M2M 환경에서 지능형 자동차 네트워크기반의 보안 요구사항

김기원*, 김수균**, 이근호***

요약

지능형 자동차망의 성공은 보안위협에 대처하기 위한 견고한 보안 구조의 설계와 잠재적인 보안 위협 분석을 통해서 가능하다. 본 논문에서는 M2M(Machine to Machine) 환경에서 지능형 자동차망의 보안에 대해서 살펴본다. M2M에서 지능형 자동차망의 적합한 보안 관리와 보안 위협요소 분석을 제공한다. 지능형 자동차 망에서 왜 안전이 필요한지와 이러한 문제 요구를 구체적으로 어떻게 접근하는지에 대해서 설명한다. 임베디드 시스템 보안, 포렌식 보안, 사용자와 자동차 인증, 키관리와 Threshold 암호 기법에 대한 보안 요구사항을 제안한다.

The Security Requirement based on Intelligent Vehicular Network in M2M Environment

Gi-Weon Kim*, Soo-Kyun Kim**, Keun-Ho Lee***

ABSTRACT

A success of the intelligent vehicular networks has to pass through the analysis of potential security threats and the design of a robust security architecture able to cope with security threats. In this paper, we present the security of intelligent vehicular networks in M2M environment. We provide a detailed security threat analysis and an appropriate security management of the intelligent vehicular networks in M2M . We have explained why intelligent vehicular networks need to be secured, and why this problem requires a specific approach. We proposed a security requirement that imbedded system security, forensic security, user and vehicular authentication, key management and threshold encryption scheme.

Key Words : M2M(Machine to Machine), Authentication, Intelligent Vehicular, Forensic, Key Management

* 초당대학교 컴퓨터과학과(✉kwkim@chodang.ac.kr)
** 배재대학교 게임공학과
*** 백석대학교 정보보호전공
· 제1저자(First Author) : 김기원 · 교신저자(Correspondent Author) : 이근호
· 접수일(2010년 11월 1일), 수정일(1차 : 2010년 11월 30일), 게재확정일(2010년 12월 3일)

Ⅰ. 서 론

IT분야의 급격한 발전은 개인용 PC, 인터넷, 스마트폰 등의 다양한 새로운 서비스 환경을 만들어 가면서 급속도로 사회의 변화를 주도하고 있다. 특히 언제 어디서나 정보를 이용할 수 있는 유비쿼터스 환경으로 빠르게 진화가 이뤄지고 있다. 유비쿼터스 환경은 정보통신기술 분야를 기반으로 융합분야의 발전과 함께 많은 새로운 분야의 연구가 이뤄지는 계기가 되었다. 그러한 분야중에서 장치와 기계간의 통신을 위한 M2M (Machine to Machine)은 이동통신 사업자와 연구자들간의 주요기술 연구분야로서 다양한 서비스 환경을 만들어가면서 새로운 기술을 적용하고 있다.

M2M 통신은 기기의 기구들을 컴퓨터의 본체에서부터 일상적인 전자제품과 자동차까지 연결해 다양한 정보전송이 가능하도록 진행중이다. 이 개념은 기계들이나 기기들이 원격지에서 이동통신과 전송매체를 통해서 자신이 원하는 데이터와 주변 정보를 수집하여 수집 장소로 전송하는 것이 가능하도록 하는 것이다. 기계들과 우리의 일상생활 속에 널리 퍼져있는 기기장비간의 통신을 통한 다양한 서비스 제공을 위한 새로운 개념이다.

현재의 M2M 통신 개념은 최신 이동통신 서비스인 LTE(Long Term Evolution)망을 넘어 다양한 유무선망의 진화를 통해 사람과 사물 사이의 상호작용을 통해 위치 기반의 교통정보, 건강, 주변 온도 등 다양한 데이터를 얻을 수 있으며, 수집된 정보를 통한 다양한 서비스의 제공이 가능하도록 하기 위한 IT기반의 융합의 한분야로서 활발한 연구가 진행되고 있다[1,2].

