차량 네트워크 보안 이슈 및 기술 동향

정수환* · 최재덕**

1. 서 론

최근 차량 네트워크 (Vehicular Ad-Hoc Network, VANET)가 산업계 및 학계에서 큰 주목을 받고 있다. 미국에서는 IEEE, ASTM, ANSI와 같은 다양한 ITS (Intelligent Transportation System) 표준 단체에서 차량 네트워크에 대한 표준 작업을 진행하고 있으며, 유럽에서는 C2C-CC (Car-to-Car Communication Consortium) 산업 컨소시엄을 구성하여 차량 네트워크 인프라 및 응용 서비스에 대한 연구 활동을 진행하고 있다 [1-3]. 차량 네트워크는 차량 운전자의 안전을 도모하기 위한 Vehicle-to-Vehicle (V2V) 네트워크와 주행 중에 RSU (Roadside Unit)와 같은 네트워크 액세스 노드를 이용하여 인터넷 서비스를 이용할 수 있는 Vehicle-to-Infrastructure (V2I) 네트워크 구조로 구분된다.

차량 네트워크는 차량 안전 통신을 통해 운전자 및 승객의 생명을 보호하는 것을 주목적으로 하기 때문에, 다른 어떤 네트워크보다 신중하고 엄격한 보안 기술이 요구된다. 예를 들어, 공격자가 차량 추돌 및 충돌 방지를 위한 경고 메시지를 조작 및 전파하는 방법으로 고의적인 차량 사고를 유발하여 운전자의 생명을 위협할 수 있다. 이와 같은 보안 위협들을 차단하기 위하여 차량 네트워크에서는 인증, 서명, 부인 방지 기능이 반드시 필요하다. 또한, 최근에 개인의 사생활 정보 유출에 대한 관심이 높아지면서, 차량 네트워크에서도 운전자의 이동 경로 및 위치 파악에 대한 프라이버시 보호 기능이 요구된다.

차량 네트워크에서는 서명과 같은 보안 기능을 요구하기 때문에 공개키 암호 알고리즘을 이용한 보안 구조가 적합하다. 현재 차량 네트워크 보안 기술은 PKI (Public Key Infrastructure) 환경에서 보안 구조와 ID-based Cryptosystem (IBC)을 이용한 보안 구조가 연구되고 있다. PKI 구조는 안전한 보안 기능을 제공하지만, CRL (Certificate Revocation List) 관리에 대한 오버헤드 문제 때문에 빠르게 이동하는 차량들 사이에서 실시간으로 전송되는 차량 안전 메시지에 신속하게 대응하기 어렵다. PKI의 구조적인 문제를 해결하기 위하여, IBC를 이용한 보안 구조가 연구되고 있지만, IBC 기반의 보안 구조는 Key escrow 문제와 같은 IBC 자체의 본질적인 보안 문제 때문에 신중하고 엄격하게 다루어져야 하는 차량 네트워크에서 보안 취약성이 발생할 수 있다.

※ 교신저자(Corresponding Author) : 정수환, 주소 : 서울시 동작구 상도동 1-1(156-743), 전화 : 02)820-0714, FAX : 02) 821-7653, E-mail : souhwanj@ssu.ac.kr
* 숭실대학교 정보통신전자공학부 부교수
** 숭실대학교 정보통신전자공학부
(E-mail : cjduck@cns.ssu.ac.kr)

본 논문에서는 차량 네트워크에서 보안 요구사항을 살펴보고, 최근에 연구되고 있는 PKI와 IBC 방식의 차량 네트워크 보안 기술들에 대해서 살펴본다.

2. VANET 보안 위협 및 요구사항

2.1 보안 위협

차량 네트워크에도 다양한 공격들이 존재하지만, 다음과 같이 크게 두 가지 보안 위협 형태로 분류 할 수 있다.

• 메시지 조작

거짓 정보를 생성하거나, 정상 메시지를 일부 조작하여 다른 차량들에게 전달하는 공격으로, 차량 네트워크에서 인적 피해 및 물적 피해를 야기할 수 있는 보안 위협이다. 차량 안전과 관련된 응용 서비스에서, 공격자가 조작된 메시지를 발생하여 사고를 유발하거나, 교통 흐름 관리 서비스에서 차량들을 특정 경로로 유도하는 메시지를 발생하여 교통 정체를 야기할 수 있다.

