프라이버시 보호를 위한 V2V 통신 인증 서비스의 간략화

박승수[1], 한근희[2]*, 김기천[3]
[1]건국대학교 IT융합정보보호학과, [2]고려대학교 정보보호대학원, [3]건국대학교 컴퓨터공학과

The Simplified V2V Communication Authentication Service for Privacy Protection

Sung-Su Park[1], Keun-hee Han[2*], Keecheon Kim[3]
[1]Division of IT Convergence Information Security, Konkuk University
[2]Graduate School of Information Security, Korea University
[3]Division of Computer Science, Konkuk University

요 약 차세대 자동차 기술 중의 하나인 V2V 통신은 차량 간에 통신할 때 사용되는 기법으로 차세대 ITS의 핵심 기술이다. 기존 V2V 통신 인증 서비스 구조를 살펴보면 프라이버시 보호에 대한 보안 요구사항을 충족시키기 위해 가명 인증서를 사용한다. 가명 인증서를 사용하기 위해 발급 및 관리하는 기관이 필요하고 한번 발급할 때 여러 개의 인증서를 발급하기 때문에 시간이 많이 소요된다. 본 논문에서는 가명 인증서를 사용하지 않고 프라이버시 보호에 대한 보안 요구사항을 충족시키기 위해 차량 ID를 활용한 기법을 제시하고자 한다.

주제어 : WAVE, V2V, C-ITS, ITS, Authentication, Privacy Protection

Abstract One of the next generation of automotive V2V communication technology is a core technology for next-generation ITS as a technique used for communications between the vehicle. Looking at the existing V2V communication using the pseudonym certificate authentication service structure to meet the security requirements for privacy protection. Since the issuance of multiple certificates when needed authority in issuing and managing to use the pseudonym certificate issued once and it takes a lot of time. In this paper, we present the method utilizing a vehicle ID to meet the security requirements for the privacy protection without the use of a pseudonym certificate.

Key Words : WAVE, V2V, C-ITS, ITS, Authentication, Privacy Protection

1. 서론

사람들은 편리함을 추구하면서 많은 기술의 발전을 이뤄 왔다. 스마트 교통 분야도 예외는 아니다. 현재는 편의성을 넘어 교통사고를 줄일 수 있는 방안으로 차세대 ITS(Intelligent Transport Systems) 중 하나인 C-ITS(Cooperative-ITS)가 시범 사업 중에 있다[1].

기존의 ITS(Intelligent Transport Systems)는 교통정보를 수집하여 가공하고 제공하는 서비스로서, 상황판 및 인터넷, 모바일 등을 통해서 교통정보를 제공한다. 하지만 정작 운전자가 주행 중에 돌발 상황에 대한 교통 정보를 제공받기가 쉽지 않아 교통사고 시 신속한 대응에

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업(IITP-2016-H8501161012000100 2) 및 글로벌 딜리버리 클라우드 플랫폼의 대규모 OTT 서비스 적용을 위한 방송·통신 사업자 공동의 시범 사업의 연구결과로 수행되었음(No.B0511-15-0001)."
*교신저자 : 한근희(khhan@formal.korea.ac.kr)
접수일 : 2016년 3월 20일, 수정완료 : 2016년 3월 20일, 최종게재확정 : 2016년 3월 30일

한계가 있었다. C-ITS는 주행 중에 지속적으로 도로 인프라 및 다른 차량, 차 내/외부의 여러 사물들과 상호 통신을 통해 교통서비스를 실시간으로 교환 및 공유가 가능해짐으로 사전 대비 및 사후 대응이 가능해진다[2]. 여기서 차량과 차량 간 통신을 위해 나온 기술이 V2V(Vehicle to Vehicle) 통신 기술이다[3].

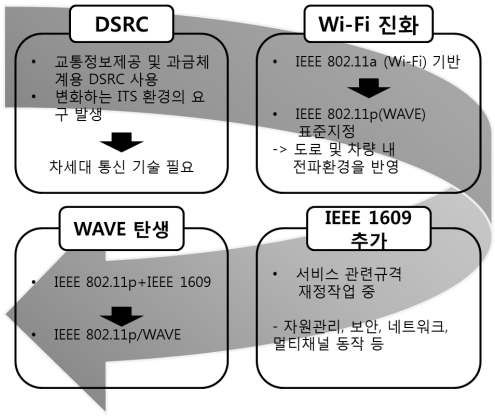
본 논문에서는 V2V와 V2I(Vehicle to Infra)를 위한 통신 기술인 WAVE와 그에 관련된 국제 표준인 IEEE 1609.2 대해 소개하고 V2V 통신상의 보안 위협 및 보안 요구 사항에 맞춰 현재의 인증 서비스 구조에 대해 살펴본 후, 한정된 자원에서의 효율성을 증대하기 위한 방안을 제안한다.