최근 융합기술이 생활에 다양한 영향을 미치고 있으며, 융합기술을 주도하는 국가가 세계를 주도할 정도를 중요한 기술이다. 융합의 중심에는 정보통신 기술이 있으며, IT기반의 융합이 필요하다. IT기반의 융합발전에는 수많은 문제점이 존재하고 있으며, 그중에서도 가장 중요한 요소가 각 기계간의 통신이 안전성을 보장하는 보안이다.

2010년 현재 이코노미스트 연구소 정보화 지수에 따르면 세계자동차공업협회(OICA) 자동차 생산 53개국 중 5위로써 정보기술과 자동차 생산에 있어 세계적으로 우위에 서 있다. 이러한 세계적인 우위의 입장을 고수하면서 현재 IT 분야의 장점과 융합이 이뤄지면 놀라운 성장이 예상된다. 세계적으로 화두가 되고 있는 을 가지고 세계적으로 화두가 되는 M2M 기술발전에 따른 지능형 자동차 분야의 보안 위협요소를 분석하여 보안문제점을 제시하고 이에 따른 보안위협요소 해결을 위한 방안을 제안한다.

본 논문에서는 M2M에 대한 정의와 보안 위협요소를 살펴본다. 지능형 자동차 환경에서의 보안위협요소를 살펴보고, M2M 환경에서의 발생 가능한 보안 위협요소를 제시하고, 보안 위협을 해결 할 수 있는 방안을 제안한다.

Ⅱ. 관련연구

2.1 M2M 통신 네트워크

M2M(사물통신) 서비스는 주변의 사물이나 기기에 정보를 수집하고 통신을 가능하게 하는 장치를 설치한 후 이를 통하여 수집되거나 상호 공유되는 정보를 이용하여 사용자 혹은 사물 자체에게 정보를 제공하는 정보 서비스의 개념이다. 사물통신 네트워크를 위한 기술은 추상적인 개념이 아니며, 실제 이미 우리 주위에서 볼 수 있다. 예를 들어, 물류나 제조업 분야에서는 물품에 바코드나 RFID 를 부착하여 제품의 유통경로 및 부가 정보 획득을 가능하게 한다. M2M에서의 적용할 수 있는 주요기술은 다음과 같다.

- 식별기술 : 사물들을 외부로부터 질의에 대응하거나 외부로의 질의를 가능하게 하는 식별자가 필요하며, 전파를 이용하는 RFID 기술은 사물 통신 네트워크 기술의 핵심기술로서 고속도로 통행료 징수, 물류관

리 등 스포츠와 여가 활동에서 개인 보안까지 매우 다양한 분야에서 활용되고 있다.

- 정보수집기술 : 사물의 물리적인 상태 정보와 주변 환경 정보를 수집하기 위해 센서기술과 센서가 탑재된 장치간의 네트워킹 기술인 센서 네트워킹 기술은 매우 중요한 역할을 통해 사물 주변 환경의 변화에 적극적으로 대응 할 수 있다.

- 통신 네트워크 기술 : 사물간의 정보 전송을 위한 통신은 유선과 무선, 이동통신 등으로 구분할 수 있으며, 3G나 4G와 같은 이동통신기술을 사용하고, 네트워크에 접속하기 위해 접근하는 액세스 네트워크로 무선랜과 유선네트워크를 사용할 수 있다. 통신기술에서는 배터리 소모를 줄일 수 있는 저전력 및 소형 기기를 위한 무선 통신 기술이 필수적이다.

- 지능화 기술 : 사물에 내장된 정보처리 능력으로 원격 객체의 도움없이 자체적인 정보처리 능력과 외부 환경의 변화에 스스로 대응하는 기술이 필요하다.