• 개인 프라이버시 침해

최근 개인 프라이버시 문제가 중요한 이슈가 되고 있는 가운데, 차량 네트워크에서도 운전자의 위치 및 이동 경로에 대한 사생활 침해 문제가 크게 부각되고 있다. 차량 환경에서 근거리 무선 통신 규격인 DSRC (Dedicated Short Range Communications)/ WAVE (Wireless Access in Vehicular Environment)에 의하면, 차량들은 매 100 ~ 300 ms 마다 차량 통신에 관련된 제어 메시지를 전송해야 한다. 따라서 운전자는 자신의 의도와는 상관없이 차량의 위치 또는 이동 경로 정보를 그대로 무선 네트워크상에 노출한다.

2.2 보안 요구사항

앞서 살펴본 보안 위협과 빠르게 이동하는 차량 네트워크의 고유 특성을 고려할 때, 다음과 같은 보안 기능들이 필요하다.

• 인증 및 부인 방지

차량 네트워크의 모든 메시지에 대해서, 수신측은 송신측을 인증할 수 있어야 하고, 전송되는 모든 메시지에 대해서 서명 기능이 제공되어야 한다. 또한, 서명 기능을 통해 전파된 메시지에 대해서 송신측이 메시지 전송 사실을 부인할 수 없어야 한다. 이와 같은 보안 요구 사항을 통해 차량 네트워크에서 메시지 조작에 의한 다양한 공격들을 예방할 수 있다.

• 빠른 서명 생성 및 검증 시간

차량은 MANET (Mobile Ad-Hoc Networks) 이동 노드와 달리 풍부한 컴퓨팅 능력과 자원을 보유한 노드이기 때문에, 암호 알고리즘 적용시 큰 부담이 없다. 하지만, 차량들은 시속 200 Km/h의 빠른 속도로 이동할 수 있기 때문에 차량 안전 메시지 송·수신시 암호 알고리즘 적용에 따른 처리 시간을 최소화해야 한다.

• 조건부 프라이버시

운전자의 개인 정보를 보호하기 위하여, 차량 네트워크 통신에서 차량의 ID에 대한 익명성을 제공해야 한다. 그러나 무조건적인 익명성을 제공할 경우, 차량 사고 또는 범죄와 연관된 차량들에 대해서 실제 차량을 추적할 수 없는 문제점이 발생한다. 따라서 차량 사고 및 범죄와 같은 특수 상황에서는 정부 기관에 의해서 익명성을 제공받는 차량의 실제 ID가 무엇인지 추적할 수 있는 기능을 제공해야 한다.

3. VANET 보안 기술 동향

차량 네트워크 보안 기술은 메시지에 대한 서명 기능이 필요하기 때문에 공개키 암호 알고리즘을 사용하여 보안 구조를 구축해야 한다[4]. 현재 공개키 암호 알고리즘을 사용한 차량 보안 구조는 PKI 방식과 IBC 방식으로 분류된다.

3.1 PKI 방식의 보안 구조

그림 1은 IEEE 1609.2에서 정의하는 PKI 방식의 차량 네트워크 보안 구조이다[5]. 송신 차량이 WAVE 메시지를 생성하고 자신의 개인키로 메시지를 서명한 후 서명된 메시지를 브로드캐스트한다. 메시지를 수신한 차량 및 RSU들은 송신 차량의 인증서의 유효성을 검증한 후 서명된 메시지를 검증하고 적절한 행동을 취한다.

