情 報 保 護 學 會 誌
第19卷 第1號, 2009. 2

VANET에서의 보안 기술동향

조 영 준*, 이 현 승*, 박 남 제**, 최 두 호**, 원 동 호*, 김 승 주*

요 약

VANET(Vehicular Ad-hoc Network)은 MANET(Mobile Ad-hoc Network)의 한 형태로, 다수의 차량들이 무선통신을 이용하여 차량 간 통신 또는 차량과 노변장치(Roadside Equipment) 간의 통신을 제공하는 차세대 네트워킹 기술이다. VANET은 주로 사고를 예방하기 위해 사용된다. VANET은 사람의 안전과 생명을 보호 하는 중요한 역할을 하기 때문에 보안을 반드시 고려해야 한다. 본 고에서는 VANET에서의 보안과 관련된 고려사항 및 제약사항과 위협을 서술하고 VANET이 만족해야 할 보안요구사항에 대해 분석한다.

Ⅰ. 서 론

최근 들어 차량에 IT 기술을 접목시키려는 노력이 가속화되고 있다. 현재까지는 휴대 단말기에 국한되었던 다양한 서비스들이 향후에는 차량의 지능화에 의해서 실현될 것으로 전망된다. 이러한 서비스는 C2E(Car to Enterprise), C2C(Car to Car), C2H(Car to Home)에서 이루어지며 그 종류는 매우 다양하다. 이러한 지능형 차량 서비스가 가능하기 위해서는 인프라 확충이 필수적이다. 그 중에서도 차량 통신에 관한 연구가 매우 중요하다.

VANET(Vehicular Ad-hoc Network)은 차량과 차량 사이 또는 차량과 RSU(Road Side Uint) 사이의 통신을 위한 네트워크이다. 이러한 VANET은 교통안전 정보를 제공해주는 V2V(Vehicular to Vehicular) 환경과, 차량 내의 단말기 또는 사용자 휴대용 단말기 등을 사용하여 인터넷 서비스를 이용할 수 있는 V2I(Vehicular to Infrastructure) 통신 구조로 구분된다. V2V 환경은 이동 애드 혹(Mobile Ad hoc) 네트워크 구조이고, V2I는 RSU를 거쳐 기존 인프라 구조에 액세스 할 수 있는 구조이다.

VANET에서는 운전자의 생명을 보호하기위해 교통사고 발생, 갑작스런 기상 변화, 노면 결빙 상태 등의 정보를 뒤따르는 차량들에게 안전하고 신뢰성 있게 전달해주어야 할 필요가 있다. 또한, 최근 사용자의 멀티미디어 서비스에 대한 수요가 증가하면서 차량 내에 장착된 단말기 또는 사용자의 노트북, PDA와 같은 단말기들을 사용하여 이동 중에도 멀티미디어 서비스를 받고자 하는 경향 또한 증가하고 있다. 따라서 이러한 서비스에 의한 역기능, 즉 개인정보 및 프라이버시 침해, 차량 정보/통신 메시지/트래픽 정보 등의 위변조 위협 등을 해결할 필요가 있다.

본 고의 2장에서는 VANET과 MANET (Mobile Ad Hoc Network)에 대해 알아보고 VANET의 구성에 대해 서술한다. 3장에서는 VANET의 프로젝트 동향에 대해 알아보고 보안 관련 연구의 진행 상황을 서술한다. 4장에서는 VANET에서 있을 수 있는 보안문제, 즉 취약점과 가능한 공격에 대해 알아본 뒤, 5장에서 보안문제를 해결하기 위한 보안요구사항에 대해 알아본다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. VANET

2.1 VANET과 MANET

MANET은 특정한 네트워크 인프라가 없는 환경에

본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업[2005-S-088-04, 안전한 RFID/USN을 위한 정보보호 기술]의 일환으로 수행되었습니다.

