기존의 VANET환경과 클라우드 환경을 융합하여 통신 프레임워크를 설계하였다. 차량 클라우드 환경의 통신 프레임워크는 [그림 2]와 같다. 차량의 등록 및 인증 과정을 거쳐서 차량 클라우드 환경에서 Vehicle to Interface과 Vehicle to Vehicle의 통신 프로토콜을 설계하였다. 또한 본 논문에서는 관련연구 2절의 차량 환경 보안 요구사항을 기반으로 프레임 워크를 설계하였다.

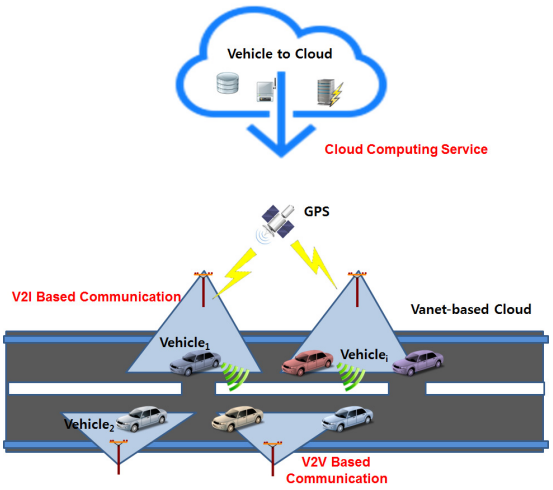

그림 2. 차량 클라우드 환경 통신 프레임워크
Fig. 2 Vehicle Within Cloud Environment Communication of Framework

제안된 프로토콜은 차량환경의 보안요구사항을 참고하여 설계하였으며, 통신 프로토콜에서는 세션 키를 생성 후 암호화하여 통신한다. 제안 프로토콜의 약어는 [표 2]와 같다.

표 2. 제안 프로토콜 약어
Table. 2 Proposed Protocol of Abbreviation

	Description
VehicleVIN	Vehicle Identification Number and Vehicle Number of Xor Operation Value (Operation to fit a front seat)
VehicleNonce	Vehicle of Generation Nonce
VehicleSig	Vehicle of Signature Value
BSCert	Base Station of Authentication of Value
Ex(M)	x of Public Key M Encryption
EX-Y(M)	X and Y of Value using bilinear pairing Encryption
Session	Session Key
GP	GPS ofGP (Talker ID)
GGA	GP of GGA (Sentence ID)

3.2. 차량 등록 및 인증

V2I, V2V 메시지 통신을 수행을 하기 전에 소유주의 차량을 클라우드 서버에 등록 및 인증하는 과정을 수행한다. 차량과 Base Station은 클라우드 서버로부터 인증을 받고, 차량을 등록한다.

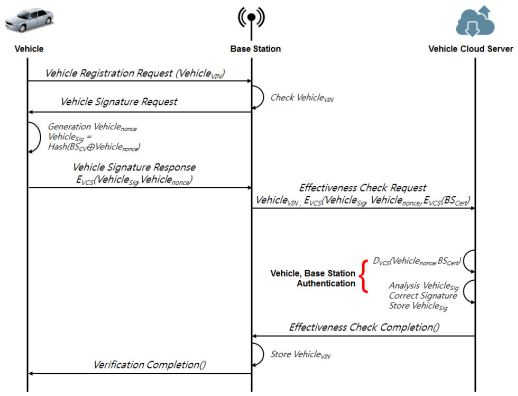

그림 3. 차량 인증 프로토콜
Fig. 3 Vehicle Authentication Protocol

1. 차량은 Base Station으로부터 $Vehicle_{VIN}$을 포함하여 등록 요청 메시지를 전송한다.
2. Base Station은 $Vehicle_{VIN}$을 검사 후 차량으로부터 서명 요청 메시지를 전송한다.
3. 차량은 $Vehicle_{Nonce}$을 생성 후 BC_{CV}와 Xor 및 해쉬 연산을 수행하여 서명 값을 생성 후 Base Station으로 전송한다.

$$Vehicle_{sig} = Hash(BS_{CV} \oplus Vehicle_{Nonce})$$
$$E_{VCS}(Vehicle_{Sig}, Vehicle_{Nonce}) \quad (1)$$