PKI 환경에서 인증서는 인증서 소유주나 CA (Certificate Authority)의 비밀키 손상 또는 의심

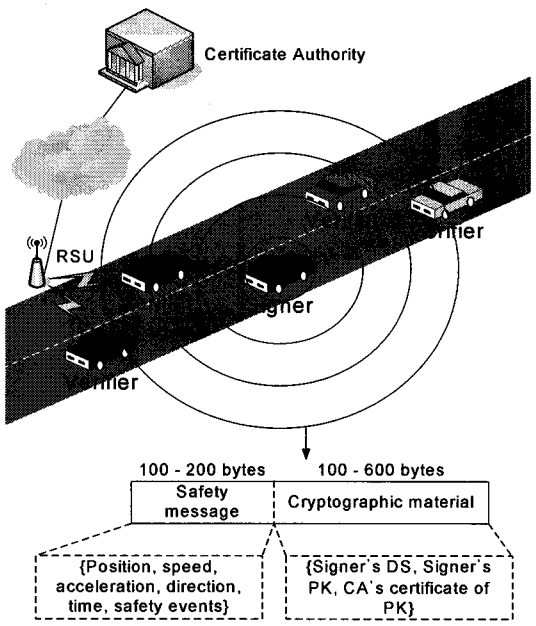


그림 1. PKI 방식의 보안 구조

될 경우, 비밀키 도난 또는 누출, 비밀키 저장 장치의 손상, 인증서 정보의 변경, 인증서 소유주 관련 정보가 더 이상 유효하지 않은 경우, 다른 인증서로 대체한 경우에 폐기되어야 한다. 인증기관으로부터 인증서 폐기가 결정되면 폐기가 결정된 인증서는 X.509 CRL에 포함되어 CA로부터 차량들에게 발송되며, CRL을 수신한 차량은 자신의 CRL에 포함 시킨 후 이웃한 차량에게 전달함으로써 모든 차량은 동일한 CRL을 공유한다. 이후 차량은 CRL에 포함된 인증서를 사용하여 생성된 메시지를 수신한 경우에 악의적인 사용자로 인식하여 수신된 메시지를 무시한다.

그러나 CRL 구조에서 메시지 수신 차량은 송신 차량의 인증서를 검증하기 위하여 온라인 통신을 해야 하기 때문에, 기반 구조가 갖춰져 있지 않은 V2V 네트워크에 적합하지 않다. 또한, 차량들이 고속으로 이동하기 때문에 차량 안전 메시지와 같이 신속한 반응을 요구하는 서비스에서 메시지 송신 차량의 인증서 유효 검증을 위한 온라인 통신으로 수신 차량들이 신속하게 대응하기 어렵다. 이와 같은 문제를 해결하기 위하여 효과적으로 CRL 기능을 해결할 수 있는 기술이 연구되고 있다[6].

• RTPD

RTPD (Revocation of the Tamper-Proof Device)는 자신의 인증서가 TPD (Tamper-Proof Device)에서 안전하게 폐기되어 그 폐기된 인증서를 소유한 사용자가 공격자 자신이라고 하더라도 더 이상 폐기된 인증서를 사용할 수 없게 하는 방식이다. 즉, CA에서 발급한 CRL 리스트를 공격자가 인식하지 못하고 TPD에서만 인식하여 자동 폐기하도록 하는 방식이다. 그림 2는 RTPD 동작 절차를 보여준다. CA에서 악의적인 차량 M의 인증서를 CRL 리스트에 포함하고, M의 공개

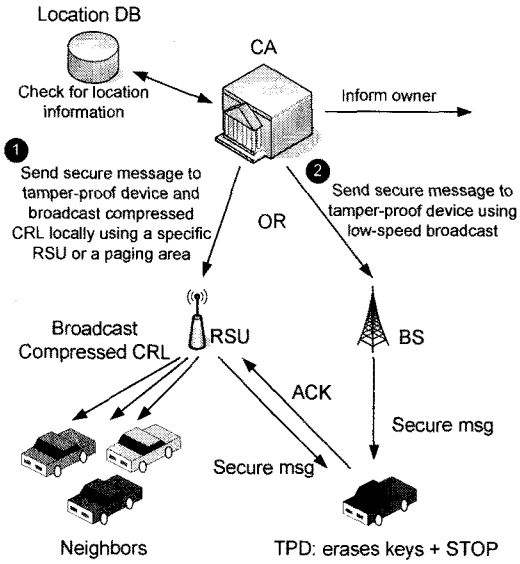


그림 2. RTPD 인증서 폐기 방법

키로 암호화해서 M에게 전달한다. M은 암호된 CRL 리스트 목록을 메시지 스니핑을 통해서 확인할 수 없다. 오직 TPD에 저장된 개인키로만 CRL 리스트가 복호화 되기 때문에 공격자 M은 자신의 인증서가 폐기되었다는 사실을 인식하지 못한다.