2. 관련 연구

2.1 WAVE

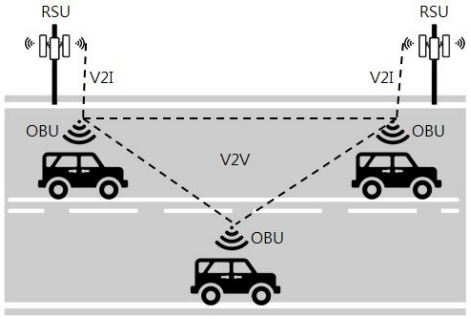
(Wireless Access in Vehicular Environments)

WAVE는 고속으로 주행하는 차량 환경에서 차량과 차량 간(V2V, Vehicle to Vehicle) 또는 차량과 길 위에 설치된 장치간의 무선 통신(V2I, Vehicle to Infra)을 제공하기 위해 특화된 차세대 ITS 통신 기술이다[4]. WLAN 기술을 기반으로 자동차 환경에 맞도록 수정된 기술로서 DSRC (Dedicated Short Range Communication) 기술의 일종이다. Fig. 1은 WAVE 규격의 탄생 과정에 대해서 보여준다.



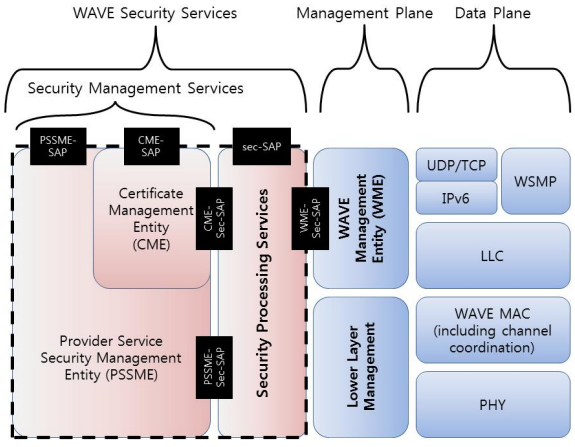
[Fig. 1] WAVE Protocol Process

이동성을 가진 차량에 설치된 무선 통신 장치를 OBU(On Board Unit)라 부르고 도로주변 시설물에 설치된 무선 통신 장치를 RSU(Road Side Unit)라고 한다. RSU와 OBU간의 통신이 가능하고 이를 V2I(Vehicle to Infra) 통신이라 하며, V2I 통신을 통해 실시간 교통상황과 돌발 상황, 교통 제어상태 등의 교통 정보를 제공하게 된다. OBU와 OBU간의 통신은 V2V 통신이라 하며 이를 통해 전방의 교통 정보와 차량 접근 알림, 추돌 경고등의 교통 정보를 제공받을 수 있다. 이러한 WAVE를 위한 표준으로 IEEE 1609 Series가 있다. 그 중 IEEE 1609.2는 어플리케이션 및 관리 메시지를 위한 보안 서비스 (Security Services for Applications and Management Messages)에 관한 표준으로 보안 메시지 형식을 정의하고 있다[5]. Fig. 2는 WAVE의 예를 보여주고 있다.



[Fig. 2] WAVE Protocol Example

WAVE Security Service의 Protocol stack은 Fig. 3과 같다. 본 논문에서는 IEEE 1609.2에서 정의하는 WAVE Security Service에 제한한다.



[Fig. 3] WAVE Security Service Protocol Stack

WAVE Security Service는 크게 Security Processing Services와 Security Management Services로 구성된다. Security Processing Services는 차량 데이터와 WSAs(WAVE Service Advertisements)가 보안 통신을

하기 위한 프로세스를 제공하고 Security Management Services는 CME(Certificate Management Entity)와 모든 인증서의 유효성과 관련된 관리 정보와 PSSME (Provider Service Security Management Entity)와 secured WSAs를 전송하는데 사용하는 개인키 및 인증서 관련 정보를 제공받는다. Table 1은 IEEE 1609.2에서 정의하고 있는 Security Service를 보여준다.

