VANETs 기반 텔레매틱스 서비스를 위한 안전한 개방 플랫폼

오선진* · 배인한**

1. 서 론

지난 20년 동안 자동차는 주로 기계적이고 전기적인 상품으로부터 매우 복잡한 모바일 컴퓨터 시스템으로 진화하였다. 지난 수 년 동안 차량 내의 컴퓨터 하드웨어와 소프트웨어의 양은 폭발적으로 증가해 왔다. 그러나 현재 모든 그러한 모바일 시스템들은 서로 연결되지도 않았고 폐쇄된 소프트웨어 플랫폼 상에서 작동한다.

비연결(Unconnected) - 시스템은 서로 연결되지 않았고 상호간이나 인터넷과 같은 망과 통신할 수 없다. 어떤 특별한 응용은 외부 세상과 데이터 채널을 가질 수 있음에도 불구하고, 예를 들어, 네비게이션 시스템이 망으로 부터 GPRS/GSM을 경유하여 차량 트래픽 정보를 수신할 수 있듯이, 다른 차량이나 망과의 일반적이고, 표준화되어 장착된 차량 통신 시스템이 존재하지 않는다.

폐쇄된 플랫폼(Closed Platform) - 차량 내부 시스템은 폐쇄된 플랫폼이다. 소프트웨어는 차량 메이커와 공급자에 의해 작성되었으며 단지 그들에 의해서 설치되고 갱신된다. 어느 순간에도 제3자 회사가 어떤 종류의 차량을 위한 응용을 개발할 수도 고객이 그들의 차량에 설치할 수도 없다.

향후에 새로운 기술 및 표준과 더불어 앞으로 10년 내에 기술과 표준 둘 다 변할 것이다. 자동차는 개방된 소프트웨어와 서비스 플랫폼에서 작동할 연결된 모바일망의 노드가 될 것이고, 회사들이 망이나 직접 차량 내부 응용을 통해서 서비스나 소프트웨어를 제공할 수 있을 것이다. 따라서 안전하고 개방된 플랫폼이 이러한 새로운 가능성들의 이용을 위하여 필요하다.

본 논문의 구성은 다음과 같다. 1장에서 차량들의 무선 연결이 가능하도록 하는 주요 기술들을 소개한다. 2장에서는 그러한 망의 특징과 가능한 응용들을 소개한다. 3장에서는 그러한 망의 보안을 위한 특별한 요구사항과 도전들을 논의하고 차량 애드혹 망을 위한 통합된 보안 구조의 접근 방법을 제시한다. 4장에서는 텔레매틱스를 위한 가능한 개방 플랫폼의 구조를 소개한다. 그리고 마지막 장에서 이러한 기술들이 미래에 어떻게 개발 적용되고 향후 과제의 어느 분야에 눈에 띄게 발전할지에 대한 전망과 함께 결론을 맺는다.

1.1 애드혹 P2P 망

일반적인 고정된 컴퓨터 망들은 망 인프라 구조 상에 구축된다. 대부분의 경우 예를 들어 사용

※ 교신저자(Corresponding Author) : 오선진, 주소 : 충북 제천시 세명로 117(390-711), 전화 : 043)649-1279, FAX : 043)649- 1758, E-mail : sjoh@semyung.ac.kr
* 세명대학교 정보통신공학부 교수
** 대구가톨릭대학교 컴퓨터정보통신공학부 교수 (E-mail : ihbae@cu.ac.kr)

자 디렉터리나 이름 데이터베이스와 같은 일종의 중앙 서비스들이 있다. 망들은 고정된 통신 인프라 구조를 사용하며 유선망과 스위치나 라우터와 같은 스위칭 하드웨어로 구성된다. 이러한 컴포넌트들의 위치나 논리적 계층은 수동적으로 구성되고 망 위상의 변화는 종종 재구성을 요구한다.

P2P 망은 분산 망으로 어떠한 고정된 인프라 구조나 중앙 집중식 서비스에 독립적이다. 망의 종단은 망 자체에 국한되며 인프라 구조나 망의 백본을 구축한다. 라우팅이나 주소 할당과 같은 모든 망 기능들은 노드 스스로에 의해 수행된다. 직접 연결되지 않은 노드들 사이의 트래픽은 중간 노드로 동작하는 다른 노드를 경유하여 전달된다.

애드혹 망은 자기 조직화 P2P 망이다. 참여하는 노드들은 수동적 방해 없이 자동적으로 망구조를 구성하며 동적인 노드의 망 이탈이나 결합에 대처할 수 있다. 망은 노드들 사이의 어떠한 이전의 관계나 초기화에 의존하지 않는다.

1.2 모바일/차량 애드혹 망

모바일 애드혹 망(MANET)은 특별한 특징을 가진 애드혹 망이다. 망의 노드들은 시간에 따라 이동하고 결합하며 이탈한다. 주로 무선 통신을 사용하면서 노드들 사이의 링크는 매우 불안정하여 노드들은 지속적으로 통신 범위를 벗어나 다른 노드의 통신 범위에 도달한다. 만약 MANET의 노드들이 차량이면 망은 차량 애드혹 망 또는 간단히 VANET이라 부른다. VANET은 일반적으로 매우 이동성이 높은 망 노드들을 가지며 노드들 사이의 상대 속도가 500Km/h에 이르는 매우 고속으로 이동하고, 매우 짧게 지속되고 불안정한 통신 링크를 갖는다. 그림 1은 VANET의 예를 보여준다. 7개의 노드가 애드혹 망을 형성하고 거기서 메시지가 노드 A와 B사이에 중간노드 H와

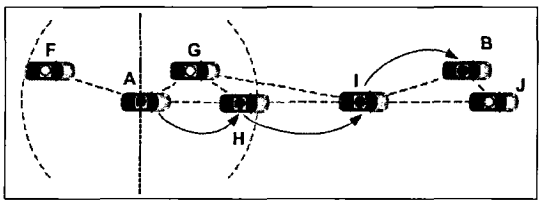

그림 1. VANET

I를 통해 전달된다.

VANET은 고정된 도로변의 게이트웨이와 연결할 수 있는 메커니즘을 가질 수 있고 인터넷과 같은 공통 망을 이들 게이트웨이를 통해 접근할 수 있다.

지난 5년 동안 P2P 기술의 연구와 개발을 위해 수많은 프로젝트가 자동차 산업 분야에서 수행되었다[1-5].

이전 프로젝트들은 하나의 자동차 제조사를 위해 작동하는 VANET을 만들기 위하여 초점이 맞추어진 반면 VANET을 구축하기 위한 하부 기술이나 프로토콜들은 지금 표준화 과정에 있다[2, 6]. 이것이 망이 다수의 생산자들을 포괄하는 망을 가능하게 만들고, 협력 가능한 VANET 기술을 위한 빠른 설치를 수월하게 한다. 많은 VANET 응용들이 적절하게 기능을 다하기 위하여 도로 위의 VANET 가능 차량의 어느 정도의 보급이 요구되기 때문에 빠른 설치가 중요하다.