• RCCRL

RCCRL (Revocation by Compressed CRLs)은 폐기해야 하는 인증서의 목록이 많을 경우 CRL의 크기를 줄이기 위하여 Bloom 필터를 사용하는 방식이다. CA에서 차량 M 또는 다수 차량의 인증서가 폐기 대상으로 결정되면 정상적인 차량들에게 CRL을 효율적으로 알리기 위해 CA는 폐기 대상 인증서 리스트를 Bloom 필터를 사용하여 생성한다. CA는 압축된 RCCRL을 서명하여 모든 차량들에게 전달한다. BS (Base-Station)를 통해 전달된 RCCRL을 수신 한 차량들은 RCCRL을 저장하고, 추후에 다른 차량의 인증서를 수신하였을 때, RCCRL에 포함되어 있는지 확인하는데 사용한다. 만약 특정 차량 M의 인증서가 RCCRL에 포함되어 있다면 차량 M으로부터 수신되는 메시지를 무시한다.

• DRP

DRP (Distributed Revocation Protocol)는 악의적인 사용자를 CA에 알리는 과정으로 주변의 차량들이 평판 시스템을 이용하여 악의적인 차량 M에 대해서 평가를 하고, 이를 CA에게 알리는 방식이다. CA는 대표 차량 A로부터 차량 M이 악의적인 사용자라는 신고를 접수 받은 경우 CRL을 다른 사용자들에게 알린다. DRP는 기존 인증서 폐기 과정을 CA가 아닌 차량들에 의해서 시작된다는 점이 앞서 설명한 것과 차이점이다. DRP는 신속하게 의심되는 차량을 주변 차량들에 의해서 신속하게 인증서 폐기 리스트에 포함할 수 있지만, 의심되는 차량을 정확하게 식별하기 어려운 문제점이 있다.

3.2 IBC 방식의 보안 구조

인증서 관리를 위한 기반 구조와 CRL 리스트에 대한 오버헤드 문제 때문에 PKI 방식 대신에 또 다른 해결 방안으로, IBC 방식의 보안 구조가 연구되고 있다. IBC는 Ad-hoc 네트워크와 같이 기반 구조가 없는 환경에 적합한 공개키 암호 기술로써, IP 주소 또는 이메일 주소와 같은 사용자의 식별자를 이용한 암호 방식이다[7]. IBC 방식에서는 KGC (Key Generation Center)라는 제 3의 신뢰 기관이 자신의 마스터 키와 사용자의 ID를 사용하여 사용자의 개인키를 직접 생성하여 분배한다. KGC로부터 개인키를 분배받은 사용자들은 메시지를 서명할 때, 자신의 개인키를 이용하여 메시지를 서명하고, 서명된 메시지를 수신한 사용자는 송신자의 ID를 이용하여 서명된 메시지

를 검증한다. 또한, 메시지 기밀 통신에서는 수신측의 ID를 이용하여 송신측에서 메시지를 암호화하고, 수신측에서 자신의 개인키를 사용하여 암호화된 메시지를 복호화 한다. IBC 방식에서는 상대방 인증을 위한 절차가 따로 없고, 메시지 서명 검증 단계를 통해서 신뢰하는 방식이기 때문에 PKI에서와 같이 상대방의 인증서를 검증하기 위한 추가적인 절차를 요구하지 않는다. 따라서 Ad-hoc 네트워크와 같이 기반 구조가 없는 환경에서 유용하게 사용될 수 있다. 다음은 IBC 방식을 이용한 차량 네트워크의 보안 기술들이다.

• PKI와 IBC Signcryption을 조합한 보안구조

IBC 기법을 이용하여 차량 네트워크에 실질적으로 적용한 보안 구조로써, PKI 방식과 IBC signcryption 기법을 조합한 방식이 연구되었다[8]. 이 방식에서 CRL은 RSU에서만 관리하고, 차량에서는 CRL을 관리하지 않는 방법을 통해 차량 네트워크 전반에 걸쳐 CRL 관리 부담을 줄였다. 그림 3에서 차량들은 최초 CA로부터 ID, 공개키, 인증서, IBC 파라미터들을 받고, RSU들은 CA의 IBC 마스터 키를 안전하게 분배받아 저장한다. 이후 차량들은 RSU를 통해 운전자 프라이버시를 위한 pseudonym과 IBC 개인키를 다음과 같은 절차를 통해 발급 받는다. 먼저, RSU에서는 각 차량들의 인증서를 받아 인증서 유효성을 검사하고, 이상이 없을 경우에 차량의 인증서에 포함된 공개키를 사용하여 각 차량의 임시 ID와 그에 맞는 IBC 개인키를 암호화하여 전달한다. RSU로부터 임시 ID와 IBC 개인키를 받은 차량은 IBC signcryption 기법을 이용하여 보안 통신을 한다.