- 소형화 기술 : 사물통신 서비스 환경에서는 사용되는 모든 기기 및 사물에 통신과 컴퓨팅 장치가 탑재되어야 하므로 소형화를 통한 탑재가 필요하며 비용에 대한 절감이 필수적인 기술요소이다.

이러한 필수 기술요소를 통해 사물통신 환경에서 정보의 수집과 활용이 사람과 사람의 관계에서 사람과 사물, 사물과 사물간의 관계로 변화되어 사물간의 정보교환과 제어를 통해 모든 기기와 시스템을 자율적으로 안전하게 관리해야 한다[3].

2.2 M2M에서 보안위협 요소

M2M 네트워크 서비스 환경에서 발생할 수 있는 문제점은 새로운 기술뿐만 아니라 기존 기술의 결합에 의한 컨버전스 서비스에서 가지고 있는 문제점과 보안 위협요소들이 그대로 나타날 수 있다. 사물통신 서비스에서는 기기나 기계간의 이동으로 인한 빈번한 형태 변화와 무선 채널을 사용하는 구조적인 취약점을 가지고 있다.

잦은 네트워크의 변화와 무선채널의 위험에 따른 정보 수집이 어려움과 안정적인 관리와 효율적인 해결방안이 요구된다. 사물통신에서도 기존 보안의 특성을 이용하여 보안 위협요소로부터 안전한 정보수집 등의 서비스를 제공해야한다. 보안에서 살펴보아야 할 특징은 가용성(Availability), 기밀성(Confidentiality), 무결성(Integrity), 인증(Authentication), 부인봉쇄(Non-repudiation)와 같은 요구들을 충분히 만족할 수 있는 보안 요소기술 개발이 필요하다.

M2M에서의 Device의 위협에는 기기간의 도청, 가로채기, 부인과 관련된 프라이버시 및 변조 위협요소가 있으며, Gateway에서는 불법 도용 및 접근을 통한 권한 위배, 물리적 침입, 재사용 공격, 중간자 공격의 위협요소가 존재한다. M2M 네트워크에서는 불법침투, 서비스 거부를 통한 마비, 바이러스, 웜, 트로이목마, 자원고갈 등의 보안 위협 요소가 있다[1].

III. 지능형 자동차의 보안위협 요소

3.1 지능형 자동차

지능형 자동차는 디지털 홈, 텔레매틱스, 지능형 로봇 등이 접목되어 네트워킹 및 인포테인먼트가 가능한 형태로 진화되고 있다. 특히 차량의 경우 IT와 컨버전스를 통해서 비즈니스 모델 뿐만 아니라 AM 시장을 확대하고 있다.

그림 1은 차량을 통한 다양한 서비스 시나리오에 관한 것이다[5]. C2E, C2C, C2H간의 다양한 서비스 모델을 제시하고 있다. 이중에서도 현재도 가능한 서비스도 있지만 아직 현실화되지 않은 서비스도 있다. 본 논문에서는 C2C를 기반으로 주변 교통정보, 환경정보 등의 다양한 정보를 수집하는 환경에 대한 보안 위협요소에 대해서 살펴보고자 한다.

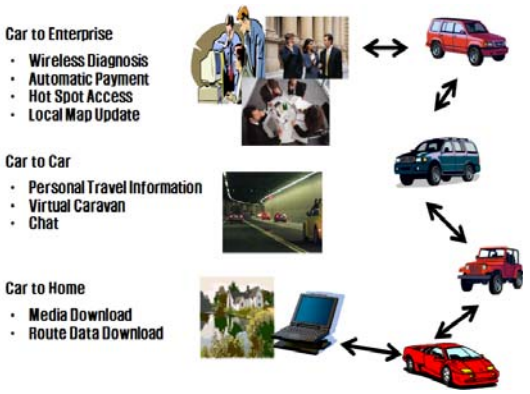

그림 1. 지능형 차량 유형
Fig. 1 Type of Intelligent Vehicle

3.2 지능형 자동차의 보안 취약성

지능형 자동차 서비스에서의 주요 역기능으로 개인정보 및 프라이버시 침해, 차량정보, 차량간 통신 메시지, 통신트래픽 정보 등의 위변조 등의 위협 요소로부터 안전한 메시지 전송이 필요하다. 안전한 차량 서비스 및 통신을 위한 지능형 자동차의 보안 프레임워크에는 Secure Positioning, Vehicle-to-Infrastructure Secure Communication, Vehicle-to-Vehicle Secure Communication, User Access Control, VPKI(Vechicular PKI) 등을 포함하고 있다.