현재와 향후 프로젝트들은 이러한 VANET 상에서 실행될 수 있는 응용의 개발을 시작할 것이다[7-9].

이전의 연구들은 라우팅, 어드레싱, 통신 프로토콜과 같은 VANET의 기능성에 집중되었다. 이러한 프로젝트의 주요 목표는 작동하는 VANET의 개발과 모형의 구현이고 VANET의 보안은 두 번째 문제였다. 어떤 프로젝트에서는 모바일 애드혹 망의 보안을 연구하였으나[11-13] 이러한 프로젝트들은 단일, VANET 보안의 하나의 격리된

면(예를 들어 라우팅)에 집중되었고 좀처럼 주요 VANET 프로젝트에 통합되지도 않고 VANET 시스템 구조 안으로의 통합 방법을 제안하지도 않았다.

그러나 현재 WILLWARN[7]과 같은 응용 위주 프로젝트들은 블랙박스 VANET 통신 시스템의 사용을 가정하기 때문에 진행 중인 NOW[8]과 같이 구현을 참조하고 이러한 시스템 안에 보안을 통합하는 것이 중요하게 된다.

2. VANET 텔레매틱스

VANET 텔레매틱스를 위한 사용 사례는 안전과 비안전 응용의 두 가지 주요 응용 분야로 분류될 수 있다.

안전(Safety) 응용은 또한 "능동적 안전(active-safety)" 응용이라고도 불린다. 차량 간 통신은 새롭고 매우 전망이 좋은 안전 응용을 허용한다. 근처의 차량과의 끊임없는 통신을 통해 센서 데이터나 다른 정보의 교환, 사고 예방 그리고 운전 지원이 가능하게 되고 도로상에서의 재난이나 부상을 줄일 수 있다. 사고 예방 응용들은 다가올 위험과 특별한 상황(그림 2참조)에 대해 운전자에게 능동적으로 경고한다. VANET은 운전자의 시야의 라인을 따라 통신 범위를 확장하기 때문에 이러한 응용들은 사전 경고 시간을 충분히 확장하여 사고의 횟수를 줄인다. 차선 머징 지원, 추월 지원, 트래픽 관리, 가상 경고 신호 그리고 비상등과 같은 응용들은 역시 사고의 횟수나 도로의 위험을 줄인다.

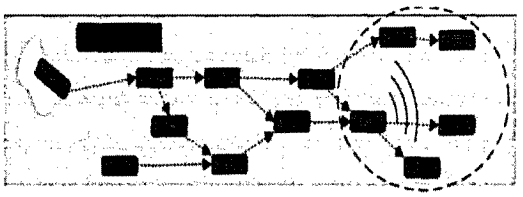

그림 2. 위험 경고 다중 홉 시나리오

비안전(Non-Safety) 응용들은 편의, 오락 정보와 위치 기반 서비스에 초점을 맞춘다. 예를 들어, 모바일 이메일 서비스, 음악 다운로드 서비스, 다른 차량과의 통신, 또는 차량내의 소프트웨어 설치나 갱신을 허용하는 설치와 유지보수 서비스 등이 있다. 또 다른 사용 사례로는 원격 진단과 차량의 유지보수 등이 있다.

차량들이 서로 간 또는 인프라 구조와 통신하는 상호 작동 시스템(자동화 또는 독립 시스템으로의 확장)은 차량의 위치 그리고 도로 환경에 대한 가용 정보의 품질과 신뢰성을 증가시키며 도로 사용자를 위한 개선되고 새로운 서비스를 가능하게 한다.

2.1 통신 패턴

VANETs과 VANETs에 기반한 텔레매틱스 응용들은 전통적인 망으로 부터 일반적으로 알려진 것과는 다른 통신 패턴을 사용한다.

단일 홉 통신과 다중 홉 통신의 두 가지 다른 범주의 VANET 통신이 있다. 단일 홉 통신은 무선 통신 시스템을 통해 직접 서로 도달할 수 있는 노드들 간의 통신을 말한다. 다중 홉 통신은 직접 서로 통신하기에 노드들이 너무 멀리 떨어진 곳에서의 통신을 말한다. 노드들은 중간 노드로 다른 노드들을 사용해야 하고 특별한 MANET 라우팅 프로토콜[14-16]로 메시지를 목적지로 전송한다.

이러한 분류에 기반 하여 일반적인 VANETs에서 4가지의 통신 패턴을 구분할 수 있다.

- 직접 노드-대-노드 통신: 노드는 그들의 무선통신 시스템의 범위 내의 하나 또는 모든 노드들과 통신한다.
- 직접 노드-대-인프라 구조 통신: 노드는 그

들의 무선통신 시스템 범위 내의 고정된 인프라 구조와 통신한다.

- 노드-대-노드 다중 홉 통신: 노드는 다른 노드를 중간 노드로 사용하면서 그것들의 무선통신 시스템 범위 밖의 다른 노드들과 통신한다.
- 노드-대-인프라 구조 다중 홉 통신: 노드는 다른 노드를 중간 노드로 사용하면서 그것들의 무선통신 시스템 범위 밖의 고정된 인프라 구조와 통신한다.

전통적인 망에서 가장 일반적인 형태의 통신은 유니캐스트로 하나의 노드가 망 주소를 통해 어드레스된 다른 노드에 메시지를 송신한다. 이것이 아직도 VANETs에서는 유용한 반면 대부분의 VANET 응용들은 다른 통신 요구조건을 가진다. 특히 안전 분야에서 많은 VANET 응용들은 특별한 노드로가 아닌 노드 그룹으로 메시지를 보낸다. 둘째로 이 노드그룹은 종종 지리적 위치를 통해 주소화 되는데 이것은 이 지역 내의 단일 노드가 아닌 주소화 된 지역이기 때문이다.

이 통신 패턴은 지오캐스트(geocast)라 불린다. 노드는 메시지를 지리적인 지역으로 주소화 된 곳으로 전송한다. 송신노드가 주소화 된 지역 안에 있다면 메시지는 직접 전파되거나 그러한 지오캐스트 메시지의 전달 프로세스는 두 상태로 분리되기도 한다. 즉, 메시지는 먼저 진로 전송(line-forwarding)을 통해 주소화 된 지역에 도달할 때까지 전달되고 나서 이 지역에서 전파된다[17]. 약간 다른 변종인 지오애니캐스트(geoanycast)에서는 메시지가 어느 특별한 지역 내의 하나의 랜덤 노드에 어드레스 된다. 그 메시지는 또한 이 지역 내의 첫 번째 노드로 전달되는 주소화 된 지역에 도달할 때까지 진로 전송을 통해 전달된다.