• IBC Threshold 서명 기법 기반의 보안구조

IBC threshold 서명 방식을 이용한 보안 구조는 차량들에게 pseudonym 기반의 프라이버시를 제

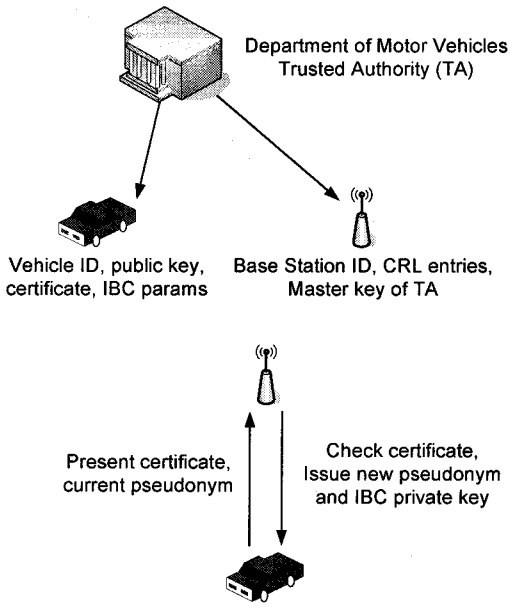


그림 3. 시스템 초기 설정과 Pseudonym 생성 단계

공하고, 만약 차량 사고와 같은 사건이 발생할 경우 threshold 서명 기법을 사용하여 어느 하나의 정부 기관에 의해서만 독단적으로 사용자의 ID를 추적할 수 없도록 하는 기능을 제공한다[9]. 즉, threshold 개의 기관으로부터 서명 받은 메시지를 수집해야만 차량의 원래 ID를 추적할 수 있는 권한이 생긴다. 또한 차량 네트워크를 홈 도메인과 외부 도메인으로 정의하여 차량들이 서로 다른 도메인을 이동할 경우, 경계 BS에서 이전 도메인에서 인증 받은 차량인지 인증을 수행하고, 이상이 없을 경우 새로운 도메인에서 사용할 수 있는 IBC 기반의 개인키와 임시 ID를 발급한다.

• 그룹 서명과 IBC 서명 기법 기반의 보안구조

본 보안 구조에서는 차량과 차량 간의 통신과 차량과 RSU 간의 통신 구조로 나누어 각각 그룹 서명 기법과 IBC 서명 기법을 분리하여 적용하는 방식을 제안하였다[10]. 그림 4는 차량과 차량 사이에서 안전 통신을 위한 보안 구조를 보여준다.

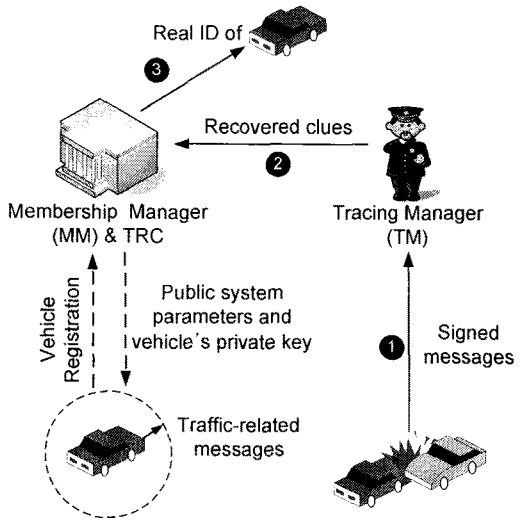


그림 4. 차량 간 안전 통신을 위한 보안 구조

차량과 차량 간 통신에서 프라이버시 기능을 제공하기 위한 그룹 서명 기법은, TRC (Transportation Regulation Center)라는 정부 기관을 통해 그룹 관리가 이루어진다. 그룹 서명을 통해 차량과 차량 사이에 통신에서 상호 신분을 확인할 수 없지만, TRC에 의해서 필요한 경우에 신분을 확인할 수 있다. 차량과 RSU 사이에 통신에서는 RSU가 차량 안전 메시지 등을 제공하기 때문에 RSU에 대한 프라이버시 기능을 제공할 필요가 없어서 IBC 서명 기법을 이용한다.