* 성균관대학교 정보통신공학부 정보보호연구소 ({yjcho, hsrhee, dhwon, skim}@security.re.kr)
** 한국전자통신연구원 ({namjepark, dhchoi}@etri.re.kr)

[표 1] MANET과 VANET의 비교

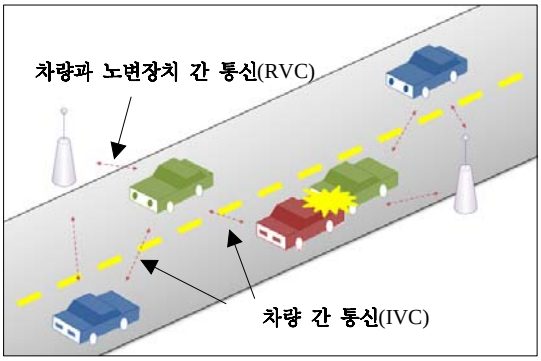
구분	MANET	VANET
이동성	중/저속 (보행속도)	고속 (최대 200Km/h)
노드 생산 단가	저가	고가
네트워크 토폴로지 변화	느림	빠름
노드의 밀도	낮고 변화가 느림	높고 변화가 빠름
노드의 전송범위	100m 내외	400m 내외
노드의 전송 대역폭	협대역 (저속데이터)	비교적 광대역 (고속데이터)
전력자원	저용량의 제한된 전원사용	고용량의 전원사용 (지속적으로 재충전)
노드의 생명 주기	전력 공급원의 성능에 의존	차량의 상태에 의존
컴퓨팅 능력	8~16bit 저속	32bit 이상의 고속
어드레싱 기법	속성기반 어드레싱 기법 (Attributed-based addressing)	위치기반 어드레싱 기법 (location-based addressing)
메시지의 전송과 내용에 대한 신뢰성 요구도	중간 (어플리케이션에 의존)	매우 높음 (주로 안전과 관련된 메시지)
노드의 위치 획득 방법	라디오 신호 강도(RSSI) 및 초음파를 이용한 삼각측량기법	GPS
노드의 이동 패턴 (속도 및 방향)	임의 위치로 이동 (random)	도로를 따라 정해진 이동경로를 가짐 (이동 방향 및 속도가 서로 연관되어지며, 예측 가능함)

서 무선 인터페이스를 가진 다수의 노드들에 의해 자율적으로 구성되는 네트워크이다. VANET은 MANET의 한 형태로, 다수의 차량들이 무선통신을 이용하여 차량 간 통신 또는 차량과 RSU 간의 통신을 제공하는 차세대 네트워킹 기술이다. 각각의 차량은 애드혹 네트워크(Ad-Hoc Network)의 노드 역할을 하게 되고 인프라스트럭처(Infrastructure)나 서버 없이 차량 간 통신이 가능하다.

VANET은 노드의 이동성과 자가 네트워크 구성 측면에서 MANET과 동일하다. 하지만 근본적으로 다음과 같은 차이점이 있다. VANET을 구성하는 차량들(이하 노드)은 MANET에 비해 고속의 이동성을 가지며 노드밀도와 네트워크 토폴로지의 잦은 변화 등의 특징들을 가진다. 이러한 특징들로 인해 빈번한 네트워크 단절과 메시지 전파 지연 그리고 제한된 대역폭에 의한 메시지 중복의 제한과 짧은 연결 생존시간 등의 문제점을 가진다. MANET의 네트워크 프로토콜들은 이러한 특징들을 고려하지 않고 있기 때문에 VANET을 위한 새로운 네트워크 프로토콜이 요구된다. MANET과 VANET의 차이점을 정리하면 [표 1]과 같다[1].

2.2 VANET의 구성

VANET은 크게 차량(Vehicle)과 RSU로 구성된다. 차량은 VANET에서 노드 역할을 하며 통신의 주체가 되며 개인용 차량과 공공 차량(버스, 경찰차 등)으로 구분된다. RSU는 Base station으로 불리기도 하며, 주로 서버와 차량 간의 통신을 중개하는 역할을 하고 기업 또는 정부 소유로 구분할 수 있다[2].



[그림 1] VANET 시스템 모델

VANET의 통신 방법에는 차량 간 통신(V2V)과 차량과 노변장치 간 통신(V2I)이 있다. 차량 간 통신 IVC (Inter-Vehicle Communication)로, 차량과 노변장치 간 통신은 RVC(Roadside-to-Vehicle Communication)로도 불린다[3]. 차량 간 통신은 차량 간 1:1 통신, 방송(Broadcasting), 멀티홉 라우팅 기능을 제공하여 이동중이거나 정지중인 차량들 간의 신호 또는 데이터를 송수신하는 무선통신을 말한다[4]. 차량 간 통신은 기간망의 통신 범위를 확대할 수 있을 뿐만 아니라 기지국의 경유 없이 신속한 정보의 전파를 가능하게 함으로써 통신 장비의 설치비용 감소 및 네트워크의 통신용량 증가에 기여할 수 있다[5].