2.2 위치 기반 라우팅

전통적인 망은 대부분 망의 위상에 기반한 라우팅 접근방법을 사용한다. 망 주소는 망의 계층적 위상에 기반하여 주소화 되고 한 노드에서 다른 노드로 쉬운 라우트 발견을 위해 허용된다.

VANETs에서는 위상 기반 라우팅이 가능하지 않다[18]. VANET의 위상은 계속해서 변화하고 노드들은 고속으로 이동하며 지속적으로 망에 결합하거나 이탈하고, 불안정하고 변화하는 링크를 만든다. 따라서 대부분의 VANET 시스템은 위치 기반 라우팅 접근방법을 사용한다. 패킷들은 송신자와 수신자의 위치에 따라 라우트 된다.

많은 연구들은 VANETs에서 위치기반 라우팅 프로토콜이 위상기반 접근 방법보다 망 처리력과 안정성 측면에서 훨씬 우수함을 보여 주었다.

위치기반 라우팅을 위한 일반적으로 사용되는 라우팅 알고리즘은 탐욕 전송(greedy forwarding)이다. 모든 노드들은 그 통신 범위 내에서 자신의 위치를 알리는 주기적 비컨(beacon)을 모든 직접 이웃들에게 전송한다. 노드들은 이웃 위치를 갖는 데이터 테이블을 유지한다. 만약 노드가 자신이 목적지가 아닌 데이터 패킷을 수신하면 그 패킷으로부터 목적지 위치를 찾아보고 그 노드의 이웃의 테이블을 통해 목적지 위치에 가장 근접한 이웃을 찾아 패킷을 전달한다. 이런 작업을 반복하여 목적 노드에 도달할 때까지 이런 전달과정으로 목적지 위치에 근접한 곳으로 패킷을 계속해서 보내게 된다.

탐욕 전송 알고리즘의 문제점은 지역 최대점 문제(local-maximum problem)이다. 만약 메시지가 노드에 도달했을 때 그 노드가 자신보다 더 가까운 목적지 위치를 갖는 직접 이웃이 없다면 메시지는 이 노드에서 블록 될 것이다. GPSR (Greedy- Perimeter-State-Routing)[14] 프로토

콜은 이런 상황을 감지하고 이 패킷을 위한 라우팅 알고리즘을 주변 모드로 전환함으로써 이 문제를 해결한다. 패킷들은 그래프 이론으로부터 알려진 오른손 법칙을 사용하여 국부 최대점 주변 경계로 라우트 된다.

2.3 어드레싱과 위치 검색

이미 언급했던 위치기반 라우팅 메커니즘은 노드의 위치에 종속적이며 어드레싱과 라우팅 방법에서 위치를 사용한다. 노드들은 비컨이라는 작은 데이터 패킷을 통해 그것들의 직접 이웃들에게 자신의 위치를 방송한다. 그러나 노드 위치는 어드레싱의 일부이기 때문에 노드는 메시지를 간접 이웃들에게 전송하기를 원한다면 그것들의 위치 또한 알아야만 한다. 현재 노드의 위치를 탐색할 수 있는 네트워크상의 위치 서비스가 있어야만 한다. 정적 노드 식별자와 결합되어 이것은 망에 대한 거대한 프라이버시 문제를 초래한다.

제 3자에 이동 패턴을 노출하여 노드의 수명 동안에 추적되는 것이 가능할 수 있다. 그러한 빅 브러더 시나리오에 대한 보호가 VANETs의 소비자 수용 수준에 도달할 필요가 있다.

그러나 망이 비안전 영역에서 매우 유망한 응용을 위해 필요한 유니캐스트 통신을 지원해야만 한다면 노드가 임의의 다른 노드의 위치를 탐색할 수 있는 메커니즘이 존재할 것이다. 이것은 프라이버시 보안을 이 메커니즘에 도입하는 커다란 도전인 반면 중앙 집중적이지 않고 인프라 구조가 없는 망[19-21] 내에서는 매우 복잡해 질 것이다.

노드의 위치 탐색이 가능하면서도 프라이버시가 보호되는 시스템을 구축하기 위한 현재의 연구들에는 많은 접근 방법들이 존재한다. 위치 탐색의 문제는 VANETs에서 노드 식별자의 문제와 강하게 연결되어 있다.

각 노드의 지역 프라이버시를 보호하는 동시에 기능적 노드 식별과 어드레싱을 제공하기 위하여 어드레싱과 VANETs을 위한 식별 시스템에 대한 다수의 다른 아이디어들이 존재한다. 이러한 시스템의 일부는 분산되고, 다른 시스템들은 노드에 초기 인증을 제공하는 중앙 인가에 기초한다.

2.4 응용

(1) 안전(Safety): 협력하는 운전을 위한 첫 번째 단계로 차량 간 정보의 교환은 도로 상에서 더욱 안전하기 위한 핵심 도구 중의 하나일 것이다. 따라서 안전은 VANETs의 중요하고 가장 유용한 응용이다(그림 3 참조).

다가오는 능동적 안전 시스템의 한 예로 WILLWARN 프로젝트가 있는데 VANET 안전 응용의 생성에 목표를 두고 있다. WILLWARN [7] 프로젝트는 "무선 지역 위험 경고 (Wireless Local Danger Warning)"의 약자로 EU가 펀드를 제공하는 PReVENT 프로젝트의 서브 프로젝트이다[22].

PReVENT(Preventive and Active Safety Applications integrated project)의 전체 목표는 안전 응용들을 개발, 검사, 평가하는 것이고, 현재 센서와 통신 기술의 발전으로 결국 그것들을 전용

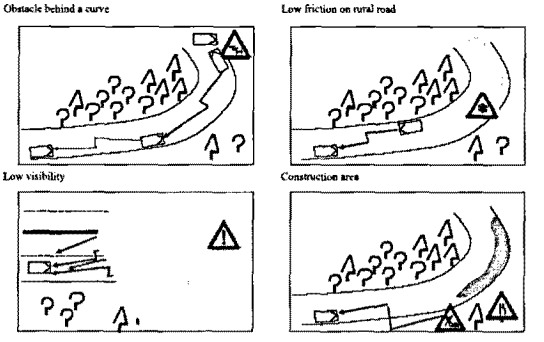

그림 3. WILLWARN 응용 시나리오

전시품 플랫폼에 통합하는 것이다. PReVENT의 야심찬 목표를 성취하는 것은 그 연구를 분할하고, 분할되었지만 서로 영향을 미치는 분야들을 그룹화 하는 것이 요구된다. 수직적 활동들을 통하여 하나의 안전한 기능의 독립적인 개발과 다른 수직적 기능 분야들이 통합된 안전 시스템을 생산하는 수평적 활동 지원으로 상호작용하는 것을 허용한다.