3.3 PKI vs IBC 방식의 보안 구조

현재 PKI와 IBC 방식을 이용한 연구가 진행되고 있는 가운데 IEEE 표준에서 PKI 방식을 이용하여 표준화 작업이 이루어지고 있다. PKI 방식이 차량 네트워크에서 요구하는 보안 기능을 충분히 제공하지만, 효율적인 인증서 관리에 대한 연구에도 불구하고 여전히 PKI 환경 구축에 대한 부담과 CRL 관리 부담이 존재한다. 또한 PKI 방식에서는 운전자의 프라이버시 문제도 해결해야 할 과제이다.

PKI의 구축 및 CRL 관리 부담을 해결하기 위하여, IBC를 이용한 보안 구조가 제안되었지만, IBC는 key escrow 문제 때문에 차량 네트워크에서 요구하는 강력한 보안 기능을 제공하기 어렵다. 즉, KGC에서 모든 사용자의 개인키를 생성할 수 있기 때문에 차량 네트워크에서 임의의 메시지에 대해 KGC에 의해 메시지가 서명되거나 기밀 통신에 사용된 암호키가 복구될 수 있는 문제가 존재한다. 또한, IBC 방식에서는 차량의 개인키를 더 이상 사용할 수 없게 될 경우 개인키 폐기 문제도 해결해야 할 과제이다.

4. 결 론

차량 네트워크에 대한 활용도가 높이 평가되면서, 보안 구조에 대한 연구가 최근 활발하게 이루어지고 있다. 본 논문에서는 차량 네트워크에서 보안 요구사항과 최근 연구되고 있는 PKI와 IBC 방식을 이용한 보안 기술에 대해서 살펴보았다. PKI 방식이 IEEE 표준으로 정의되어 있지만, 앞으로 차량 네트워크에 실제로 적용하기 위한 PKI와 IBC 보안 구조에 대해 지속적인 연구가 필요한 시점이다.

참 고 문 헌

[1] National ITS Architecture, http://www.odetics-its.com/itsarch/html/standard/standard.htm
[2] Car 2 Car Communication Consortium, http://www.car-to-car.org/
[3] 최병철, 김정녀, "차량 통신 보안 및 프라이버시 주요 이슈," *한국정보과학회 학술지*, Vol.22, No. 1, May 2008.
[4] M.E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a fu-

ture vehicular network," *Proc. European Wireless 2002*, Feb. 2002.

[5] IEEE Std 1609.2, IEEE Trial-use standard for wireless access in vehicular environments - Security services for applications and management messages, 2006.

[6] M. Raya, P. Papadimitratos, and J.P. Hubaux, "Securing vehicular communications," IEEE *Wirel. Commun.*, Vol.13, No.5, pp. 8-15, Oct. 2006.

[7] A. Shamir, "Identity-based cryptosystems and signature schemes," *Proc. CRYPTO'84, LNCS 196*, pp. 47-53, 1984.

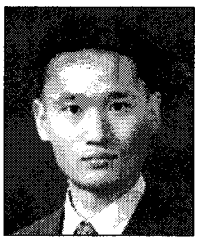
[8] P. Kamat, A. Baliga, and W. Trappe, "An Identity-based security framework for VANETs," *Proc. VANET06*, pp. 94-95, Sept. 2006.

[9] J. Sun, C. Zhang, and Y. Fang, "An ID-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," *Proc. MILCOM2007*, Oct. 2007.

[10] X. Lin, X. Sun, P.H. Ho, and X. Shen, "SIS: A secure and privacy preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, Vol.56, No.6, pp. 3442-3456, 2007.

정 수 환

- 1985년 서울대학교 전자공학과 학사
- 1987년 서울대학교 전자공학과 석사
- 1996년 University of Washington 박사
- 1996년~1997년 Stellar One SW Engineer
- 1997년~현재 숭실대학교 정보통신전자공학부 교수
- 관심분야 : 차량네트워크 보안, VoIP 보안, 이동 네트워크 보안, RFID/USN 보안 등



최 재 덕

- 2002년 숭실대학교 정보통신전자공학부 학사
- 2004년 숭실대학교 정보통신공학과 석사
- 2005년~현재 숭실대학교 전자공학과 박사과정
- 관심분야 : 차량네트워크 보안, VoIP 보안, 이동 네트워크 보안