4. Base Station은 Vehicle Cloud Server로부터 Base Station의 인증 값과 $Vehicle_{VIN}$을 첨부하여 유효성 검사 요청 메시지를 전송한다.

$$Vehicle_{VIN}, E_{VCS}(Vehicle_{Sig}, Vehicle_{Nonce}, BS_{Cert}) \quad (2)$$

5. Vehicle Cloud Server는 수신된 메시지를 복호화 하고 인증을 수행하고 서명 값을 검증 후 맞으면 $Vehicle_{Sig}$을 저장 후 유효성 검사 완료 메시지를 Base Station으로 전송한다.

$$D_{VCS}(Vehicle_{Nonce}, BS_{Cert}) \quad (3)$$

6. Base Station은 메시지를 수신하고 $Vehicle_{VIN}$을 저장한다. 이후 검증 완료 메시지를 차량으로 전송한다.

3.3 Vehicle to Interface 환경의 통신 프로토콜 설계

본 절에서는 V2I기반의 메시지 전송 절차에 대하여 설명한다. 차량은 RSU로 상황메시지를 전송한다. 이후 Base Station을 통하여 메시지 검증을 완료 후 RSU로 상황 메시지를 전송한다. RSU 지역 내 차량으로 메시지를 전송한다.

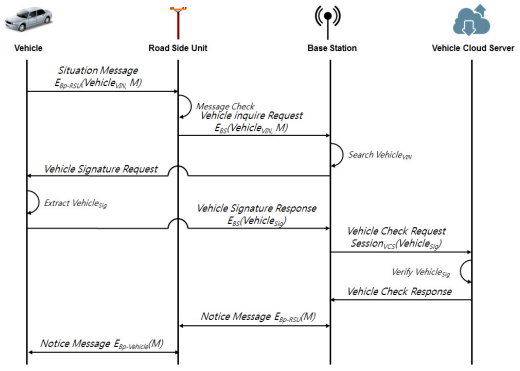

그림 4. Vehicle to Interface 메시지 통신 프로토콜
Fig. 4 V2I Message Protocol

1. 차량은 Road Side Unit으로부터 상황 메시지를 전송한다.

$$E_{Bp-RSU}(Vehicle_{VIN}, M) \quad (4)$$

2. Road Side Unit는 메시지를 검증 후 Base Station으로 차량 조사 요청 메시지를 전송한다.

$$E_{Bp-BS}(Vehicle_{VIN}, M) \quad (5)$$

3. Base Station은 $Vehicle_{VIN}$을 검사 후 차량으로 서명 요청 메시지를 전송한다.
4. 메시지를 수신 후 차량은 $Vehicle_{Sig}$을 추출한다. 그리고 Base Station으로부터 $Vehicle_{Sig}$을 전송한다.
5. Base Station은 Vehicle Cloud Server로 차량 검사 요청 메시지를 전송한다.

$$Session_{VCS}(Vehicle_{Sig}) \quad (6)$$

4. $Vehicle_{Sig}$를 검사 후 응답 메시지를 Base Station으로 전송한다.
5. Base Station은 다른 Road Side Unit로부터 Message를 전송한다.

$$E_{BP-RSU}(M) \quad (7)$$

6. Road Side Unit은 지역 내 차량으로부터 처음 차량 상황에서 송신 받은 메시지를 전송한다.

$$E_{BP-Vehide}(M) \quad (8)$$

3.4. Vehicle to Vehicle 환경의 통신 프로토콜 설계

V2V기반에서 GPS를 활용하여 차량 메시지 전송 절차에 대하여 설명한다. 차량은 GPS로부터 상황 요청 메시지를 전송 후 Vehicle Cloud Server로부터 차량 및 GPS검증을 완료 후 GPS는 상황 요청 메시지를 전송한다.

1. 차량i은 GPS로부터 상황 요청 메시지를 전송한다.

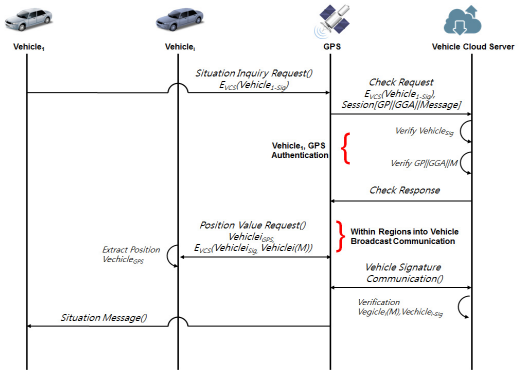

그림 5. Vehicle to Vehicle 메시지 통신 프로토콜
Fig. 5 V2V Message Protocol

2. GPS는 NMEA프로토콜을 이용하여 GPS의 Talker ID, Sentence ID, Message를 인증 받으며, $Vehicle1_{Sig}$을 Vehicle Cloud Server로 전송한다.

$$E_{VCS}(Vehicle1_{Sig}), Session[GP\|GGA\|Message] \quad (9)$$

3. Vehicle Cloud Server는 $Vehicle_{Sig}$와 GPS의 $GP\|GGA\|M$을 검증 후 GPS로부터 검증 응답 메시지를 전송한다.
4. GPS는 다른 차량으로부터 위치 값을 요청 후 전송받는다.