그림 4는 수직적 활동과 수평적 활동이 요구되는 PReVENT 구조를 보여준다. 수직적 활동은 차량 주변의 전자적 안전 지역을 만들기 위하여 필요한 하나의 응용과 기능의 개발을 다룬다. 개발 중인 모든 응용들은 공지, 경고, 지원 그리고 사고 상황에서 차량 승객 보호를 위하여 운전 상황에 대한 더 나은 이해를 목표로 한다. 수평적 활동은 개발 방법, 공통 구조, 지도 데이터의 사용과 관련 차량 위치 작업, 기능적 통합, 수평적 안전 시스템과 통합된 안전 시스템의 잠재적인 안전성 영향 평가를 커버한다[22].

PReVENT 통합 프로젝트 내의 3년간 WILLWARN 서브 프로젝트는 안전 관련 치명적인 상황이 발생할 때마다 비록 그것이 운전자의 시야로 부터 멀리 떨어져 발생하더라도 운전자에게 경고하는 안전 응용을 개발 통합 그리고 인증

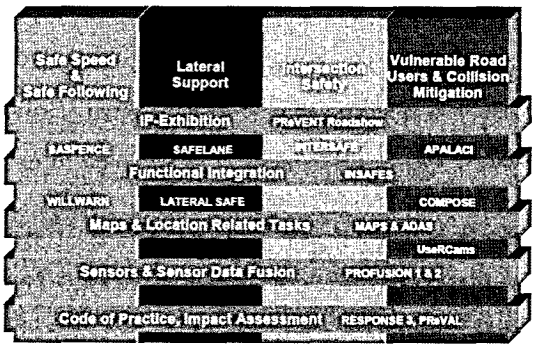

그림 4. PReVENT의 구조

한다. 목표는 온 보드 위험 탐지, 차량 내 경고 관리, 그리고 도로 망 위의 차량들 간 통신에 의한 분산 경고 분배 등을 포함한다. 위험 탐지, 적당한 검사, 메시지 전송 그리고 온 보드 메시지 평가 등이 비록 낮은 장착률에서도 운전자에게 높은 장점을 가능하게 할 것이다[7].

WILLWARN 응용은 그림 3에서 보여 진 것처럼 다음의 시나리오를 포함한다.

- 커브 아래의 장애물(다중 홉 플러딩/지오캐스트)
- 도시 도로 상의 낮은 마찰(다중 홉 플러딩/지오캐스트)
- 낮은 가시도(다중 홉 플러딩/지오캐스트)
- 공사구간(단일 홉 플러딩)
- 비상 긴급차량(단일 홉과 다중 홉 플러딩)

WILLWARN 시스템은 그것들의 경고 메시지를 전파하기 위하여 단일 홉과 다중 홉 VANET 통신을 사용할 것이다. 그것은 가상 경고 신호와 같은 도로변 장치(RSUs, 고정된 노드)를 역시 고려한다. WILLWARN 프로젝트는 그것들의 기초로 진행되고 있는 NoW 참조 구현[8] 같은 기존의 VANET 통신 플랫폼 사용을 대상으로 하고 응용 계층에 집중할 것이다.

(2) 비안전(Non-Safety): 요구되어진 더 필요한 안전 기능성 외에 VANET은 더욱 다양한 다른 응용들을 위해 사용될 것이고, 새로운 비지니스 기회를 창출할 것이다. 비안전 응용은 운전자와 다른 차량 승객의 편의, 정보 그리고 오락에 목적을 둘 것이다.

이것의 예는 홈 네트워크, 중앙 집중식 서버 또는 회사 네트워크와 연락, 스케줄 또는 멀티미디어 데이터의 동기화가 될 수 있다. 진보된 오락 응용들은 라디오에서 현재 재생 중인 노래를 운전

자가 구입해서 차량 내에 그것을 다운로드 하는 것을 허용할 것이다.

위치 기반 서비스는 현재 환경과 차량의 상황 그리고 운전자에 적합한 맞춤형 정보를 제공할 것이다. 이것은 유동적인 차량 데이터 또는 트래픽 센터에 기반한 실시간 트래픽 정보, 차량의 근처에서의 흥미로운 이벤트에 대한 전자적 안내이고, 각각의 경우에서 이 정보는 운전자/승객의 개인 프로파일에 적응될 수 있다. 약속된 견인을 위한 가상 에이전시와 같은 협력적인 응용들 역시 가능하다.

안전한 VANET은 차량 제조사나 서비스 제공자에 의해 차량의 원격 진단, 차량 내 소프트웨어 설치 및 갱신, 차량 내 소프트웨어 기능의 원격 시동 등을 허용한다.

통신 응용은 자동차 내에서 이메일과 같은 표준 망 서비스와 다른 차량과의 직접통신 또는 차량군집 주행 응용과 같은 추가적 통신 서비스를 허용할 것이다. VANETs은 차량들 간 멀티 플레이어 게임을 할 수 있는 새로운 차량 내 게임을 통하여 또는 고정된 망을 통하여 뒷좌석 오락을 위한 설치와 통신 플랫폼을 제공할 수 있다.

3. VANETs에서 보안

MANETs의 주요 장점 중의 하나는 그들의 고정된 인프라 구조, 중앙 통제 관련 라우팅 장비로부터의 독립이다. 그러나 보안 측면에서는 이러한 장점들도 역시 커다란 도전이다. MANET의 인프라 구조는 망 내에 참여하는 모든 노드들에 의해 형성되기 때문에 망의 신뢰는 단일 노드의 신뢰에 종속적이다. VANETs은 대부분 개방 망으로 중앙 집중식 제어 없이 누구나 접속을 허용하기 때문에 망상에 해롭고 비정상 행위 모드들에 대한 기회가 매우 높다. 많은 전통적인 망 보안 메커니즘들은 중앙 컴포넌트나 노드 간 사전 통신 상호작용을 요구한다.

VANETs의 보안과 프라이버시는 중요한 속성이고 VANETs이 성공적이고 사용 가능 기술이 될지를 결정하게 될 것이다. 보안에 가장 중요한 응용은 안전 응용이다. 틀리거나 지연된 경고 메시지는 사고를 야기하므로 예방되어야만 한다. 만약 비인증 노드들이 거짓 경고 메시지를 유포할 수 있다면 트래픽 흐름상의 충격은 엄청날 것이고 주요 도로를 완전히 블록 시키거나 다른 트래픽의 방해를 초래할 것이다. 특별히 유럽에서의 고객들은 매우 프라이버시에 민감하여 운전자/차량의 식별이나 위치추적이 가능한 시스템은 용납하지 않을 것이다.