[Table 1] The role of WAVE Security Service Component

항목	역할
Sec-SAP	데이터 통신 시 보안 서비스 제공
PSSME-SAP PSSME-Sec-SAP	Secure WSA 전송 시 사용하는 인증서 및 개인키 정보 관리
CME-SAP CME-Sec-SAP	인증서 및 인증서 폐지 목록에 대한 정보 관리
WME-SAP	WSA 서명 생성 및 검증

2.2 V2V 통신 보안 위협 및 요구 사항

V2V 통신 환경에서 구체적인 보안 위협에 따른 공격 형태는 여러 형태가 있으나 이 논문에서 살펴볼 공격 형태는 차량 및 RSU 인증에 대한 공격과 프라이버시에 대한 공격 이 두 가지를 집중적으로 살펴본다.

차량 및 RSU 인증에 대한 공격으로 4가지의 공격 형태가 있다. 우선 차량의 위치 정보를 조작하여 전송하거나 GPS의 신호 정보를 조작하고 GPS 위치 정보를 스푸핑(spoofing)하는 라우팅 테이블과 LDM(Local Dynamic Map)의 변조 공격이 있고 공격자가 응급 차량 ID를 도용하여 전방에 있는 차량에 응급 차량이 접근한다는 잘못된 정보를 전송하는 위장(Impersonation) 공격이 있다. 또한, 공격자가 다수의 차량 ID를 도용하여 도로가 병목 상태에 있다는 잘못 된 정보를 전송하는 Sybil 공격, 마지막으로 PKI 인증 센터로 OBU가 침해당했다는 거짓 정보를 전달함으로 인증서를 폐기시키도록 유도하는 서비스 인프라에 대한 공격이 있다.

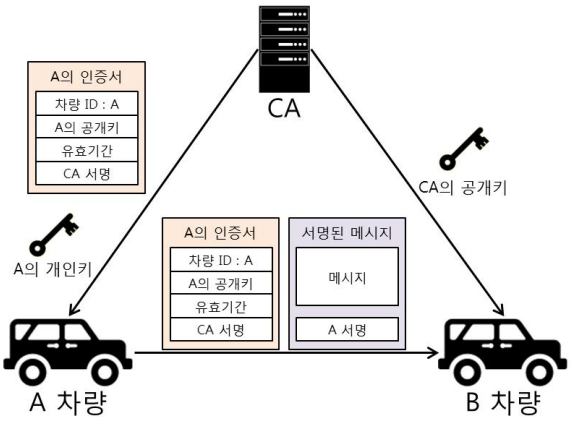
[Table 2] Detailed Security Requirements

항목	보안 요구 사항
차량 및 RSU 인증	-메시지 수신 차량은 메시지를 송신하는 차량을 인증할 수 있어야 함 -메시지 수신 차량은 메시지를 송신하는 RSU를 인증할 수 있어야 함 -차량 그룹 통신 서비스의 경우에는 특정 차량이 그룹의 멤버임을 확인 할 수 있어야 함
프라이버시 보호	-비인가 된 개체는 차량 통신상의 메시지를 분석하여 차량 또는 차량의 ID 또는 차량 위치 정보를 유추할 수 없어야 함 -비인가 된 개체는 차량 통신상의 메시지를 분석하여 차량의 경로를 유추할 수 없어야 함

프라이버시에 대한 공격 형태는 차량 통신 메시지를 수집 및 분석하여 차량의 소유자와 출발지, 경유지 및 목적지 등의 정보를 수집 및 활용하는 공격이다. Table 2는 세부적인 보안 요구 사항이다[6].