차량 간 통신기술은 주로 사고를 예방하기 위하여 사용되거나 사고의 연속 발생을 막기 위하여 사용되는데 특히 전방 사고위험 경보나 교차로 충돌 방지 등에서 활용되거나 시험되고 있다. 최근에는 센서 정보를 이용하여 차량의 위치나 상태정보를 차량 간 통신에 활용하는 사례도 검토되고 있다[6].

차량과 노변장치 간 통신은 WAVE 규격을 근간으로 다수의 차량과 기지국간 10Mbps급 고속의 양방향 통신을 지원함으로써 차량이 이웃한 기지국을 통과할 때 패킷 서비스를 중단 없이 받을 수 있는 통신기술이다[4]. 이러한 차량과 노변장치 간 통신 기술은 차량에 인포테인먼트(Infortainment) 서비스, 교통정보 수집 및 분배 등의 통합 서비스를 제공하는 통신기술로서 텔레매틱스 서비스와 ITS 서비스에도 활용이 가능하다.

이러한 VANET의 목표는 운전자에게 안전과 편의를 제공하는 것이다. VANET 장치가 설치된 차량은 주변의 교통사고 상황이나 교통 흐름 등의 정보를 실시간으로 제공받는다. 또한 차량 내에서 인터넷에 접속할 수도 있으며, 주차를 하거나 톨게이트 통과 시 자동 과금 서비스를 이용할 수 있다.

Ⅲ. VANET 프로젝트 동향

본 장에서는 VANET의 연구 동향을 살펴본다. VANET은 차량의 안전한 운행과 편리한 통신 서비스 제공을 목표로 유럽, 미국 등에서 다음과 같은 다양한 프로젝트가 진행되고 있다.

• FleetNet

차량 간 통신에서 센서 데이터의 교환으로 동작하는 운전자 보조 어플리케이션의 개발을 목적으로 하고 있는 프로젝트이다. 사고를 방지하기 위해 도로 상의 정지 차량의 존재를 경보하거나 사용자 간 통신이 가능한 어플리케이션을 제공한다[11].

• C2C-CC
(Car 2 Car Communication Consortium)

무선랜을 기반으로 한 차량 간 통신 시스템을 표준화하기 위해 결성된 프로젝트이다. 능동적 안전 어플리케이션(Active safety application)의 프로토타입 개발과 C2C 시스템구현을 위한 주파수 할당을 목표로 연구가 진행 중이다. 이 프로젝트는 IEEE 802.11 a/b/g/p PHY/MAC 기반으로 한 통신 기술을 이용한다[12].

• Willwarn

PreVENT(유럽의 도로안전 연구 프로젝트)의 하부 프로젝트이다. 802.11 a/p를 기반으로 연구한다. 잠재적인 위험상황을 운전자에게 미리 경고함으로써 사고를 방지할 수 있는 서비스를 연구하고 있다[13].

• VII(Vehicle Infrastructure Integration)

도로상의 교통 인프라와 차량 간의 통신 체계를 통합할 수 있는 통신 기술을 개발하는 것이 목적인 프로젝트이다. 교통량에 따라 교통 신호 등을 최적화하여 이용할 수 있게 되어 교통 정체 해소 및 운전자의 안전을 확보할 수 있도록 한다[4].

• CVIS
(Cooperative Vehicle-Infrastructure System)

무선 통신을 이용하여 실시간으로 교통 정보와 차량 정보를 수집하여 위치를 기반으로 한 정보를 제공한다. CALM, 802.11p, 등의 통신 기술을 기반으로 도시에 대해서는 차량정보 수집 및 교통관리와 유동적인 버스 차선을 관리하는 서비스를 연구하며 고속도로 및 외부 도로에 대해서는 여행 정보를 제공하고 위험 경고 신호 전송에 대한 연구를 하고 있다. 또한 화물 및 주차 시 위험 화물에 대한 정보를 관리하고 주차 정보를 알리는 연구를 하고 있다[14].