그러나 비안전 분야에서도 많은 가능한 응용들은 강력한 안전과 프라이버시를 요구한다. 특히 만약 VANET을 통해 비지니스가 이루어지거나 차량 내 소프트웨어 갱신 또는 원격 진단과 같은 중요한 작업이 수행되었다면 종단 간 보안이 필요하다. WILLWARN 프로젝트[7]는 보안 스레드와 프라이버시 스레드 그리고 시스템의 그것들의 대응하는 요구사항들을 차별화 한다. 예를 들어, 보안 스레드는 거짓 경고 메시지의 유포, 실제 경고 메시지의 억제 또는 블로킹, 다른 메시지를 위한 시스템의 남용 등을 들 수 있다. 위험감지 모듈에 대한 센서 입력의 보안 역시 고려되어야만 한다.

이미 언급했듯이 프라이버시를 위반하는 시스템은 고객들에 의해 받아들여 질 수 없기 때문에 WILLWARN에서의 프라이버시 요구사항인 차량의 추적 또는 차량의 원격 위치탐색 등은 가능하지 않다. 또한 운전자 또는 차량에 대한 정적 식별도 없다.

VANET은 다중 계층의 동적 통신 시스템이다.

따라서 시스템의 각 계층에 대한 보안 요구사항은 분석되어져야만 하고 그것들에 대한 요구 사항들이 정의되어야 한다.

라우팅에 대한 공격이 VANETs에서는 가장 큰 문제이다. 그들의 위치에 대한 노드 위조나 부당 변경은 거짓된 지리적 지역에 대한 메시지를 발생할 수 있고 VANET의 어떤 부분의 모든 트래픽을 블록하거나 가로챌 수 있으며 또는 망 분할을 초래할 수 있다[23]. 그러나 응용계층과 데이터 채널 상에서의 보안 역시 매우 중요하다. 전통적인 망과 대조적으로 VANETs에서 보안 방향은 교차 계층 문제이다. VANET 라우팅 스택의 보안 컴포넌트의 예로는 그것의 알려진 위치를 부당 변경한 노드를 탐지하고 라우팅 프로세스에서 그것을 제외하는 것이다. 공통 망 통신 스택의 계층적 구조를 통해 응용계층은 라우팅 단계에서 이러한 이상행위 탐지가 알려지지 않는다.

반면 능동적 안전 응용 예로 응용계층은 위험 경고를 수신하고 그럴듯한 타당성 검사를 통해 해로운 노드를 탐지한다. 라우팅 계층에서 이와 같이 분명하게 해로운 노드들을 신뢰할 수 없을 것이다. 하지만 라우팅 계층에서는 이 정보에 접근할 길이 없다.

따라서 수직적 안전 컴포넌트를 VANETs을 위한 안전 구조로 개발되었다(그림 5 참조). 먼저 VANET 스택의 모든 계층상의 모든 보안 관련 컴포넌트들과 그것들의 기능을 격리시킨다(그림 5의 오른쪽 그림 참조). 그리고 수직적 보안 컴포넌트를 통해 이것들의 컴포넌트들을 위한 발행-구독 기반 통신 메커니즘을 제공한다. 예를 들어 응용계층상의 컴포넌트는 라우팅 스택의 모든 보안 관련 이벤트를 구독할 수 있다. 가상 보안 컴포넌트는 전체적으로 VANET 노드들의 보안 상황으로 보안 데이터베이스를 구축하고 결과적으로

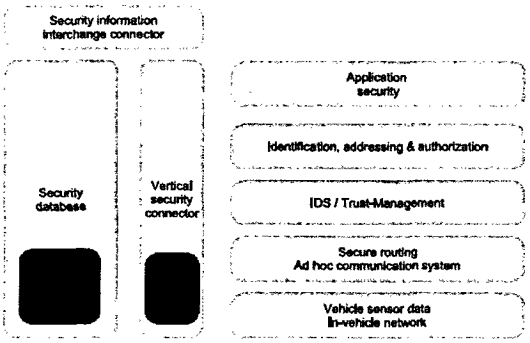

그림 5. 보안 구조 계획

모든 계층들의 정보를 갖는다. 이 데이터베이스 안에 또한 신뢰된 컴퓨팅 컴포넌트가 있으며 중요한 암호 키와 증명서에 대한 보안 저장소를 제공한다.

아울러 많은 보안 컴포넌트들은 암호화 함수 또는 키 저장소 그리고 신뢰 저장소와 같은 동일한 기본 기능을 사용할 것이다. 이러한 기능들은 다른 컴포넌트를 위한 가상 보안 컴포넌트에 의해 중앙에서 제공되며 이는 개발 노력을 낮추고 기능을 보다 안전하게 만든다.

4. 개방 텔레매틱스를 위한 모델

현재의 차량 컴퓨터 시스템은 폐쇄된 플랫폼이다. 제 3자에 의해 차량에 설치될 소프트웨어를 개발할 수 없다. 소프트웨어는 단지 자동차 생산자나 공급자에 의해만 생산된다. 고객들은 자신의 차량을 위해 서로 다른 판매자로 부터 다양한 소프트웨어를 선택할 수 없으며 소프트웨어 판매자들은 텔레매틱스 시장으로의 진입에 높은 장벽이 있다.

미래에 이것은 새로운 텔레매틱스 플랫폼의 등장과 표준화된 차량-대-인프라 구조 그리고 차량-대-차량 통신시스템의 설치와 함께 변화할 것이고 텔레매틱스를 위한 개방 플랫폼이 생성될 것이

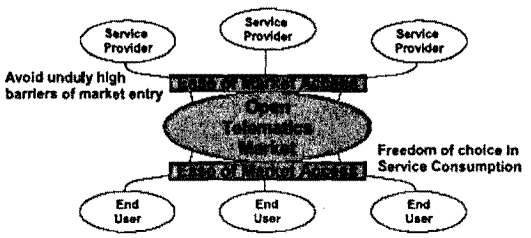

그림 6. GST 개방 플랫폼

다. 이러한 플랫폼으로 어떠한 소프트웨어 판매자도 텔레매틱스 시장을 위한 소프트웨어를 생산하기 쉬워지고 고객들은 다양한 소프트웨어 판매자, 응용 그리고 서비스 사이에서의 선택의 자유를 갖게 된다(그림 6 참조). 또한 이러한 개방 플랫폼은 텔레매틱스와 모바일 서비스 분야에 개방된 경쟁을 유발하여 새롭고 흥미 있는 응용들을 이끌어 낼 것이다.

텔레매틱스 서비스를 위한 이러한 개방 플랫폼의 개발을 위한 알려진 프로젝트로는 EU 통합 프로젝트인 "GST(Global System for Telematics)"를 들 수 있다.

4.1 GST 프로젝트

GST는 EU가 펀드를 제공한 통합 프로젝트로 자동차 텔레매틱스 서비스를 위한 개방형 표준화된 종단 간 구조를 생성하는 것이다[9].

GST의 비전은 모든 미래의 차량들이 공통 구조와 표준 인터페이스에 기반한 환경과 서로 상호작용을 위한 다양한 통신 도구들을 장착하게 될 것이다. 운전자나 소유자는 유럽 내에서 그들이 운전하는 어느 곳에서든지 온라인 안전, 효율성, 그리고 편의를 높이는 서비스의 동적 제공에 근접하기 위한 온 보드, 통합된 텔레매틱스 시스템에 의존할 수 있게 될 것이다[9].

차량 내 텔레매틱스 장치는 중요한 온 보드 안전 응용의 정확성과 신뢰성을 향상시키기 위해 온 보드 정보의 갱신을 허용하는 자동차 응용을 위한 지원자 역할을 역시 할 것이다. 이러한 비전을 달성하기 위해 GST는 종단 간 텔레매틱스를 위한 개방되고 표준화된 프레임 워크 구조를 생성할 것이다. 개방성은 새로운 서비스와 응용의 삭제, 갱신 그리고 설치를 위한 공통 메커니즘뿐만 아니라 기존의 또는 새로운 전달자나 프로토콜을 지원하기 위한 구조의 능력과 관련된다. 표준은 지원하는 기술의 복잡도와 이질성을 감추도록 허용하는 주요 인터페이스를 위해 필요하다[9].

GST의 목적은 혁신적인 텔레매틱스 서비스가 효율적인 비용으로 개발되고 보급되어 생산자나 소비자들에게 경제적인 텔레매틱스 서비스가 가능한 지역을 증가시킬 수 있는 환경을 생성하는 것이다[9].

GST안에 4가지 기술 중심 서브 프로젝트와 3가지 서비스 중심 서브 프로젝트가 있다. 4가지 기술 중심 서브 프로젝트는 온라인 서비스를 위한 수평적 시장의 지원을 목적으로 한다.

- 개방 시스템: 모든 섹터들 간의 협력과 인프라 구조 공유 가능
- 보안: 시스템과 데이터, 프라이버시, 신뢰성의 보호
- 서비스 지불: 지불과 청구에 대한 공통적인 방법
- 인증: 시장에 빠른 서비스 설치 촉진

3가지 서비스 중심 서브 프로젝트의 목적은 몇몇 안전 서비스와 시장을 용이하게 하는 서비스를 시장으로 가져오는 것을 돕는데 있다.

- 재난구조 인프라 구조, e-call을 미래 차량에서 표준 특징에 이르게 하는데 도움을 주는 비상 긴급 차량을 포함하는 폐쇄된 루프

- 향상된 유동 차량 데이터 업로드
- 안전 향상과 부가 서비스의 폭넓은 범위를 허용하기 위한 안전 채널 방송/다운로드

GST는 예를 들어 다중 도메인에 걸친 서비스 호환성 촉진, 하나의 서비스 컴포넌트의 간단한 교환이나 갱신, 서비스 컴포넌트의 원격 설치나 유지보수, 전체 응용의 쉬운 확장성, 다른 표준이나 버전의 적응성, 전체 종단 간 체인의 안전 작동과 같은 서비스 시장을 가능하게 하는 유연하고 개방된 텔레매틱스 구조를 유도해야 한다. 아울러, 이러한 개방 텔레매틱스 구조에서 전체 생명주기 문제도 다루어 져야 한다. 이것은 예를 들어 차량 텔레매틱스 플랫폼의 다른 개발 단계에 대한 적응 능력, 또는 다른 무선 통신 기술에 무단절 무선 네트워킹의 관리와 같은 것을 지원한다[9].

차량 내 컴퓨팅 플랫폼은 서로 다른 브랜드 간에 그리고 또한 같은 브랜드의 다른 모델 간에 판이하게 다르다. 교차 제조사 또는 교차 모델 텔레매틱스 소프트웨어를 구축하기 위해서 소프트웨어 판매자는 모든 이러한 특별 플랫폼과 모델에 그것들의 응용이 적응되어야 하며 응용들이 소프트웨어 변경이나 다른 설치 메커니즘으로 최신 응용을 유지해야 한다.

GST 프로젝트는 텔레매틱스 서비스의 개발을 용이하게 하는 표준화된 API를 생성할 것이다. GST 개념에서 제어 센터(Control-Center: CC, 서비스 제공자와 터미널 사이의 그림 7의 오른쪽 참조)는 보안 메커니즘, 지불과 청구 메커니즘, 인증 메커니즘, 인간-기계 인터페이스 기능에 대한 접근 메커니즘 또는 표준화된 통신 메커니즘과 같은 플랫폼과 그것의 기능들에 대한 표준화된 접근을 제공한다.

많은 텔레매틱스 서비스는 GPS나 충돌 센서와

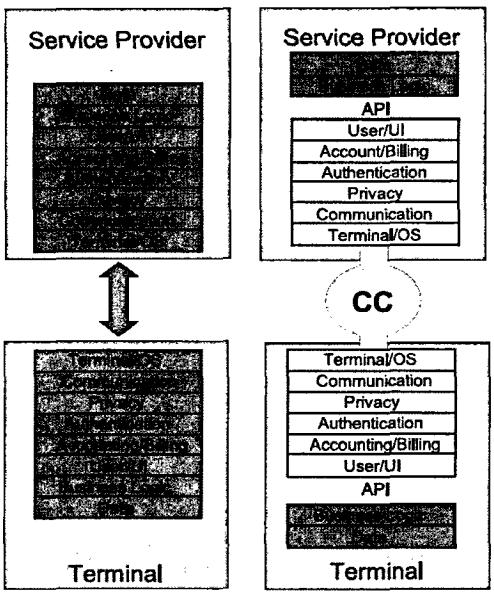

그림 7. GST API 방법

같은 차량 내 센서나 장치에 접근할 필요가 있다. 이러한 센서나 장치에 접근하는 방법은 차량 브랜드나 모델에 따라 크게 다르다. 또한 자동차 생산자는 이러한 시스템이나 차량 내 설치된 소프트웨어를 위한 CAN(Car Area Network) 또는 MOST (Media Oriented Systems Transport)와 같은 차량 내 망에 직접 접근을 허용하지 않는 대신 표준화된 API를 통해서만 접근이 제공된다.

소프트웨어와 서비스 제공자는 그것들의 응용과 서비스를 위한 비지니스 로직의 개발에 초점을 맞출 수 있는 반면 CC는 단지 응용과 서비스를 개발하고 관리하는 인스턴스이다. 어떤 차량 브랜드에 대한 전용 CC도 있으나 많은 브랜드와 모델에 대한 접근을 제공하는 CC 역시 이론적으로 가능하다.

GST 내의 개방 시스템 서브 프로젝트의 목적은 무단절 인터네트워킹을 설립하는 온라인 서비스에 대한 오픈 마켓을 위한 조건의 생성, 치명적인 사고의 횟수를 줄이는 안전 서비스의 설치, 그

리고 가치 체인의 서로 다른 참가자들이 새로운 기능 또는 서브시스템을 쉽게 개발하고, 구현하고, 설치하는 것을 허용하는 핵심 인터페이스를 표준화하여 오픈 텔레매틱스 시장의 생성이다 [24].

새로운 프로토콜을 발명하는 대신 GST 플랫폼은 이미 존재하는 입증된 표준화된 프로토콜을 사용한다. 통신은 SOAP 메시지[25]를 사용하여 수행되어지고, 소프트웨어 컴포넌트는 OSGI 플랫폼[26] 상에서 실행되고, 소프트웨어 컴포넌트의 설치와 유지보수는 SyncML-DM[27]에 기반하고, 식별 관리는 SAML[28]을 통해서 실행된다. 접근 정책들은 XACML[29]에 기반한다. SAML의 사용은 연합 식별 개념을 가지고 서비스 제공자와 전체 시스템에 대한 관리 오버헤드를 제한하면서 GST 플랫폼을 제공할 것이다. GST 보안 서브 프로젝트는 모든 서비스와 인터페이스가 신뢰성 있는 종단 간 보안과 보호되는 플랫폼 상의 프라이버시를 보장한다.

GST 프로젝트는 자동차-대-자동차 또는 자동차-대-인프라 구조 통신의 하나의 가능한 채널로 기존의 VANET 통신 시스템을 사용할 수도 있다. 따라서 VANET 통신 시스템의 보안 구조는 그러한 오픈 마켓의 일부분이 될 수도 있다.

4.2 상황 인식 소프트웨어 플랫폼

J. Sun은 스마트 승용차 환경에서 정보의 포괄적인 정의와 분류를 계층적 상황 모델을 제안하고, 하드웨어 인프라 구조와 소프트웨어 플랫폼을 포함하는 스마트 승용차 모형을 제시하였다[34].

스마트 승용차를 위한 상황 인식 소프트웨어 플랫폼은 그림 8과 같다. 그 플랫폼은 4가지 계층: 네트워크 계층, 브로커 계층, 상황 인프라 구조, 그리고 서비스 계층을 포함한다.

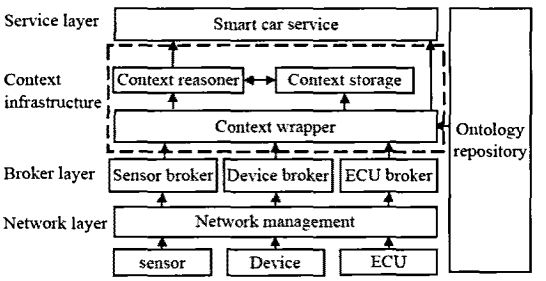

그림 8. 스마트 승용차를 위한 소프트웨어 플랫폼

4.2.1 네트워크 계층

스마트 승용차는 다른 통신 방법들을 지원한다. ZigBee 무선 센서망은 모든 소형 센서들을 연결한다. 스마트 차량 네트워크는 기계장치의 노드들 간의 통신을 위해 시리얼-버스 시스템이다. WLAN 802.11a/b/9 망은 디지털 장치들 간의 통신을 지원한다. CDMA 1xRTT 망은 광역 통신을 책임지고 있다.

4.2.2 브로커 계층

센서 브로커는 스마트 승용차에 추가된 새로운 센서들의 발견과 등록을 책임지고 있다. 하나의 브로커는 센서들의 하나의 범주를 관리한다. 센서들은 WLAN, 시리얼 포트, 이더넷, USB을 통하여 데이터를 전송할 수 있다. 그 브로커는 어떤 센서에 대한 광역적으로 유일한 주소 또는 인증을 할당하고, 갱신하는 주기를 명시하고, 그리고 데이터 전송을 위한 센서와 데이터 파스를 위한 시스템을 위한 방법을 정의한다. 장치 브로커는 새로운 장치 발견과 스마트 승용차에서 협동을 위해 장치들의 등록을 책임지고 있다. ECU(electronic control unit) 브로커는 프로세서들을 관리하고 특정 상황을 수집하는 것을 목표로 한다.

4.2.3 상황 인프라 구조

상황 인프라 구조는 3 부분: ① 센서 데이터를 시맨틱 상황 원자로 바꾸는 상황 래퍼(wrapper);

② 다양한 종류의 상황 원자들을 수집하여 상황을 학습하고 인식하는 상황 추론자; ③ 과거 상황을 위한 저장소와 질의 서비스를 제공하는 상황 저장 장치로 구성된다.

4.2.4 서비스 계층

스마트 승용차는 운전자들을 위해 더 안전하고 더 효율적이고 더 편리한 운전 환경을 생성할 것이다. 따라서 특정 서비스들이 개발되어야 한다. 스마트 승용차에서, 앞 차와의 거리가 안전 제한보다 짧을 때 감속과 같은 대부분 서비스들은 어떤 작동 장치를 제어하기 위하여 CAN을 통하여 신호의 전송을 요구한다. 서비스 실행을 위하여 서비스 API (application programming interface)와 매개변수를 포함하는 메시지가 작동장치를 관리하는 ECU에 전송되어야 한다. ECU는 그 메시지를 파스하고 제어 신호를 그것의 상태를 변경하기 위하여 작동 장치를 제어할 중계기에게 전송한다.

5. 결 론

차량 애드혹 망(VANETs)을 생성하기 위한 기술과 인프라 구조는 지금으로부터 10년 이내에 소개될 수 있을 것이다. VANETs에 의해 차량 간 정보의 교환은 협동 운전의 첫 번째 단계이고, 도로 상에서 더욱 안전을 위한 중요한 도구 중의 하나로 보인다. 의심할 나위 없이 안전은 VANETs의 중요하고 가장 유용한 응용이다.

상상되어진 VANETs에서, 현재 차량의 위치 탐색을 위하여 요구되는 위치기반 서비스는 거대한 프라이버시 문제를 제기할 수 있다. 본 논문에서는 VANETs에서 프라이버시 인식 컴포넌트를 포함하는 보안 구조가 소개되었다. 전통적인 보안 방법들은 응용계층이나 또는 데이터 채널과 같은 하나의 계층에만 초점이 맞추어 진다. 그러나 VANETs에서의 보안 측면은 교차 계층 문제이다. 분명하게 부정을 저지르는 악의 있는 행동을 하는 차량은 라우팅 계층에서 신뢰될 수 없어야 한다.

본 논문에서는 상황 인식, 텔레매틱스 서비스를 위한 오픈 플랫폼 내의 안전한 VANETs에 대한 연구를 소개하였다. 이것은 수많은 협력하는 비지니스 시나리오들과 승객들이 자신의 자동차에서 시간을 보내는 동안 개인적 활동과 비지니스 활동을 위한 협조 지원과 같은 승객을 위한 비안전 서비스를 가능하게 할 것이다.

참 고 문 헌

[1] The CarTALK project website. [Online]. Available: http://www.cartalk2000.net/

[2] The DSRC project website. [Online]. Available: http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[3] The Fleetnet project website. [Online]. Available: http://www.et2.tu-harburg.de/fleetnet/

[4] W. Franz, R. Eberhardt, and T. Luckenbach, "Fleetnet - internet on the road," in 8th World Congress on Intelligent Transportation Systems, Braunschweig, Germany, 2001.

[5] W. Franz, C. Wagner, C. Maihoefer, and H. Hartenstein, "Fleetnet: Plat-form for inter-vehicle communications," in 1th International Workshop on Intelligent Transportation, Hamburg, Germany, 2004.

[6] The Car2Car Communication Consortium website. [Online]. Available: http://www. car-to-car.org

[7] The PReVENT WILLWARN subproject website. [Online]. Available: http://www.prevent-ip.org/en/prevent_subprojects/safe_speedand safe_following/willwarn/

[8] The NOW project website. [Online]. Available:

http://www.network-on-wheels.de/

[9] The GST (Global System for Telematics) project website. [Online]. Available: http://www.gstforum.org/

[10] H. Hartenstein, H. Fuessler, and A. Festag. (2003, Nov.) The Fleetnet Demonstrator. [Online]. Available: http://www.et2.tu-harburg.de/fleetnet/pdf/ITS2003fleetnet2.pdf

[11] J.-P. Hubaux, S. Capkun, and L. Jun, "The security and privacy of smart vehicles," IEEE Security and Privacy, Vol.4, pp. 49-55, 2004.

[12] Y.-C. Hu, A. Perrig, and D. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in Proceedings of the 2003ACM Workshop on Wireless security, San Diego, CA, USA, 2003, pp. 30-40.

[13] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Mobile Computing and Networking, pp. 255-265, 2000.

[14] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in Mobile Computing and Networking, 2000, pp. 243-254.

[15] C. Perkins, "Ad-hoc on-demand distance vector routing," Nov. 1997.

[16] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications, 1994, pp. 234-244.

[17] W. Franz and C. Maihoefer, "Geographical addressing and forwarding in fleetnet," Mobile Computing and Networking, 2002.

[18] H. Fuessler, M. Mauve, H. Hartenstein, M. Kaesemann, and D. Vollmer, "A Comparison of Routing Strategies for Vehicular Ad Hoc Networks," Department of Computer Science, University of Mannheim, Mannheim, Tech. Rep. TR-3-2002, 2002.

[19] J. Li, J. Jannotti, D. S. J. DeCouto, D. R. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," in Proceedings of the sixth annual ACM/IEEE International Conference on Mobile computing and networking, Boston, Massachusetts, USA, 2000, pp. 120-130.

[20] M. Kaesemann, H. Fuessler, H. Hartenstein, and M. Mauve, "A reactive location service for mobile ad hoc networks," Department of Computer Science, University of Mannheim, Mannheim, Germany, Tech. Rep. TR-14-2002.

[21] W. Kiess, H. Fuessler, J. Widmer, and M. Mauve, "Hierarchical location service for mobile ad-hoc networks," in ACM SIGMOBILE Mobile Computing and Communications Review, 2004, pp. 47-58.

[22] The PReVENT project website. [Online]. Available: http://www.prevent-ip.org/

[23] T. Leinmueller, E. Schoch, F. Kargl, and C. Maihoefer, "Influence of Falsified Position Data on Geographic Ad-hoc Routing," in ESAS 2005, 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, 2005.

[24] The GST Open Systems subproject website. [Online]. Available: http://www. gstproject.org /os/index.php

[25] SOAP specification. [Online]. Available: http://www.w3.org/TR/soap/

[26] The OSGI alliance website. [Online]. Available: http://www.osgi.org/

[27] The SyncML website. [Online]. Available: http://www.syncml.org/

[28] OASIS Security Services (SAML) TC. [Online]. Available: http://www.oasis-open.org/committees/tc_home.php?wg abbrev=security

[29] The OASIS website. [Online]. Available: http://www.oasis-open.org/specs/index.php

[30] The GST Security subproject website. [Online]. Available: http://www.gstproject.org/sec/

[31] The e-Safety initiative website. [Online]. Available:http://europa.eu.int/information_society/activities/esafety/index_en. htm

[32] The EU Information Society Technologies framework program website. [Online]. Available: http://www.cordis.lu/ist/

[33] M. Schaefer, A. P. Karduck, "Secure and Open Market Platforms for Telematic Services," Proceedings of CollECTeR Europe 2005, June 2005

[34] J. Sun, Z-h. Wu, G. Pan, "Context-aware smart car: from model to prototype," Journal of Zhejiang University SCIENCE A, Vol. 10 No. 7 pp. 1049-1059, 2009.

오 선 진

- 1981년 한양대학교 공과대학(공학사)
- 1987년 미국 Wayne State University 컴퓨터과학과(이학사)
- 1989년 미국 University of Detroit 컴퓨터과학과(이학석사)
- 1993년 미국 Oklahoma State University 컴퓨터과학과(박사 과정)
- 1999년 曉聖 Catholic University 전자계산학과(이학박사)
- 1994년~2000년 선린대학교 컴퓨터정보학과 교수
- 2000년~현재 세명대학교 정보통신학부 교수
- 관심분야 : VANETs, MANETs, 센서 망, 스마트 응용 등

배 인 한

- 1984년 경남대학교 전자계산학과(공학사)
- 1986년 중앙대학교 대학원 전자계산학과(이학석사)
- 1990년 중앙대학교 대학원 전자계산학과(공학박사)
- 1996년~1997년 Department of Computer Science and Engineering, The Ohio State University(Post-Doc)
- 2002년~2003년 Department of Computer Science, Old Dominion University (Visiting Professor)
- 2009년~현재 Department of Computer Science, Old Dominion University (Visiting Professor)
- 1989년~현재 대구가톨릭대학교 컴퓨터정보통신공학부 교수
- 관심분야 : VANETs, MANETs, 센서 망, 스마트 응용, 미들웨어 등