$$Vehiclei_{GPS}, EVCS(Vehicle_{i-Sig}, Vehicle_i(M)) \quad (10)$$

5. GPS는 Vehicle Cloud Server로부터 차량i의 서명 및 메시지를 검증 후 차량1로부터 상황메시지를 전송한다.

Ⅳ. 성능 분석 및 평가

4.1. 안전성 분석

차량 클라우드 환경은 VANET환경과 인터넷기반의 클라우드 환경이 융합되어 보안에 많이 취약하다. 위장, MITM, 부인, 정보유출과 같은 차량 클라우드 환경에서 발생하는 보안위협에 대하여 안전성을 분석하였다.

위장공격 : 인가되지 않은 사용자가 차량 클라우드 서버로 접속하여 불법적으로 데이터를 획득하는 행위이다. 하지만 차량 등록 및 인증 프로토콜에서 차량의 $Vehicle_{Sig}$을 생성 후 Vehicle Cloud Server로 인증함으로써 위장에 대해서 안전하다.

데이터 위·변조 및 MITM : 중간자 공격은 클라우드 환경에서 상호간에 통신을 수행 중 중간자가 침입하여 상호간의 메시지를 도청 및 위·변조 하는 공격이다. V2I 및 V2V기반에서 Bilinear Pairing기반의 암호를 사용하여 메시지를 전송함으로써 중간자 공격은 실패한다.

부인 : 악의적인 사용자가 차량을 탑승 후 V2I기반에서 메시지를 부인하고 전송해 피해를 주는 공격이다. 또한 DDos 및 Dos 공격으로도 안전할 수 없다. 본 논문에서는 $Vehicle_{Sig}$을 검증한다. 상호간의 Session Key를 활용하여 안전하게 전송하고 Base Station, GPS는 BS_{Cert}, $GP\|GGA$를 확인함으로서 부인방지를 할 수 있다.

정보 유출 : 인가되지 않은 사용자가 차량 클라우드 서버로 접속 후 Storage Server의 정보를 노출 시킬 수 있다. 이를 보완하기 위해 Vehicle Could Server는 차량 및 Road Side Unit의 접속 시 $Vehicle_{Sig}$을 확인하며 Base Station은 차량의 $Vehicle_{VIN}$을 등록함으로써 정보유출에 대하여 추적이 가능하다.

4.2. 보안성 평가

본 논문에서 구현된 시스템은 Inter(R) Core(TM)2 Quad CPU Q9400 @ 2.66HZz 2.66GHz, 4.00GB와 Windows 7 Ultimate K환경으로 구성되어 있으며, 시뮬레이션은 Eclipse IDE for Java Developers로 메시지 통신 프로토콜을 평가 하였다. 기존 차량환경에서 암·복호화를 수행하여 메시지의 통신하는 방법과 제안된 프로토콜에서 암·복호화를 수행하여 메시지를 통신하는 방식과의 비교 분석하였다. 성능평가는 [그림 6]과 같다.

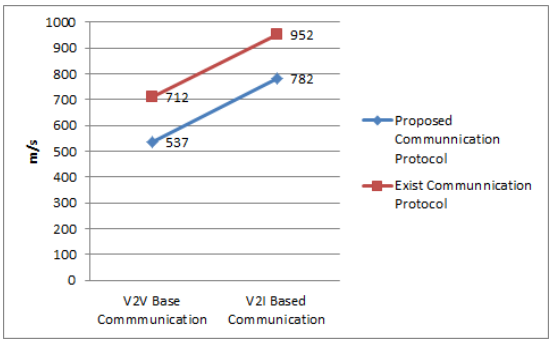

그림 6. 기존 시스템과 제안 프레임워크의 비교분석
Fig. 6 existing System And Proposed Framework of Comparison Analysis

V2I과 V2V의 통신 프로토콜에서 비교 분석을 하였으며, TTAK.KO-06.0174 표준 문서에서 참조된 ITS/Telemetic환경에서 수행되는 무선 통신환경의 통신방식을 기존의 시스템(PKI-1024)으로 구성하여 V2I 기반의 통신시스템과 제안된 프레임워크(IBE-160)와 비교분석하였다. 기존의 시스템은 6Encryption, 2Hash Function, 제안된 시스템은 6Encryption(2PKI+4IBE), 2Hash Function을 수행하였다.