3. V2V 통신 인증 서비스 구조

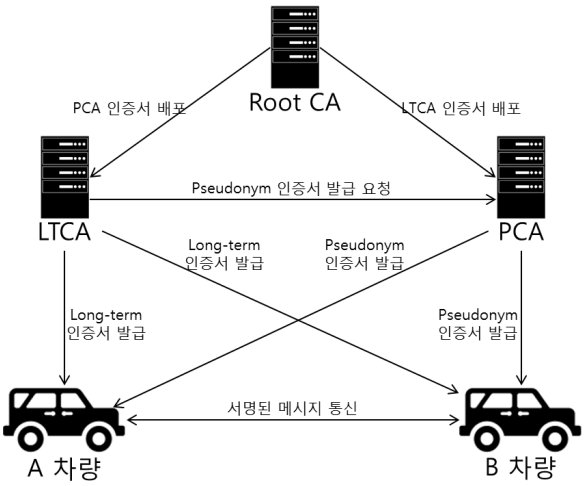
보안 요구 사항에서 보이듯이 2011년부터 개인정보보호법이 시행되면서 프라이버시 보호에 대한 보안 요구 사항이 추가되었다[7]. 프라이버시 보호에 대한 보안 요구 사항이 추가되기 전의 단순히 차량 간에 전송되는 메시지의 송신자와 위/변조 여부에 대한 검증을 위한 인증서비스 구조는 Fig. 4와 같다. CA(Certificate Authority)는 A차량에게 A의 인증서와 개인키를 발급하고 A의 인증서는 A에 대한 ID와 공개키, 유효기간 및 CA의 디지털 서명이 포함된다. A차량이 B차량과 통신을 한다고 가정하였을 때 A차량은 전송할 메시지를 A의 개인키를 활용하여 디지털 서명을 생성하여 A의 인증서와 함께 B차량에게 전송한다. B차량은 CA의 공개키를 활용하여 A의 인증서에 저장된 CA의 디지털 서명을 검증함으로써 A의 인증서에 대한 유효성을 증명하고 그 과정에서 획득한 A의 공개키를 활용하여 A의 디지털 서명을 검증함으로써 B차량이 수신한 메시지가 위/변조 되었는지, A차량으로부터 전송된 것이 맞는지 대한 여부를 알게 된다.



[Fig. 4] V2V Authentication Service Structure

앞선 프라이버시 보안 요구 사항에서 제시한바와 같이 차량의 위치와 이동 경로를 추적할 수 없어야 한다는

요구 사항을 만족하기 위해 가명(Pseudonym) 인증서를 활용한다. Fig. 5는 가명 인증서 발급 구조에 대해 나타내고 있다.

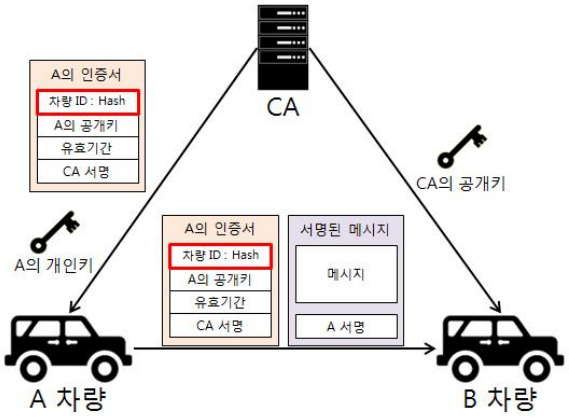


[Fig. 5] Issue Pseudonym Certificate Structure

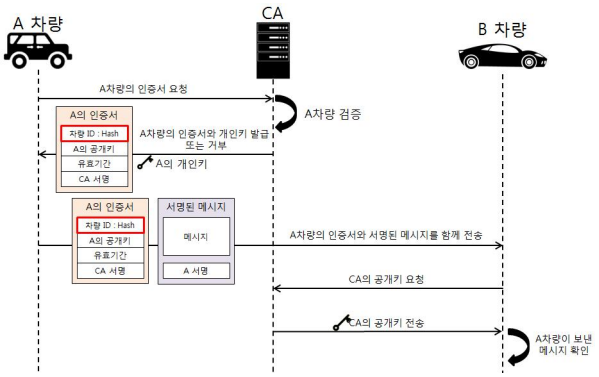
V2X 통신에서 사용되는 인증서는 Long-Term 인증서와 가명 인증서 두 가지 종류의 인증서를 사용한다. Long-term 인증서를 활용한 인증은 차량의 고유 ID가 필요한 경우에 사용되고, 가명 인증서는 차량 간 통신할 때 상대방 차량에 대해 식별이 가능해지면 프라이버시 보호에 문제가 발생하므로 상대방 차량에 대해 식별이 아닌 신뢰가 필요한 경우에 사용된다. 가명 인증서는 하나의 차량에 여러 개가 할당되어 사용된다. 가명 인증서가 발급되는 과정은 Fig. 5에 나타나 있다. Root CA는 LTCA(Long-term CA)에게 PCA(Pseudonym CA)의 인증서를 배포하고, PCA에게 LTCA의 인증서를 배포하여 LTCA와 PCA를 믿을 수 있는 기관이라고 인증해주는 역할을 한다. LTCA는 차량의 고유 ID와 연관된 Long-term 인증서를 발급하는 기관이다. 각각의 해당 차량의 수명과 연관된 긴 유효기간을 가진 인증서를 공개키 및 개인키와 함께 발급한다. 또한, LTCA는 PCA에게 해당 차량의 ID와 연관된 가명 인증서 발급을 요청한다. PCA는 LTCA로부터 요청을 수신하게되면, 해당 ID에 대한 가명 인증서를 발급한다. 가명 인증서는 공개키와 공개키의 유효기간, PCA의 디지털 서명을 포함하여 구성되며 필요에 따라서 해당 차량의 ID를 추적할 수 있도록 연관된 정보를 저장한다.

