VANET 환경에서의 사용자 인증 기법

서 화 정◆, 김 호 원°

User Authentication Method on VANET Environment

Hwa-jeong Seo◆, Ho-won Kim°

요 약

지금까지 VANET 상에서의 보안은 차량과 차량 그리고 차량과 도로 주변 장치 간의 통신에 국한되어 연구되어 왔다. 이를 통해 VANET 상에서 전송되는 메시지의 인증 및 무결성의 확보가 가능했다. 하지만 정작 차를 운전하는 운전자와 차량에 대한 인증에 대한 기법은 지금까지 활발히 연구되지 않았다. 만약 불법적인 사용자가 불법적인 차량을 통해 VANET 통신에 가입하여 잘못된 정보를 생성하게 된다면 다른 운전자의 안전이 보장될 수 없다. 따라서 VANET 상에서의 운전자의 안전을 위해 본 논문에서는 사용자와 차량 간의 인증이 가능한 기법을 제안하여 올바른 차량과 사용자만이 VANET에 참여하도록 한다. 이를 통해 운전자는 안전하고 편안한 주행을 보장받게 된다.

Key Words : 사용자 인증, 차량 애드혹 네트워크, 공개키 암호화, 공인인증서, 전자 신분증, 스마트 폰

ABSTRACT

Security over VANET among vehicles and between vehicles and infrastructures has been studied. Through the research, ensuring the message authentication and confidentiality was possible. However, authentication on drivers and vehicles were not actively covered. Once, malicious user using illegal vehicle joins VANET and then generates mistaken information, other drivers' safety will be driven to crisis. For this reason, in the paper, we present a novel authentication method between drivers and vehicles and then only right vehicles and users can participate in VANET. As a result of this, drivers can enjoy their safe and comfortable trip.

Ⅰ. 서 론

차량과 인프라 간의 통신을 의미하는 차량 애드혹 네트워크(VANET, Vehicular Ad ho NETwork)는 이동하는 차량에 설치된 통신 모듈인 OBU (On Board Unit)가 도로변에 설치된 RSU (Road Side Unit)에게 자동차의 속도, 가속도, 그리고 위치정보를 알려주고 RSU에서는 OBU에게 도로의 상태정보인 교통정보, 기상 변화, 도로의 결빙 그리고 상대방 차량의 정보 등을 알려줌으로써 발생 가능한 위험을 예방하는데 있다[1-3]. VANET에 대한 효용성이 높아짐에 따라 현재 VANET 통신에 대한 다양한 표준화 작업이 진행되고 있으며 미국에서는 특히 통신 표준인 DSRC (Dedicated Short Range Communication)을 제정하여 차량통신에 대한 명확한 기준을 제시하고 있다[4]. 차량은 표준에 따라 400m의 전송반경으로 메시지를 전송하며 이는 멀티홉을 통해 먼 거리까지 정보를 전달하게 된다. VANET은 그 응용에 따라 차량 간의 통신인 V2V (Vehicular to Vehicular) 혹은 V2I (Vehicular to

※이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2010-0026621).
◆ 주저자 : 부산대학교 컴퓨터공학과 정보보호 연구실, hwajeong@pusan.ac.kr, 준회원
° 교신저자 : 부산대학교 컴퓨터공학과 정보보호 연구실, howonkim@pusan.ac.kr, 종신회원
논문번호 : KICS2012-04-225, 접수일자 : 2012년 4월 29일, 최종논문접수일자 : 2012년 6월 11일

Infrastructure)로 수행되며 이를 통해 차량은 안전한 운행에 필요한 정보를 전달함과 동시에 다른 차량들에게 정보를 제공하는 제공자의 역할을 하게 된다. 전송되는 메시지는 차량 운행에 매우 민감한 정보를 포함하기 때문에 정보의 변조 및 악용은 사용자에게 큰 위협으로 다가오고 있다. 따라서 차량 들 간의 안전한 보안 통신은 VANET 통신을 활성화하기 위한 초석으로써 큰 의미를 가진다.