V2V기반에서는 기존 시스템(4Encryption, 2Hash Function), 제안 프레임워크(4Encryption(2PKI+2IBE), 2Hash Function)을 수행하였다. 기존의 시스템에서는 PKI 암호화 부분을 활용하여 인증, 검증, 메시지 통신을 수행하는 반면, 제안된 시스템에서는 인증은 PKI기반 검증 및 통신 구간에서는 IBE기반을 활용하여 보다 빠르고 효율성을 확인 할 수 있었다. 정량적인 수치로는 수행속도단위 m/s으로 측정하여 기존의 시스템보다 V2I는 대략 32%, V2V는 대략 21%을 속도 향상을 확인할 수 있었다.

V. 결 론

본 논문에서는 차량 클라우드 환경에서 안전한 통신을 수행하기 위해서 보안 프레임워크를 설계하였다. 제안된 통신 프레임 워크는 클라우드 컴퓨팅 환경의 차량 클라우드 서버를 활용하여 차량을 등록 및 인증 후 V2I기반, V2V기반에서 통신 프레임 워크를 설계하였다.

기존의 차량네트워크 환경과 클라우드 환경에서 발생하는 공격기법과 보안 요구사항을 적용하여 안전성을 분석하였으며, 기존의 차량통신환경에서 수행하는 통신 프로토콜과 제안된 프로토콜과의 효율성을 비교분석하였다. 제안된 프로토콜은 기존의 환경보다 대략 32%, 21%을 확인할 수 있었다. 기존까지는 차량 네트워크, 클라우드 환경에 대한 연구는 활발하나 차량 클라우드 환경에 대한 연구는 미비하므로 신규 및 변종공격에 대한 안전성을 보장하기 위해서 보안사항 및 무선기반환경의 통신을 수행함으로써 개인정보 누출이 발생할 수 있으므로 기술 강화 및 보안정책이 필요하다.

REFERENCES

[1] Myung Hak Hu, Kyung Hyun Lee, “Vehicular And Security Requirement”, *korea institute of information Security & Cryptology*, vol 24, no 2, April.2013.

[2] TTAK.KO-12.0208, Security Requirements for Vehicle-to-Vehicle Communication, TTA, 2012.12.21

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

[4] S. Olariu, M. Eltoweissy, and M. Younis, “Towards autonomous vehicular clouds,” *ICST Transactions on Mobile Communications and Applications*, 11(7~9), 2011

[5] G. Yan, D. Wen, S. Olariu, and M. C. Weight, “Security Challenges in Vehicular Cloud Computing,” *IEEE Transactions on Intelligent Transportations System*, 14(1), pp.284-294, 2013.

[6] S. Olariu, T. Hristov, and G. Yan, “*The Next Paradigm Shift: From Vehicular Networks to Vehicluar Cloud*,” Mobile Ad Hoc Networking : Cutting Edge Directions, Second Eition, John wiley & Sons, Inc., 2013

[7] Brijesh Kumar Chaurasia, “Infrastructure based Authentication in VANETs. *International Journal of Multimedia and Ubiquitous Engineering*, Vol 6, No. 2, Apl, 2011

[8] G. YAN, D. B Rawat and B. B. Bista, “Toward Secure Vehicular Clouds,” *2012 Sixth International Conference on Complex, Intelligent, and SoftWare Intensive System*, pp. 370-375, 2012.

박중오(Jung-Oh Park)

성결대학교 컴퓨터학과 공학사
명지대학교 전자계산교육 석사
숭실대학교 컴퓨터공학 석사
숭실대학교 컴퓨터공학 박사
동양미래대학교 조교수
※관심분야 : PKI, Network security, Cryptography

최도현(Do-Hyeon Choi)

동서울대학 컴퓨터소프트웨어 공학사
숭실대학교 컴퓨터학과 석사
숭실대학교 컴퓨터학과 박사과정
※관심분야 : 모바일보안, 가상화, PKI