일정 네트워크 영역내에서 다른 차량의 통신에 장애를 초래하는 신호를 발생시키는 Jamming (like DoS Attack)공격과 거짓 정보를 발생하는 공격 차량에 의해 일정 네트워크 영역 내의 다른 차량들을 거짓 정보로 오염시키는 Forgery 위협이 존재한다. 주행중에 메시지 또는 정보의 전달 과정에서 drop, corrupt, 또는 modify를 통한 정보의 위변조 공격하는 In-transit Traffic Tampering과 차량의 상태 정보를 변경하여 다른 차량으로 하여금 오인하도록 하는 공격하는 Impersonation 공격이 있다. 시간, 위치, 차량 ID, 이동정보 등의 차량과 관련된 개인 프라이버시 정보에 대한 침해하는 Privacy Violation과 차량 내부의 정보(속도, 위치, 차량 전장 부분의 상태, 각종 센싱 정보 등)에 대한 위변조 공격하는 On-board Tampering이 위협요소이다[4,5].

3.3 지능형 자동차의 고려사항 및 제약사항

지능형 차량은 고속(약 시속 180km 이하) 이동 환경에 의한 제약사항을 고려하여야 한다. 차량 네트워크(VANET)는 고속 주행으로 인하여 빠르게 토폴로지가 변화되는 네트워크 휘발성을 내재한 Network Volatility와 차량 정보를 이용한 사고 처리 등에서 책임 및 법적 자료 제공에 따른 개인 정보 침해 가능성이 존재하는 Liability vs. Privacy가 있다.

VANET의 특성상 실시간성으로 정보 처리가 이루어져야 하는 Delay-sensitive Applications과 전 세계에는 수십억 대의 차량이 존재하며 이들간의 안전한 관리 및 키 분배 등에 제한이 따르는 Network Scale이 있다. 또한 서로 다른 국가, 제조 업체, 서비스 업체에 따라서 차량을 이용한 서비스의 이질성이 존재하는 Heterogeneity가 있다[4].

IV. 지능형 자동차의 보안 요구사항

지능형 자동차의 서비스 구성요소는 그림 2와 같이 교통정보 서비스, 생활정보 서비스, 안전 서비스, 원격 고객 관리, 엔터테인먼트, 보안 서비스로 구성이 이뤄진다. 이러한 서비스는 실시간 제어 네트워크를 통해 차량제어 시스템을 기반으로 구동하게 되어 있다.

이러한 지능형 자동차의 안전성을 보장하기 위해서는 Security Hardware, VPKI, Authentication, Certificate Revocation, Privacy의 보안 프레임워크 구성이 필요하다. 차량 통신 보안을 위한 하드웨어로는 ELP(전자번호판), EDR(차량용블랙박스), TPD(차량용 TPM, Advanced EDR), 정보수집을 위한 센서 등이 필요하다. 차량간의 안전한 통신을 보장하기 위한 인프

라를 위해 PKI 기반의 인증 인프라의 구축도 이뤄져야 한다. 각 자동차마다의 정당한 사용자 인증과 보안 처리에 의한 오버헤드를 줄이기 위한 암호화 알고리즘을 사용하고, 빠른 인증 처리를 위한 인증기술이 있어야 한다. 인증 인프라에서 생성된 키 관리나 폐기 및 갱신은 매우 중요하므로 효율적인 키 관리, 폐기, 갱신을 위한 연구가 중요하다. 차량간의 통신을 통해서 다양한 정보(시간, 위치, 차량 ID, 주변 정보 등) 실시간으로 개인정보 및 차량 정보가 노출되므로 개인정보 및 프라이버시 침해 대응기술이 연구되어져야 한다.