4. 개선된 V2V 통신 인증 구조

본 절에서는 가명 인증서를 활용하지 않고 프라이버시 보안 요구 사항을 만족하기 위한 방안에 대해 제시한다. Fig. 6은 개선된 V2V 통신 서비스 인증 구조를 나타낸다.



[Fig. 6] Improved V2V Authentication Service



[Fig. 7] Improved V2V Service Flow Chart

Fig. 7과 같이 CA에서 A차량에게 인증서를 발급해주기 전에 A차량의 고유한 ID를 테이블에 저장하고, salt 값을 이용하여 Hash 된 값을 인증서의 차량 ID란에 추가시킨다. 이렇게 생성된 A의 인증서는 주기적으로 약속된 salt값을 이용하여 차량 ID의 Hash값을 변형시킴으로 Hash함수 출력으로부터 Hash함수 입력을 찾아 낼 수 있다는 이론에 근거하여 반복적인 대입으로 암호를 알아내어 공격하는 birthday attack과 같은 공격에 대해 대비한다. 또한, A차량과 B차량이 통신을 할 때 차량 ID에 대해 Hash된 A의 인증서와 A의 개인키를 활용하여 디지털 서명된 메시지를 함께 B차량에게 전송한다. B차량은 CA의 공개키를 이용하여 A의 인증서를 검증함으로써 유효

성을 증명하고 그 과정에서 획득한 A의 공개키를 활용하여 A의 디지털 서명을 검증한다. 이 검증을 통해서 B차량이 수신한 메시지가 위/변조 되었는지, A차량으로부터 전송된 것이 맞는지에 대한 여부를 확인한다. 이 과정에서 A차량의 ID값에 대한 정보는 Hash되어 있기 때문에 식별이 불가능하다.

[Table 3] Comparison of Pseudonym Certificate and Hashed Certificate

가명 인증서	차량ID Hash된 인증서
-가명 인증서를 관리하는 PCA가 필요	-PCA가 생략 가능
-LPCA와 PCA를 인증하기 위한 Root CA가 필요	-하나의 신뢰할 수 있는 기관에서 처리가 가능하므로 Root CA가 생략 가능
-가명 인증서를 발급하기 위한 각각의 인증과정이 필요	-가명인증서를 발급하기 위한 각각의 인증과정이 생략 가능
-여러 개의 가명 인증서를 해당 차량에 일괄 전송으로 인해 시간소요 큼	-주기적으로 salt값을 변경하여 Hash값이 변경된 인증서를 V2I 통신을 통해 해당 차량에 전송

5. 결론 및 향후 연구 방향

본 논문에서는 V2V 통신을 할 때 차량 및 RSU 인증시와 프라이버시 보호에 관한 보안 위협과 그 위협을 감소시키기 위한 요구 사항에 대해 살펴보았고 요구 사항을 지키기 위해 가명 인증서를 활용한 V2V 인증 서비스 구조에 대해 살펴보았다.

본 논문에서 제시한 개선된 V2V 통신 인증 구조에서는 가명 인증서를 이용하지 않고 프라이버시 보안 요구사항을 만족하는 방안에 대해서 제시했다. Table 3은 가명 인증서 대신 차량 ID Hash화 시킨 인증서를 사용할 경우 취할 수 있는 이점에 대해 정리한 것이다.

향후 연구과제로는 개선된 V2V 통신 인증 구조에 맞는 가상 테스트 환경을 구축하여 차량 ID가 Hash된 인증서를 발급하는데 걸리는 시간을 측정하고 실제 서비스에 적용가능한지에 대한 연구를 진행하고자 한다.

REFERENCES

[1] Jong-Hun Byun and Byung-Woo Bae, “The Implementation of Cooperative Intelligent Transport System Pilot Project,” The Institute of Electronics Engineers of Korea, pp.1864-1867, 2015.