현재까지 VANET 상에서의 V2V 그리고 V2I 간의 안전한 통신을 위한 메시지 인증, 무결성, 부인방지, 익명성 보장을 위한 연구가 지속적으로 진행되어 왔다. VANET 상에서의 보안의 주된 동향은 그룹 서명, 조건부 익명성, RSU와 OBU 간의 인증, 메시지의 추적성의 제공 그리고 효율적인 암호화 수행을 통한 낮은 복잡도의 암호화 기법등이 제안되어 빠르고 안전한 VANET 보안 기법들이 제안되어 왔다[5-11].

이처럼 지금까지의 VANET 통신의 주된 연구 주제는 차량과 RSU 그리고 차량과 차량 간의 인증을 비롯한 보안 통신이었다. 하지만 VANET 통신을 수행하기 위한 가장 초기화 단계에는 차량 그 자체에 대한 인증이 필요할 뿐 아니라, 운전자에 대한 인증도 동시에 수행되어야 한다. 이러한 전제 조건의 성립 없이는 VANET 상에서의 안전한 통신이 불가능한 것은 자명한 사실이다. 이러한 문제점을 해결하기 위해 본 논문에서는 운전자의 스마트폰에 저장된 전자 운전면허증과 차량의 인증정보를 이용하여 상호간에 안전한 인증을 암호화된 메시지를 통해 수행하는 기법을 제안한다. 해당 기법은 사용자와 차량에 대한 인증을 통해 VANET 상에서 전송되는 메시지의 신뢰도를 높여 모든 운전자의 안전을 확보하는데 크게 기여할 것이다. 이는 지금까지 연구되지 않았던 차량과 사용자 인증에 대한 연구로써 OBU, 스마트 폰 그리고 인증기관을 묶는 새로운 개념의 구조와 스마트 폰을 통한 안전한 인증 프로토콜을 제안한다. 이를 통해 본 논문에서는 전자 신분증의 미래 효용성 및 실용성에 대한 고찰해 본다.

본 논문은 다음과 같이 구성된다. 2장에서는 사용자의 전자서명 및 스마트폰을 통한 인증에 대해 알아본다. 3장에서는 제안하는 시스템 모델 및 기법에 대해 설명한다. 4장에서는 제안하는 기법의 안전성과 효율성을 분석하고 마지막으로 5장에서는 본 논문의 결론을 내린다.

Ⅱ. 관련 연구

해당 장에서는 본 논문에서 제안하는 새로운 기법에 기반 및 근거가 되는 기술들에 대해 열거 하며 이를 통해 논리적인 논문의 전개가 가능하도록 한다.

2.1. 전자 운전면허증

국내 운전자는 자동차를 운행하기 위해서는 국내 DDP(Domestic Driving Permit)을 받아야 한다. 이는 플라스틱 형태의 신분증으로 현재 모든 운전자가 널리 사용하고 있지만 위·변조에 취약할 뿐 아니라 해외에서 운전 시 국제 면허증인 IDP(International Driving Permit)를 취득해야 하는 번거로움이 있다. 현행 플라스틱 운전면허증에 대한 문제에 대한 해결을 위해 국제 표준기구인 ISO에서는 IDL(ISO Compliant Driving License)를 제정하여 언제 어디서나 전자적으로 경찰의 터미널을 통해 확인이 가능한 운전면허증을 권고하고 있다[12-14]. 따라서 앞으로의 전자 운전면허증에 대한 관심 및 요구는 IT 산업의 발전과 기술의 보편화로 인해 점차 가속화 될 것으로 예상된다.