• Cartalk 2000

차량 간 통신을 통해 운전자에게 운행안전 정보 및 필요 정보를 제공하는 것을 목표로 하는 프로젝트이다. 통신 기술로는 UMTS, GPS를 이용하며 센서를 이용한 차량 주행 안전 시스템을 제공하고 차량 간 통신을 통해 주행 안전정보를 제공한다[15].

• Safespot

European Commission Information Society Technologies의 여섯 번째 프레임워크 프로그램 중 하나인 협력 프로젝트이다. 802.11p, CALM(Communications, Air-interface, Long and Medium range) 등을 기반 통신 기술로 이용하며 지능형 차량의 장점과 지능형 도로의 장점을 통합하여 안전을 증대시키는 것을 목표로 한다[16].

• Watch-Over

European Commission Information Society Technologies의 협력 프로젝트이다. 도로상 보행자의 사고를 줄이기 위해 연구를 진행하고 있다. 802.15.4, RFID, UWB(Ultra Wide Band Radio) 통신 기술을 기반으로 연구한다[17].

프로젝트의 대부분이 사고 예방을 위한 위험 분석 및 알림에 대한 연구로, 주변 정보의 수집과 위험 상황 인지, 위험 정보 알림 방법 등이 연구되고 있다. 국내의 한국전자통신연구원(ETRI)에서도 VMC(Vehicle Multi-hop Communication) 기술 개발로 VANET의 연구가 진행되고 있다. VMC 기술 개발에서는 주로 차량 안전 관련 메시지의 송수신에 대한 연구가 진행되고 있으며 V2V 무선링크 시뮬레이터 연구와 VMC 기반 기술 연구가 진행되고 있다[6].

VANET의 일반적인 연구와 달리 VANET에서의 보안 연구는 활발하지 않다. 진행되었거나 진행 중인 보안 관련 연구는 다음과 같다.

• NOW (Network On Wheels)

2004년 6월부터 2008년 5월까지 진행된 프로젝트로 독일의 BMBF(Federal Ministry of Education and Research)에서 진행되었다. 무선랜 기술을 기초로 한 차량 간 통신시스템 개발을 목적으로 하며 차량 간 통신프로토콜, 보안이슈 및 자동차간 통신시스템용 부품 개발을 목표로 하고 있다. 통신 기술은 IEEE 802.11a,b와 IPV6을 기반으로 이용하고 있다. 도로상태 및 교통정보를 수집하여 차량에 제공한다[18].

• SEVECOM

(SEcure VEhicular COMmunication)

2006년 2월부터 현재 진행 중인 프로젝트로 프랑스의 EPFL에서 진행 중이다. 차량 간 통신을 이용한 서비스들의 보안을 향상시키는데 목적이 있다. 채널, 데이터, Telematics Control Unit으로의 공격을 방지하기 위한 인증 연구 및 아키텍처와 보안메커니즘의 명세를 위한 연구를 진행하고 있다[19].

Ⅳ. VANET에서의 보안 문제

VANET은 앞으로 자동차와 운전자, 그리고 외부 환경과의 정보 교환을 통해서 사람의 안전과 생명을 보호하는데 중요한 역할을 할 것이다. 하지만 이를 위해서 고려해야 할 여러 가지 사항이 있다. 그 중 하나가 보안이다. VANET에서의 보안은 매우 중요한 이슈이다. 다른 네트워크와는 달리 VANET 보안은 사람의 생명과 직접적으로 연결되어 있기 때문이다. VANET은 운전자의 안전과 편의를 제공한다는 목표를 가지고 있지만, 운전자에게 정보가 제대로 전달되지 않는다면 오히려 치명적인 사고를 불러올 수 있다. 네트워크 내부 또는 외부에서 악의적인 공격자가 정보를 도청 및 변조하여 차량 사고를 일으키거나, 네트워크 전체를 마비시켜 혼란을 야기할 수도 있다. 또한 다른 네트워크와는 달리 차량 속도의 가변성, 예측하기 어려운 차량의 움직임, 동시 다발적으로 일어나는 연결성 등의 특징을 지니고 있다[7]. 따라서 이를 고려하여 적절한 VANET 보안의 연구가 필요하지만 3장에서 서술된 바와 같이 연구가 활발하지 않다.