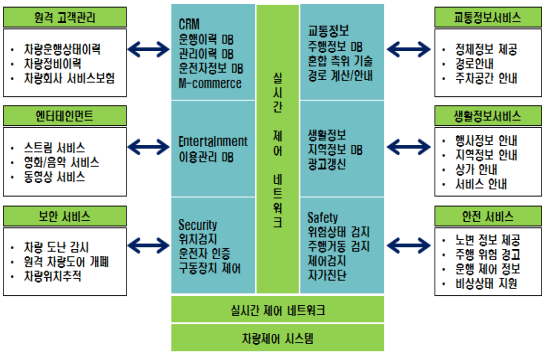

그림 2. 지능형 차량 서비스 구성
Fig. 2 Service Configuration of Intelligent Vehicle

지능형 자동차에서 안전한 보안을 제공하기 위한 보안 고려사항을 임베디드 시스템, 포렌식, 키관리, Threshold 기법에 대해서 제안한다.

4.1 임베디드 시스템 보안

M2M환경 발전에 따라 운전자가 직접 운전을 하지 않고 인공지능과 임베디드 시스템을 통한 자동주행 기법이 연구되어 발전되어 지고, 실제로 많은 연구 개발이 이뤄지고 있다. 자동주행은 차량간에 서로 차량의 위치와 주변 정보 등을 감지하고 실시간 교통정보와 주변 위기 상황에 대한 운전자가 신경 써야 할 것들을 자동차가 알아서 자동적으로 작동하도록 프로그래밍 된다. 그러므로 임베디드 시스템 소프트웨어에 대한 보안이 뒤바침이 되지 않는다면 사고의 위험에 더욱더 증가할 것이다. 또한 자동차는 운전자의 등록된 개인정보를 통해 탑승자의 개인일정과 건강상태 등 탑승자에게 필요한 정보를 제공할 것이다. 차량 절도 등의 분실이 발생하던지, 통신을 통한 해킹을 통해 개인정보와 차량에 관한 정보를 쉽게 노출이 된다면 심각한 문제가 야기 될 것이다.

이에 따른 주행보조 시스템 및 텔레매틱스 보안, 자동차 통신 보안, ID 보호 등의 프라이버시 보호기술, EDR(Event Data Recorder)을 위한 소프트웨어 배포 기술, 도난절도 방지기술, GPS를 이용한 자동차 보험 등의 자동차 내부 IT 시스템보안을 통해서 좀더 운전자의 개인정보보호가 필요하다.

4.2 포렌식 보안

현재 전 세계적으로 수십 개의 ECU(Electronic Control Unit)가 장착된 컴퓨터 장치들의 정교한 집합체로 지능화 되는 방향으로 빠르게 진화해 나가고 있다. 자동차 한대에 내장되는 ECU의 개수가 수십 개로 늘어나고 이것들이 각각 신속한 처리를 하기 때문에 ECU에 대한 효과적인 보안은 더욱 어려워지고 있다.

교통사고 발생 시 유리한 증거확보를 위한 조작, 보험사기를 위한 데이터 조작, 운행 정보조작 등, 다양한 법률에 위배되는 행위가 많이 이뤄 질 것이다. 현재 주행거리 조작은 현재에도 많이 이루어지고 있다. 보안 연구 개발을 통해 무결성이 확보되고 결정적 ECU데이터를 통해서 EDR에 기록된 내용이 법적 증거 능력을 갖추기에 충분하다.

포렌식 기법을 통해 범죄의 사전 예방 및 범죄의 법적 증거 자료로서 개인의 정보보호를 보존할 수 있는 기법의 제공이 필요하다. 지능형 자동차로 발전을 통해 자동차가 하나의 안전한 공간과 컴퓨팅을 위한 공간, 주변 정보를 수집 배부하는 서버로서의 역할을 수행하므로서 외부로부터의 네트워크를 통한 침입에 대

한 흔적과 사전 탐지 기능을 통해 안전성을 보장해 주어야 한다.

4.3 사용자 및 차량 인증

차량의 정당한 소유자로서의 인증을 위한 생체인식 정보나 스마트키 인증등을 통한 사용자 인증이 필요하다. 또한 자신의 신원을 밝히고 인증을 받는 일반적인 인증과 달리 자동차간에 주고받는 정보의 안전한 메시지의 인증은 프라이버시 보호를 위해 운전자의 신원을 드러내지 않으면서 메시지를 인증하며 신뢰성 있게 통신하기 위해서는 복잡하고 까다로운 요구조건을 만족시켜야 하는 어려움이 있어 이에 대한 효율성을 높일 수 있는 연구개발이 필요하다.

보안 요소가 첨가된 새로운 인증 모듈을 통해 모바일이나 PC에서도 자동차 정보 상태를 볼 수 있도록 하고 앞으로는 자동차 자체도 컴퓨팅 시스템으로 이용되어 자동차를 제어 할 수 있기 위해 개인정보 유출을 방지하는 안전한 인증 모듈이 필요하다.

4.4 키 관리

공개키 암호기법의 우수성을 이용하여 라우팅 정보와 데이터 트래픽에 대한 정보를 보호해야 한다. 지능형 자동차간에 그룹을 만들 수 있는 Cluster 기반으로 구성하여 Cluster 키를 통한 모든 클러스터 내에 위치한 자동차에 대해 유일하게 존재하고 클러스터에 속하는 모든 이동 자동차에게 분배한다. 이 키는 Cluster 내에 각 자동차들을 인증해주는 Cluster Head(CH)에 의해 생성되어 시스템 공개키로 암호화되고 클러스터 멤버에게 분배된다. 각 이동 자동차는 공개/개인키 쌍을 가지고 있으며, 키 관리를 위한 CA(Certification Authority)를 두어 키의 바인딩과 주기적인 갱신을 담당하도록 한다.

CA는 공개/비밀 키 쌍을 가지고 있으며, 공개키는 다른 모든 자동차에게 분배되고, 비밀키를 가지고 인증서를 서명 분배한다. 어떤 한 이동 자동차가 더 이상 신뢰할 수 없거나 네트워크 영역을 벗어나게 되면 그 자동차의 공개키는 폐지한다.

4.5 Threshold 암호화 기법

지능형 자동차에서 CA는 전체 네트워크에 대한 보안을 책임지는 개체로서 외부 적의 집중적인 공격의 대상이 된다. 만일 하나의 CA를 사용하고자 한다면 집중된 외부 공격으로 인하여 CA가 정상적인 역할을 수행하지 못하거나 혹은 적에게 변질되어 악용될 경우 상당히 심각한 문제가 발생한다. CA를 이용한 서비스가 사용 가능하지 못하다면, 이동 자동차들은 다른 이동 자동차들의 현재 공개 키를 획득할 수 없고, 다른 이동 자동차들과의 안전한 교신이 불가능하게 된다. 만일 CA가 공격자에 의해 변질되어 비밀 키를 공격자에게 누설 한다면 공격자는 그 비밀 키를 이용하여 비밀키로 거짓된 인증서를 발행할 수 있게 된다. 이러한 문제점을 해결하기 위하여 Threshold 기법을 이용하여 시스템 키 관리 서비스의 책임을 각 CH 에게 분할해서 분배하고, (n, t+1) Threshold Cryptography를 이용하여 2-tier 계층 구조의 중요한 요소인 각 CH의 신뢰 여부를 확인하며, CH가 변질된 경우 하위 계층에 속한 이동 자동차 중 새로운 CH 역할을 수행할 자동차를 신속하게 재생성하여 네트워크를 구성해야 한다. Threshold를 적용할 수 있는 방법에 대한 적용기법의 연구가 필요하다.