2.2. 스마트 폰과 OBU 통신

전자 운전 면허증에 대한 안전한 관리 및 보관을 위해서는 사용자가 가지는 안전한 장비에 인증에 필요한 정보를 보관하여야 한다. 2010년도 조사결과에 따르면 전세계의 21%의 인구가 스마트폰을 사용하고 있다고 한다[15]. 특히 스마트폰은 그 자체가 가지는 높은 성능, GPS, WIFI, 3G 그리고 다양한 센서들을 통해 차량이 감지하기 힘든 여러 가지 환경 조건들을 감지하는 것이 가능하여 앞으로의 VANET과 융합되어 새로운 기술로써 활용될 가능성이 점차 확대되고 있다[16,17]. 현재 BMW와 포드를 포함하는 차량 제조사들이 차량에 스마트 폰과의 통신이 가능한 인터페이스를 제공하여 VANET 상에서 보다 가치 높은 정보의 생성 및 조달이 가능하도록 하고 있다[18,19]. 해당 기술은 근접 네트워크 통신기술인 블루투스를 통해 스마트 폰과 차량의 OBU를 묶어주며 이를 통해 사용자는 차량의 상태 정보에 좀 더 쉽게 접근하여 사용하는 것이 가능할 뿐 아니라 차량 입장에서도 지금까지 많은 연구가 선행되었던 스마트 폰 상에서의 위치 측위 기술을 통해 보다 정확한 정보 취득이 가능하다[20-24]. 앞으로 VANET과 스마트폰의 결합은 보다 가속화 될

것으로 전망되며 이를 통해 보다 많은 서비스의 창출도 예상된다.

2.3. 스마트 폰을 통한 인증 기법

현재 스마트폰을 통한 식별 및 인증이 가능한 서비스(뱅킹, 금융서비스, 전자민원)가 폭넓게 활용되고 있다. 안전한 거래를 위해 국내에서는 1999년에 전자서명법에 근거한 공인인증서를 제정하여 사용을 권고하고 있다[25]. 이는 오프라인상에서의 기명 서명과 동일한 효력을 가지며 공개키 기반으로 서명을 하여 내용의 무결성과 서명에 대한 부인방지 기능을 포함한다. 현재 스마트폰 상에서의 공인인증서의 사용은 2010년 3월에 개정된 '무선단말기에서의 공인인증서 저장 및 이용 기술규격'에 따라 (PKCS #11)기반으로 사용되고 있다[26]. 하지만 공인인증서는 2013년 이후에는 안정성 보장이 힘들어 RSA 2,048비트와 SHA-256로의 교체를 추진 중에 있다[27,28]. 이를 기반으로 생각해 볼 때 안전하고 편리한 스마트 폰 상에서의 공인인증서를 통한 인증기법은 모든 국민들에게 빠른 시일 안에 사용될 것으로 예상된다.

Ⅲ. 본 문

본 장에서는 제안하는 기법에 대해 자세히 설명한다. 해당 기법은 사용자와 차량의 등록, 사용자와 차량 간의 상호인증 그리고 추후 사용자가 차량을 변경하는 경우에 발생하는 폐기 단계로 구성된다. 자세한 내용은 아래와 같다.

3.1. 사용자와 차량 인증 기법

사용자와 차량 간의 인증을 효율적으로 수행하기 위해 본 논문에서는 3단계에 걸친 제안 기법을 구술한다. 해당 제안 기법을 구성하는 개체는 인증을 총괄하는 인증센터, 차량을 제조하는 제조사, 운전자의 전자 운전면허증을 발급하는 사무실 그리고 차량과 운전자로 구성되며 사용되는 용어의 정리는 다음 표 1과 같다.

표 1. 제안 기법에서 사용되는 표기 및 설명
Table 1. Notation and its description in the proposed method.