이 장에서는 VANET의 보안연구를 위해 VANET에서 발생할 수 있는 보안 문제에 대해 서술한다. VANET의 위협을 분석하기에 앞서 VANET이 다른 네트워크와 다른 고려사항 및 제약사항에 대해서 알아보겠다. 대략적인 고려사항 및 제약사항은 [표 2]와 같다[8]. 고려사항 및 제약사항은 대표적으로 차량의 고속 주행으로 인한 네트워크 휘발성과 생명과 밀접한 정보의

[표 2] VANET의 고려사항 및 제약사항

고려사항 및 제약사항	내용
네트워크 휘발성 (Network Volatility)	VANET은 차량의 고속 주행으로 인하여 토폴로지가 빠르게 변화되는 네트워크 휘발성을 내재하고 있음.
책임(Liability) vs 개인정보보호 (Privacy)	차량정보를 이용한 사고 처리 등에서 책임 및 법적 자료제공에 따른 개인정보 침해 가능성이 존재함.
지연에 민감한 어플리케이션 (Delay-sensitive Applications)	VANET이 사고 경보와 같이 생명과 밀접하므로 실시간으로 정보처리가 이루어져야 함.
네트워크 규모 (Network Scale)	차량의 수에 따라 네트워크 규모가 결정되어 그 규모가 막대함. 이들 간의 안전한 관리 및 키 분배 등에 제한이 따름.
이질성 (Heterogeneity)	서로 다른 국가, 제조업체, 서비스 업체에 따라 다른 차량 서비스를 제공하므로 차량을 이용한 서비스의 이질성 존재함.

사용으로 인한 지연의 민감성 등의 특징을 가지고 있다. 이러한 고려사항 및 제약사항에 따라 VANET 환경에서는 많은 위협이 존재한다. VANET에서는 위협을 가하는 공격자를 [표 3]와 같이 소속, 동기, 방식 크게 3가지 사항으로 나눌 수 있다[2].

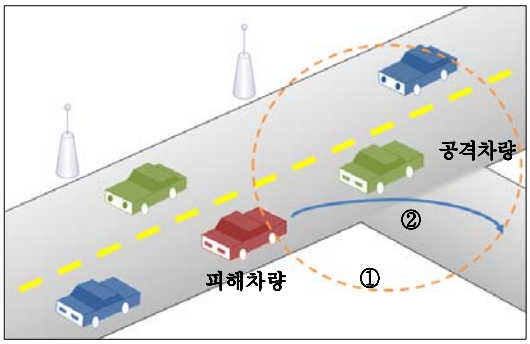
[표 3] VANET에서의 공격자 유형

구분		내용
소속	내부 (Insider)	네트워크 안의 인가된 멤버로서 다른 멤버와 통신을 할 수 있음. 즉 네트워크의 인증된 공개키를 보유
	외부 (Outsider)	네트워크의 멤버가 아닌 공격자. 침입자로 간주
동기	악의적 (Malicious)	개인적인 이득을 추구하지 않고 네트워크의 멤버에게 해를 끼치거나 네트워크 기능을 훼손시키는 것을 목적으로 함.
	합리적 (Rational)	개인적인 이익을 추구. 따라서 공격 수단이나 목표를 예측하기 쉬움
방식	능동적 (Active)	패킷이나 시그널 등을 생성
	수동적 (Passive)	무선 채널을 도청

본 고에서는 자동차 자체의 물리적 보안 문제는 범주를 벗어나므로 VANET에서의 메시지, 시스템 등과 관련된 보안 위협에 대해서 분석하였다. 관련된 위협은 아래와 같다.

• **보거스 정보**(Bogus information)

잘못된 정보를 네트워크에 확산시켜 다른 운전자의 행동에 영향을 미치는 공격을 말한다. [그림 2]와 같이



[그림 2] 보거스 정보(Bogus information)

공격차량이 주변 피해차량에 교통 상황의 허위 정보를 전송하면 피해차량은 그 정보에 따라 공격자가 의도한 경로로 이동을 하게 된다.