[2] Aymen Boudguiga, Arnaud Kaiser and Pierpaolo Cincilla, “Cooperative-ITS Architecture and Security Challenges: a Survey,” 22nd ITS World Congress, Paper number ITS-2629, October 2015.

[3] Jiang, D. and Delgrossi, L., "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," Proceedings of 67th IEEE Vehicular Technology Conference (VTC2008-Spring), Marina Bay, Singapore, May 2008.

[4] Uzcátegui, Roberto A. and Acosta-Marum, Guillermo, "WAVE: A Tutorial," IEEE Communications Magazine, vol. 47 (5), pp. 126-133, May 2009.

[5] IEEE, “IEEE Stnadard for Wireless Access in Vehicular Environments -Security Services for Applications and Management Message”, IEEE Std. 1609.2TM-2013 April 2013.

[6] TTA, “Security Requirements for Vehicle-to-Vehicle Communication,” TTAK.KO-12.0208, 2012.

[7] TTA, “Authentication Service Architecture for Vehicle -to-Vehicle Communication,” TTAK.KO-12.0238, 2013.

[8] William Whyte, Andre Weimerskirch, Virendra Kumar, Thorsten Hehn, “A Security Credential Management System for V2V Communications”, IEEE Vehicular Networking Conference, 2013.

[9] Jung-oh Park, Do-Hyeon Choi, “A Design of Framework for Secure Communication in Vehicular Cloud Environment”, Journal of the Korea Institute of Information and Communication Engineering, vol. 19, No. 9, pp. 2114-2120 Sep.2015.

[10] Seung-peom Park, Jae-won Ahn, Eun-gi Kim, “Design and Implementation of Secure Vehicle Communication Protocols for WAVE Communication Systems”, Journal of the Korea Institute of Information and Communication Engineering, vol. 19, No. 4, pp. 841-847, April 2015.

[11] Su-Hyun Kim, Im-Yeong Lee, “A Secure and Efficient Vehicle-to-Vehicle Communication Scheme using Bloom Filter in VANETs”, International Journal of Security and Its Applications, Vol. 8, No. 2, pp. 9~24, 2014.

[12] S. Dolev, L. Krzywiecki, N. Panwar, and M. Segal. Dynamic attribute based vehicle authentication. In IEEE 13th International Symposium on Network Computing and Applications (NCA), pages 1 - 8, 2014.

[13] S. Dolev, L. Krzywiecki, N. Panwar, and M. Segal. Optical puf for vehicles non-forwardable authentication. Technical Report 15-02, Department of Computer Science, Ben-Gurion University of the Negev, 2015. Also appears as a Brief Announcement in IEEE NCA 2015.

[14] S. Dolev, L. Krzywiecki, N. Panwar, and M. Segal. Vehicle authentication via monolithically certified public key and attributes. Wireless Networks, pages 1 - 18, 2015.
[15] Ernest, Foo, Christopher, Djamaludin and Andry, Rakotonirainy, “Security Issues for Future Intelligent Transport Systems”, Proceedings of the 2015 Australasian Road Safety Conference, pp.14-16, October 2015.

박 승 수(Sung-Su Park)

- 2012년 2월 : 한남대학교 전자공학과 (학사)
- 2015년 2월 ~ 현재 : 건국대학교 일반대학원 IT융합정보보호학과 석사과정

<관심분야>
사물인터넷 보안, 네트워크 보안, 스마트 자동차 보안

한 근 희(Keun-Hee Han) [정회원]

- 서울과학기술대학교 컴퓨터공학과 졸업
- 한양대학교 공학대학원 공학석사
- 고려대학교 대학원 이학박사
- 현재 : 고려대학교 융합소프트웨어전문대학원 산학교수

<관심분야>
소프트웨어 보증, 시큐어 코딩, 정보보호관리 체계, 개인정보보호, 클라우드 컴퓨팅 보안, 스마트 의료 보안, 스마트 공장 보안 등

김 기 천(Keecheon Kim)

- 1988년 : 서울대학교 계산통계학 (공학사)
- 1992년 : 미국 Northwestern Univ. (공학박사)
- 1992년 ~ 1996년 : 한국통신기술(주) 선임연구원
- 1996년 ~ 1998년 : 신세기 통신(주) 책임연구원
- 1998년 ~ 현재 : 건국대학교 컴퓨터공학과 교수

<관심분야>
mobile wireless network, 미래인터넷보안, sensor network, 네트워크 보안, 사물인터넷