Ⅴ. 결 론

자동차 발전과 융합 발전에 따른 보안 문제를 연구개발해 보안문제를 해결하기 위한 연구개발이 절실히 요구되어지고 있다. 본 논문에서는 M2M에서의 보안 위협요소를 분석해보고 그에 따른 지능형 자동차 분야에서의 보안 위협요소를 분석하였다. 이러한 지능형 자동차의 안전성을 보장하고 위한 방법으로 임베디드 시

스템보안, 포렌식, 사용자 및 차량인증, 키관리, Threshold 기법의 적용방법에 대해서 요구사항을 제안하였다. 이러한 제안을 통해 자동차 IT 시스템 보안기술에 대한 원천기술을 확보하기 위한 연구의 기초 토대가 될 것이다.

참고문헌

[1] 이근호, "M2M(Machine to Machine)통신에서의 보안 위협 분석", *한국산학기술학회 2010년도 춘계학술발표논문집*, 제11권, 제1호, pp. 416-419, 2010년, 5월.

[2] 윤필하, 이소희, 최호식, 이근호, 김수균, "M2M 발전에 따른 자동차보안 문제와 연구의 필요성", *한국지식정보기술학회 2010년도 추계학술발표대회 논문집*, 제5권,제2호, pp. 41-43, 2010년, 11월.

[3] 김형준, "사물간 통신 네트워크의 이해", *한국통신학회지*, 제27권 제7호, pp. 21~28, 2010년, 6월.

[4] 최병철, 한승완, 정병호, 김정녀, "지능형 차량 보안 기술 동향", 전자통신동향분석 제22권 제1호, pp.114-118, 2007년, 2월.

[5] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "*Securing Vehicular Communications*," In Magazine of IEEE Wireless Communications - IVC Specials, EPFL, pp.8-15, Oct. 2006.

[6] Dong-Hoon Kim, Jun-Yeob Song and Seuk-Keun Cha, "I*ntroduction of Case Study for M2M Intelligent Machine Tools*", Proceedings of 2009 IEEE International Symposium on Assembly and Manufacturing, pp. 17-20, November, 2009.

[7] Inhyok Cha, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, and Michael Victor (Mike) Meyerstein, "*Trust in M2M Communication*", IEEE VEHICULAR TECHNOLOGY MAGAZINE, pp. 69-75, SEPTEMBER, 2009 .

[8] Maxim Raya and Jean-Pierre Hubaux, "*Securing Vehicular ad hoc networks*," Journal of Computer Security 15 pecials, EPFL, pp.8-15, Oct. 2006.

김기원(Gi-Weon Kim)

1987년 한남대학교 전자계산학과(이학사)
1989년 숭실대학교 컴퓨터공학과(공학석사)
2001년 한남대학교 컴퓨터공학과(공학박사)

1996년~현재 초당대학교 컴퓨터과학과 교수
※ 관심분야 : 멀티미디어, 실시간 영상처리, 음성인식

김수균(Soo-Kyun Kim)

2006년 고려대학교 컴퓨터학과 (이학박사)
2006.3 ~2008.2 삼성전자 통신연구소 책임연구원

2008년~현재 배재대학교 게임공학과 조교수
※ 관심분야 : 기하모델링, 게임그래픽, 실감미디어

이근호(Keun-Ho Lee)

2006년 고려대학교 컴퓨터학과(이학박사)
2006년~2010년 (주)삼성전자 DMC연구소
2010년~현재 백석대학교 콤인성개발원 팀장

2010년~현재 백석대학교 정보통신학부 전임강사
※ 관심분야 : M2M 보안, 이동통신보안, 융합 보안, 개인정보보호