• **위치 정보 속이기**
(Cheating with positioning information)

차량의 알려진 위치나 속도, 방향의 변경을 유도하기 위한 공격으로 사고 등의 경우에 책임을 회피하기 위해 사용한다.

• ID **노출**(ID disclosure)

위치 추적을 위해 다른 차량의 ID가 노출되는데, Big Brother 논리(권력 남용)에 따라 관찰자가 목표한 차량의 이동경로를 감시하고, 다른 목적을 위해 그 정보를 사용할 수 있다. 수동적 공격자는 물리적인 도구가 아닌 VANET 시스템을 통하여 목표물의 신원을 밝혀내는 것이 가능하며 ID외에도 시간, 위치, 이동 정보 등의 개인 정보가 노출될 수 있다.

• **서비스 거부**(Denial of Service, DoS)

VANET에서의 통신 상태를 마비시켜서 혼란을 일으키거나 사고 발생을 목적으로 한다. 전파방해공격(jamming)은 DoS 공격의 일종으로 VANET의 특정 네트워크 영역 내에서 다른 차량의 통신에 신호를 발생시켜 네트워크 통신을 마비시킨다.

• **위장**(Masquerade, Impersonation)

공격자가 인가된 차량의 신원을 사용하여 주변 차량을 혼란시킨다.

• **위조**(Forgery)

공격자가 거짓 정보를 발생시켜서 일정 네트워크 영역 내의 다른 차량들을 혼란시킨다. 빙판길 경보와 같은 주의 정보를 허위로 유포하여 전체 트래픽의 흐름을 느리게 만드는 경우가 이에 해당한다.

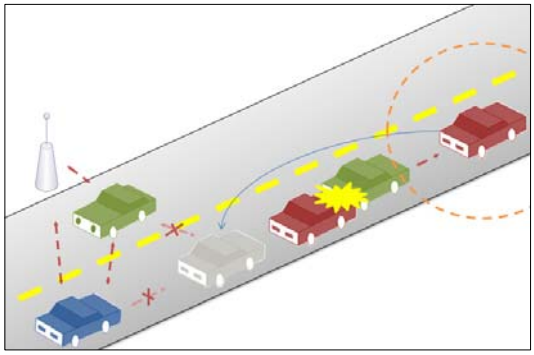
• **트래픽 위변조**(In-transit traffic tampering)

차량의 주행 중에 메시지 전송 과정에서 메시지의 삭제 또는 변경을 통해 정상적인 통신을 방해하는 공격이다.

• **차량 정보 위변조**(On-board tampering)

차량 내부의 정보(속도, 위치, 각종 센싱 정보 등)에

대한 위변조 공격이다. 이를 통해 속도, 위치 등의 정보가 부정확한 정보로 제공된다. 위조 공격과 마찬가지로 정보를 위조하지만 이 공격은 전송되는 정보가 아닌 센서나 다른 내부 장치를 통해 차량 내부의 정보를 변경함으로써 해당 차량에 사고나 오작동을 유발한다.



[그림 3] 정보 차단(hidden vehicle)

• **정보 차단**(Hidden vehicle)

VANET에서 사용되는 프로토콜의 특징을 이용한 공격이다. 프로토콜에서 정보를 전달할 차량은 정보 전송이 유리한 이웃 차량에 전송을 하게 되면 정보 전송을 중단한다. 이를 이용하여 공격자가 전송을 하고 있는 차량에게 자신이 전송이 유리한 위치의 차량으로 속여서 피해차량이 정보 전송을 중단하게 하고 다른 차량에 전달되어야 하는 정보를 전송하지 않아서 혼란을 일으키거나 사고를 유발한다.

• **터널**(Tunnel)

터널과 같은 GPS 정보를 일시적으로 받지 못하는 곳에 진입했다가 빠져나오는 차량에 허위 정보를 보내어 잘못된 정보로 업데이트 되도록 한다.

• **웜홀**(Wormhole)

일종의 교란 공격으로, 인증된 정보이지만 무의미한 정보를 전송하여 네트워크를 교란시킨다.

• **정글 통신**(Bush telegraph)

보거스 정보 공격의 확장으로 각 차량에 정보가 전달되면서 정보가 계속 변경되도록 하여 처음의 정보와 크게 다른 정보로 변경시킨다.