표기	설명
N_C	회사 일련번호
N_V	자동차 일련번호
N_O	사무소 일련번호
ID_V	자동차 아이디
ID_U	사용자 아이디
ID_{NU}	주민등록번호
ID_{UV}	자동차와 사용자의 통합 아이디
KEY	자동차 비밀키
KEY	사용자 비밀키
KEY	사용자와 자동차 간의 대칭키
T	타임스탬프
R_a	a에 의해 생성된 난수
RM	폐기 메시지
$Cert$	인증서
P_a	공개키 기반 암호화에서 a의 공개키로 암호화
S_a	대칭키 기반 암호화에서 a의 개인키로 암호화
$H(\bullet)$	해시 함수

3.1.1.등록단계

등록단계는 크게 차량의 등록과 사용자의 등록으로 나뉜다. 그림 1은 차량의 등록단계를 나타내며 수행 순서는 다음과 같다. 차량이 제조되면 차량 제조 공장에서는 회사의 일련번호와 자동차의 일련번호 그리고 난수값을 CA의 공개키로 암호화하여 전달하게 된다. 이를 확인한 CA에서는 공장의 공개키로 제조된 차량의 아이디와 비밀키 그리고 전송받은 난수값을 암호화하여 전송하게 된다. 공장에서는 해당 메시지의 복호화에서 난수값을 확인함으로써 제대로된 CA에서 온 메시지임을 확인하며 전송받은 차량의 아이디와 비밀키를 안전한 회선(SSL 암호 링크 설정)을 통해 차량으로 전송한다.

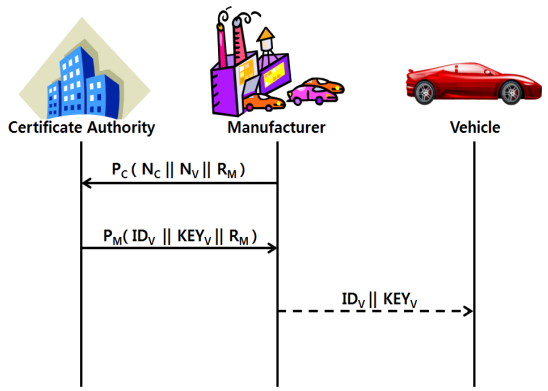

그림 1. 차량 등록 단계
Fig. 1. Registration process of vehicle

사용자는 운전면허에 합격하게 되면 운전면허증을 담당하는 사무실에서 자신의 스마트폰을 통해 운전자로 등록하는 단계를 거치게 된다. 사용자는 먼저 사무실로 안전한 회선(NFC)을 통해 자신의 주민번호를 전달하게 된다. 이를 전달받은 사무실에서는 사무실의 일련번호와 운전자의 주민번호를 신뢰기관의 공개키로 암호화하여 전달하게 된다. 신뢰기관에서는 해당 사무소가 지정된 기관인지를 확인하고 사무실의 공개키로 운전자에게 제공될 새로운 아이디와 비밀 키를 암호화하여 전송하게 된다. 사무실에서는 사무실의 비밀 키로 복호화하여 얻게 된 아이디와 비밀 키를 운전자에게 안전한 회선을 통해 전송함으로써 등록단계를 마무리하게 된다.

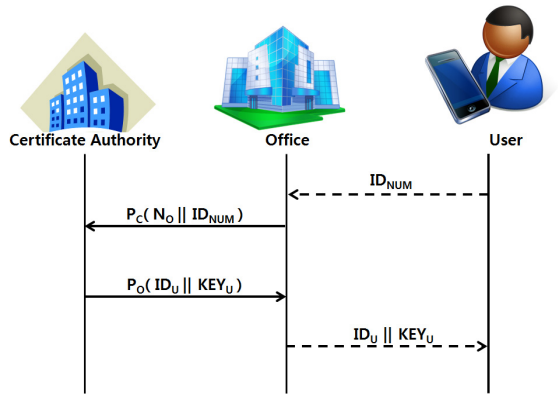

그림 2. 사용자 등록 단계
Fig. 2. Registration process of user

3.1.2. 인증단계

사용자는 자신의 스마트폰과 OBU간의 블루투스 통신을 통해 운전자 아이디를 전송하게 된다. 차량에서는 타임스탬프와 난수값을 생성하게 되며 해당 값은 해시연산을 통해 사용자와의 대칭키로 사용되게 된다. 사용자의 아이디와 타임스탬프 그리고 난수값은 CA의 공개키로 암호화하여 사용자에게 보내게 된다. 사용자는 해당 암호문에 차량의 아이디와 새로운 난수 및 타임스탬프를 묶어 CA의 공개키로 암호화하여 보내주게 된다. CA에서는 타임스탬프를 확인하여 재전송 공격을 확인한 후 비밀 키를 이용하여 암호문을 복호화하게 된다. 복호화를 통해 얻게 된 차량의 타임스탬프와 난수값은 해시연산을 통해 사용자와 차량의 대칭키로 사용이 되며 사용자와 차량의 아이디 그리고 사용자의 타임스탬프와 난수값도 해시연산을 통해 사용자와 차량을 대표하는 하나의 아이디를 생성하게 된다. 생성된 키와 아이디 그리고 난수값은 사용자의 공개키로 암호화되어 사용자에게 전달되게 되며 사용자는 해당 암호문을 복호화하여 자신의 난수값을 확인함으로써 CA와 사용자간의 상호인증이 가능하게 된다. 사용자는 이어 자신의 난수와 타임스탬프 그리고 공유 아이디를 서로 간의 대칭키를 이용하여 암호화 한 후 차량에 전송하게 된다. 전송된 값은 복호화 되어 차량은 아이디를 생성해보게 되고 해당 아이디가 전송된 아이디와 동일함을 확인하면 사용자와 신뢰기관에 대한 상호인증과정이 성공적으로 이루어짐을 확인 할 수 있다.

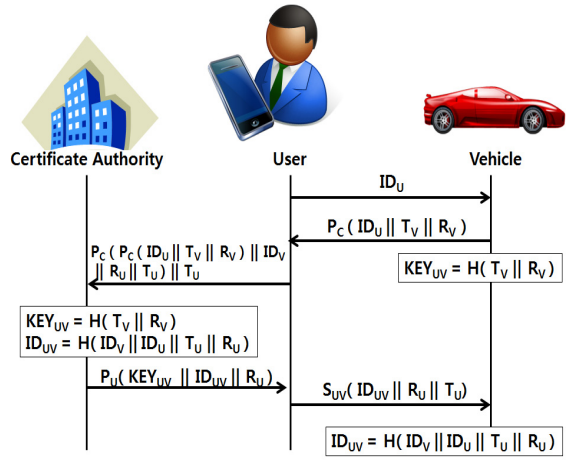

그림 3. 사용자 인증 단계
Fig. 3. User authentication process

3.1.3. 폐기단계

만약 키 폐기단계를 거치지 않은 사용자는 다른 새로운 차량에 대한 아이디와 키 생성이 불가능하도록 하는 경우사용자가 차량을 변경하는 경우 해당 사항을 신뢰기관에 신속히 전달하여 키 폐기단

표 2. 성능 분석도
Table 2. Performance analysis.

수행 단계		차량 등록	사용자 등록	사용자 인증	키 폐기
수행연산	총	$2P_E+2P_D$	$2P_E+2P_D$	$3P_E+3P_D+S_E+S_D+4H$	$P_E+P_D+S_D+S_E+2C+2V$
	CA	P_E+P_D	P_E+P_D	P_E+2P_D+2H	P_D+S_E+C+V
	U	·	·	$P_E+P_D+S_E$	P_E
	V	·	·	P_E+S_D+2H	S_D+C+V
	M	P_E+P_D	·	·	·
	O	·	P_E+P_D	·	·

P_E: 공개키 암호화, S_E: 대칭키 암호화, P_D: 공개키 암호화, S_D: 대칭키 암호화, H: 해시 함수, C: 메시지 서명
V: 메시지 인증, CA, U, V, M, O: 신뢰기관, 사용자, 자동차, 공장, 사무실

계를 거쳐야 한다. 먼저 운전자는 공유 키와 아이디를 신뢰기관의 공개키로 암호화하여 알리게 되며 이는 대칭키로 암호화되어 키폐기 메시지와 이에 대한 인증서를 첨부하여 사용자에게 전달된다. 전달된 메시지는 차량에 전달되어 인증서를 확인한 후 메시지에 이상이 없으면 키폐기 메시지에 대한 차량의 인증서를 작성하여 사용자에게 전달하게 된다. 이를 전달받은 사용자는 해당 메시지를 신뢰기관에 전달하게 되고 이를 확인한 신뢰기관에서는 해당 키 폐기가 성공적으로 끝났다는 메시지를 사용자에게 전달해주게 된다.

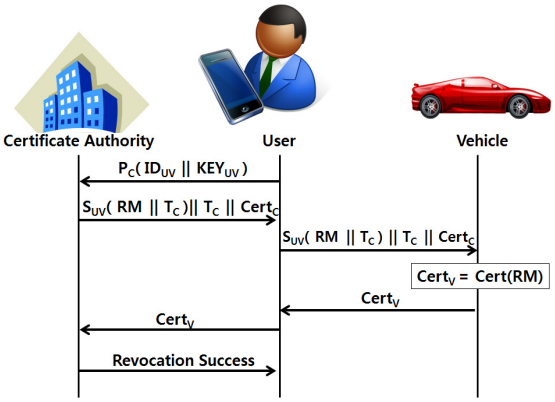

그림 4. 키 폐기 단계
Fig. 4. Key revocation process

Ⅳ. 성능 평가 및 보안성 분석

본 장에서는 해당 논문에서 제시한 사용자 인증 기법의 성능과 보안성에 대해 분석하여 나타냄으로써 제안 기법의 성능 및 안전도에 대해 살펴보게 된다.

4.1. 성능 평가

본 논문에서 제안하는 전자 신분증과 차량의 특수한 정보를 이용하여 사용자 및 차량을 인증하는 기법은 지금까지 많은 연구가 진행되지 못하여 비교할만한 뚜렷한 기준이 나타나 있지는 않다. 따라서 표 2에서는 해당 논문에서 사용된 연산을 표시하여 추후에 있을 보다 진보된 연구들의 비교 잣대가 되었으면 한다. 성능 분석도를 통해 사용자 인증 제안 기법의 복잡도를 확인해 보면 CA에서 가장 많은 연산을 수행하며 차량과 사용자는 비슷한 복잡도의 연산을 수행한다. 현재 스마트 폰과 OBU는 이전의 컴퓨팅에 비해 많은 발전이 있었지만 CA에 비해서는 낮은 성능을 보이는 것이 사실이므로 현 논문의 연구 결과는 자원 한정적인 임베디드 장비에 부담을 덜 주며 인증이 가능하므로 보다 효율적이라고 할 수 있다.

4.2. 보안성 분석

◇ 비연계성

차량의 완벽한 익명성을 보장하기 위해서는 사용되는 아이디를 통해 공격자를 사용자와 차량을 판단하는 것이 불가능하도록 해야 한다. 본 논문에서는 사용자와 자동차간의 공유 아이디 생성 시 사용자와 자동차의 아이디와 난수값 그리고 타임스탬프와 같은 다양한 인자들을 통해 연계성을 가지지 않는 신선한 아이디가 매번 생성되도록 하였다.

◇ 추적성

익명성이 보장되는 경우라도 사고가 발생하거나 사건이 발생한 경우 해당 차량과 운전자에 대한 정확한 확인이 가능하도록 해야 한다. 해당 제안 기법에서는 사용자와 자동차의 아이디가 아닌 공유 아이디를 사용하지만 등록단계와 인증단계에서 해당 아이디와 1대1로 매칭되는 데이터베이스가 유지되므로 추후 공유 아이디를 통해 추적이 가능하다.

◇ 재사용 공격

차량, 운전자, 사무실 그리고 공장 사이에는 서로 간의 물리적인 인증이 가능할 뿐 아니라 경우에 따라 안전한 채널로 전송된다. 따라서 해당 세션에 대해서는 재사용 공격을 생각하지 않는다. 사용자 인증 단계에서는 사용자가 타임 스탬프를 메시지와 함께 전송하게 된다. 이때 메시지가 해당 시간 안에 도착하게 될 경우에만 올바른 인증으로 인식하게 된다.

◇ 상호인증

메시지의 전송 시 해당 메시지를 보낸 개체와 받은 개체 간의 상호인증을 위해 전송되는 메시지는 공개키 기반의 암호화로 진행되었으며 또한 사용자 인증과정에서는 신뢰기관의 비밀키로 풀어야만 생성 가능한 사용자와 차량의 대칭키를 신뢰기관이 생성하여 사용자에게 전달하게 되고 사용자는 대칭키를 이용하여 메시지를 전달함으로써 사용자, 신뢰기관 그리고 차량을 아우르는 구조 안에서 상호간에 인증이 가능한 특징을 가진다.

◇ 패스워드 추측 공격

사용자가 사용하는 암호화 키는 RSA 2,048 비트이며 이는 현재 알려진 모든 공격에 안전하다고 알려져 있다. 따라서 현실적인 시간 안에 해당 비밀번호를 알아내는 것은 불가능하다고 할 수 있다.

Ⅴ. 결 론

본 논문에서는 사용자와 차량 간에 안전한 인증 기법에 대해 설명하였다. 이를 위해 스마트 폰과 OBU 그리고 인증기관을 묶는 하나의 인증 구조를 제안하였으며 다양한 응용을 통해 해당 기법의 효용성을 확인했다. 가능한 위협에 대해서도 안전할 뿐 아니라 공개키 기법을 이용하여 보다 효율적인 인증이 가능하도록 제안하였다. 이는 앞으로 중요시될 VANET 상에서의 인증에 도움이 될 것이며 이를 통해 사용자와 차량에 대한 인증의 필요성을 조명해보는 계기가 될 것으로 생각된다.

References

[1] Youngjun Cho, Hyunseung Lee, Namje Park, Dooho Choi, Dongho Won, Seungjoo Kim, “Security Trend of VANET Security,” KIISC, Vol. 19, No. 1, pp. 134-142, 2009.

[2] H. Hartenstein and K. P. Laberteaux, “A Tutorial Survey on Vehicular Ad Hoc Networks,” *IEEE Communications Magazine,* vol. 46, no. 6, pp. 164-171, Jun. 2008.

[3] Y. Toor, P. Muhlethaler, A. Laouiti, and A. Fortelle, “Vehicular ad hoc networks: Applications and related technical issues,” *IEEE Communication Survey & Tutorial,* vol. 10, no. 3, pp. 74-88, 2008.

[4] JongTaek Oh, “5.9GHz DSRC Frequency Standard of America,” *TTA Journal*, vol. 98, pp. 122-132, 2005.

[5] M. Raya and J. P. Hubaux, “Securing Vehicular Ad hoc Networks,” *Journal of Computer Security,* Vol. 15, No. 1, pp. 39-68, Jan. 2007.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications,” *IEEE Transaction on Vehicular Technology,* Vol. 56, No. 6, pp. 3442-3456. Nov. 2007.

[7] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications,” *Proceedings IEEE INFOCOM,* pp. 1903-1911, Apr. 2008.

[8] C. Zhang, X. Lin, R. Lu, and P. Ho, “RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks,” *IEEE International Conference on Communications,* art. no. 4533317, pp. 1451-1457, May. 2008.

[9] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, “An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor

Networks," *Proceedings IEEE INFOCOM,* pp. 816-824, Apr. 2008.

[10] A. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical Short Signature Batch Verification," *Proceedings of CT-RSA, Lecture Notes in Computer Science,* Vol. 5473, pp. 309-324, Apr. 2009.

[11] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," *IEEE Transactions on Vehicular Technology,* Vol. 59, No. 4, pp. 1606-1617, May. 2010.

[12] "ISO 18013-1, Information technology-Personal identification-ISO-compliant driving licence-Part 1: Physical characteristics and basic data set," *ISO,* 2005.

[13] "ISO 18013-2, Information technology-Personal identification-ISO-compliant driving licence-Part 2: Machine-readable technologies," *ISO,* 2007.

[14] "ISO 18013-3: Information technology-Personal identification-ISO-compliant driving licence-Part 3:Access control, authentication and integrity validation," *ISO,* 2006.

[15] Vasileios Manolopoulos, "Security and privacy in smartphone based intelligent transportation systems," *Royal institute of technology,* 2012.

[16] "White Paper: How TomToms HDTraffic And IQRoutes Data Provides The Very Best Routing." [Online]. Available: http://www.tomtom.com/lib/doc/download/HDT_White_Paper.pdf. [Accessed: 25-Apr-2012].

[17] D. Work and A. Bayen, "Impacts of the mobile internet on transportation cyber-physical systems: Traffic monitoring using smartphones," i*n National Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation, & Rail,* pp. 18-20. 2008.

[18] "Ford Sync." [Online]. Available: http://www.ford.com/technology/sync/. [Accessed: 25-Apr-2012].

[19] "BMW Connected." [Online]. Available:http://www.bmw.com/com/en/owners/bmw_apps/app_bmw_connected.html. [Accessed: 25-Apr-2012].

[20] "ITU Key Global Telecom Indicators for the World Telecommunication Service Sector." [Online]. Available: http://www.itu.int/ITUD/ict/statistics/at_glance/KeyTelecom.html. [Accessed: 25-Apr-2012].

[21] Y. Yim, "The state of cellular probes," 2003. [Online]. Available:http://escholarship.org/uc/item/8g90p0vw.pdf. [Accessed: 11-Apr-2012].

[22] D. Valerio, A. D'Alconzo, F. Ricciato, and W. Wiedermann, "Exploiting Cellular Networks for Road Traffic Estimation: A Survey and a Research Roadmap," *VTC Spring 2009 - IEEE 69th Vehicular Technology Conference,* pp. 1-5, Apr. 2009.

[23] H. Bar-Gera, "Evaluation of a cellular phone-based system for measurements of traffic speeds and travel times: A case study from Israel," *Transportation Research Part C: Emerging Technologies,* vol. 15, no. 6, pp. 380-391, Dec. 2007.

[24] M. Fontaine, B. Smith, A. Hendricks, and W. Scherer, "Wireless Location Technology-Based Traffic Monitoring: Preliminary Recommendations to Transportation Agencies Based on Synthesis of Experience and Simulation Results," *Transportation Research Record,* vol. 1993, no. 1, pp. 51-58, Jan. 2007.

[25] "Law of DSA", vol. 10008, 2010.

[26] "Technology of certificate storage and usage ", KISA, 2010.

[27] Elaine Barker, William Barker, William Burr, William Polk, Miles Smid, "Recommendation for Key Management Part 1: General(Revised)", *SP 800-57, NIST,* March 2007.

[28] Elaine Barker, Allen Roginsky, "Transitions:Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", *SP 800-131A, NIST*, January 2011.

서 화 정 (Hwa-jeong Seo)

2010년 2월 부산대학교 정보컴퓨터공학과(공학사)
2010년 2월~2012년 2월 부산대학교 컴퓨터공학부 석사
2012년 3월~현재 부산대학교 컴퓨터공학부 박사
<관심분야> 정보보안, RFID/USN, 암호 이론, VLSI 설계

김 호 원 (Ho-won Kim)

1993년 2월 경북대학교 전자공학과(공학사)
1995년 2월 포항공과대학교 전자전기공학과 (공학석사)
1999년 2월 포항공과대학교 전자전기공학과 (공학박사)
2008년 2월 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원 / 팀장
2008년 3월~현재 부산대학교 정보컴퓨터공학부 교수
<관심분야> 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안