Ⅴ. VANET에서의 보안요구사항

앞 장에서 서술한 VANET에서 발생할 수 있는 보안 문제를 해결하기 위해서는 다음의 보안요구사항을 만족해야 한다[9,10].

• **메시지 인증 및 무결성**
(Message Authentication and Integrity)

메시지는 인가되지 않은 어떠한 변경으로부터든지 보호되어야 하며 수신자가 메시지의 송신자가 정당한 정보 제공자임을 확신할 수 있어야 한다. 여기서의 무결성은 메시지에 대한 비인가된 변경이 없음을 확신하려는 것이며 메시지의 송신자 식별을 필요로 하는 것은 아니다.

• **메시지 부인 방지**(Message Non-Repudiation)

책임과 관계되는 요구사항으로 송신자는 메시지를 보냈다는 사실을 부인할 수 없어야 한다.

• **객체 인증**(Entity Authentication)

수신자는 송신자가 메시지를 생성했음을 확신할 수 있게 해야 하며 송신자가 현재 통신 중인 실제 송신자 네트워크의 노드임을 나타낼 수 있는 증거를 가져야 한다. 변경되지 않고 수신된 메시지는 충분히 작은 시간 내에 생성되어야 하므로 시간 정보를 이용하여 증거를 만들 수 있다.

• **접근 제어**(Access Control)

구성 노드와 다른 노드에게서 제공받는 특정 서비스에 접속하는 것은 로컬 네트워크의 정책을 통해 결정되어야 한다. 인증을 통해 각 네트워크 노드의 권한을 결정하여 접근 제어를 할 수 있다.

• **메시지 기밀성**(Message Confidentiality)

메시지는 접근이 인가되지 않은 노드로부터 안전하게 보호되어야 한다.

• **가용성**(Availability)

네트워크와 응용프로그램은 오류가 있거나 부당한 상황에서도 사용 가능해야 한다. 이는 문제가 있는 부분을 제거한 뒤에 정상적인 작동을 계속하기 위해 보안적인 문제뿐아니라 오류에 견딜 수 있는(fault- tolerant)

설계, 자원 소모 공격에 대한 복원 등이 요구된다.

• 개인정보보호 및 익명성(Privacy and Anonymity)

차량 통신 시스템은 사용자의 개인정보에 접근할 수 없어야 한다. 차량사고 현장 수사와 같은 분쟁에서 증거를 찾기 위한 경우에는 정보에 접근할 수 있어야 하지만 상황에 따라서 개인정보는 인가되지 않은 접근으로부터 보호되어야 된다. 또한, 모든 차량은 익명성(anonymity)이 보장되어야 한다. 이는 어떤 차량이 메시지를 보내거나 이동 등 특정 동작을 하였을 때 다른 관찰자들이 특정 동작을 한 차량을 알 수 없어야 함을 요구한다.

• 정당성 식별(Liability Identification)

운전자는 다른 노드나 전송 시스템의 작동을 혼란시킨 계획적이거나 우발적인 행동에 대해 책임질 수 있어야 한다. "상황에 따른 개인정보보호" 요구사항의 한 부분으로 기관은 메시지 송신자의 신원을 결정할 수 있어야 한다.

이러한 요구사항은 차량 통신 시스템에서 만족되어야 하는데 정당성 식별과 익명성은 사용자의 정보에 대한 공개와 보호로 상반되므로 필요에 따라 그 정도를 조절해야 한다.

Ⅵ. 결 론

본 고에서는 차량 네트워크 기술인 VANET에서 보안의 중요성을 서술하고 VANET에서 보안과 관련된 고려사항 및 제약사항과 가능한 위협을 정리하였다. 또한 VANET에서 사용자의 정보 보호와 안전한 통신을 위해 만족해야할 보안요구사항을 분석하였다. 이를 통해 향후에는 VANET에서 보안을 위해 가져야할 보안 기능을 도출하고 안전한 VANET의 시스템 모델을 제안하는 연구가 이루어져야 할 것이다.

참고문헌

[1] 김태환, 김희철, 홍원기, "차량 애드혹 네트워크를 위한 영역 기반 릴레이 노드 선택 알고리즘", 전자공학회 논문지 제43권 제9호, pp.88-98, 2006년 9월.

[2] Maxim Raya, JeanPierre Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, Volume 15, Issue 1, pp. 39-68, Jan 2007.

[3] 최병철, 김정녀, "차량 통신 보안 및 프라이버시 주요 이슈", 정보통신기술, 제22권 제 1호, 2008년 5월.

[4] 오현서, 최혜옥, 조한벽, "차량 통신기술 동향", 주간기술동향 1315호, 2007년 9월.

[5] 이우신, 이혁준, "차량간 통신을 위한 비경로형 멀티홉 패킷 포워딩 프로토콜", 한국정보과학회논문지 정보통신 제34권 제5호, pp.328-339, 2007년 10월.

[6] 이상선, "VANET(Vehicle Ad-hoc Network)환경에서의 라우팅 기술 및 서비스 개발 동향", 제 22권 제1호, 2008년 5월.

[7] Maxim Raya ,JeanPierre Hubaux, "The Security of Vehicular Ad Hoc Networks," Workshop on Security of ad hoc and Sensor Networks, pp. 11-21, Nov 2005.

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

[9] Yi Qian, and Nader Moayeri, "Design of Secure and Application-Oriented VANETs", Proceedings of IEEE VTC 2008-Spring, Singapore, May 2008.

[10] P. Papadimitratos, V. Gligor, J-P. Hubaux, "Securing Vehicular Communications-Assumptions, Requirements, and Principles", Proceedings of the Workshop on Embedded Security on Cars (ESCAR) 2006, Nov 2006.

[11] http://www.et2.tu-harburg.de/fleetnet/index.html.

[12] http://www.car-2-car.org/.

[13] http://www.prevent-ip.org/en/prevent_subprojects/ safe_speed_and_safe_following/willwarn.

[14] http://www.ertico.com/en/activities/activities/emerge.htm.

[15] http://www.cartalk2000.net/.

[16] http://www.safespot-eu.org/.

[17] http://www.watchover-eu.org/.

[18] http://www.informatik.uni-mannheim.de/pi4/projects/vanet.

[19] http://ivc.epfl.ch/.

<著 者 紹 介>

조 영 준 (Youngjun Cho)

학생회원

2008년 8월: 성균관대학교 정보통신공학부 컴퓨터공학과 졸업
2008년 9월~현재: 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정
<관심분야> 정보보호, 네트워크 보안, 암호이론

이 현 승 (Hyunseung Lee)

학생회원

2008년 2월: 성균관대학교 정보통신공학부(공학사)
2008년 3월~현재: 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정
<관심분야> 암호이론, 네트워크 보안, 금융보안

박 남 제 (Namje Park)

종신회원

2000년: 동국대학교 정보산업학과 졸업
2003년: 성균관대학교 정보보호학과 석사
2008년: 성균관대학교 컴퓨터공학과 박사
2003년 04월~현재: 한국전자통신연구원 정보보호연구본부 선임연구원
2004년 06월~현재: 지식경제부 핵심에로기술지원 기술지도전문가
2005년 03월~현재: 모바일RFID포럼 표준기획분과위원, 정보보호분과 간사
2008년 01월~현재: 영국캠브리지국제인명센터(IBC), Vice President
2008년 09월~현재: 한국과학기술자네트워크(KOSEN) 전문위원
2008년 09월~현재: ITU-T SG17 Q.9 Co-Editor
<관심분야> 정보보호, 암호이론. 모바일 컴퓨팅, 센서네트워크

최 두 호 (Dooho Choi)

정회원

1994년 2월: 성균관대학교 수학과 졸업
1996년 2월: 한국과학기술원 수학과 석사
2002년 2월: 한국과학기술원 수학과 박사
2002년~2007년: 한국전자통신연구원 선임연구원, 팀장
2006년 09월~현재: ITU-T X.1171 (X.nidsec-1) 에디터
<관심분야> 정보보호, 암호이론, RFID/USN, 위상수학

원 동 호 (Dongho Won)

종신회원

1976년~1988년: 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회 회장
현재: 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장
<관심분야> 암호이론, 정보이론, 정보보호

김 승 주 (Seungjoo Kim)
종신회원

1994년 2월~1999년 2월 : 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2004년 3월~현재 : 성균관대학교 정보통신공학부 교수
2001년 1월~현재 : 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 7월~현재 : 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET