교통안전통신에서 공공 프라이버시 확보 방안

박재복*, 박윤환*, 김현태**,조기환*
*전북대학교 전자정보공학부, **BK21 전북전자정보고급인력양성사업단
e-mail : {jbpark, yhpark, ghcho}@dcs.chonbuk.ac.kr

Achieving Public Privacy in VSC(Vehicle Safety Communication)

Jaebok Park*, Yoonhwan Park*, Hyuntae Kim**, Gihwan Cho*
*Div of EIE, Chonbuk University, **Advanced Graduate Education Center of JEIT-BK21

요 약

무선통신의 응용영역 확장으로 공공안전, 특히 교통안전 분야에서 운전자에게 제공되는 안전성과 편의성은 크게 증가한 반면에 정보보호 요구도 변화하고 있다. 본 논문은 교통안전 통신을 정보보호 관점에서 고유 특성을 분석하고, 특히 프라이버시 측면에서 위협요소를 정의하고 있다. 통신을 위한 계층구조에서 위협요소에 대응하는 프라이버시를 확보 방안을 제시하고 있다.

1. 서론

운행중인 차량이 앞차의 급정거 혹은 도로상의 장애물 등을 인지한 후 운전자가 브레이크를 작동하기까지 일반적으로 0.7-1.5 초의 반응 지연시간이 소요 되는 것으로 알려져 있다. 앞차의 급브레이크 사실을 운전자에게 미리 제공한다면 교통안전에 크게 도움이 될 것이다. OFCOM 조사에 따르면, 1 초를 선행하여 운전자가 교통 위험 요소에 대응할 수 있는 수단이 제공된다면 도로상에서 발생하는 후면 충돌 사고의 약 90%를 줄일 수 있다고 한다[1].

특히 다중 차량간에 연쇄추돌은 치명적인 인적, 재산상의 피해를 수반한다. 교통안전 통신(VSC: Vehicle Safety Communication)은 공공안전 성격의 교통 영역에 무선통신 기술을 확장, 적용하여 탄생한 미래형 교통안전의 기술이다. 교통 위험요소를 발견한 차량의 급브레이크 조작등에 수반하여 위험 알림 정보를 후위 차량에 전달하는 방식이다. 따라서 운전자의 시야를 가리는 대형 트럭, 교차로, 혹은 방향을 전환시 직면하게 될 교통 장애물 등 운전자의 인지 범위를 벗어나는 상황에서 운전자가 미리 인지/식별 범위와 능력을 유효하게 확장해주는 역할을 한다.

공공환경에서 운용되는 차량안전 통신이 실용적인 측면의 유효성을 확보하기 위해서는 보안성의 확보가 절대적이다. 본 논문에서는 특히 프라이버시 관점에서 위협요소를 분석하고 해결 방안을 제시한다.

2. 교통안전 통신에서 프라이버시 위협 요소

교통안전 통신은 교통안전에 관한 정보를 차량간(V2V) 혹은 도로상에 설비되어 있는 기반시설을(V2I) 매개로 이루어진다. V2V 는 추돌위험 알림과 같은 긴급정보의 전달에, V2I 는 V2V 의 전달 범위를 확장하거나 일반 정보 서비스 전달하기 위해서 주로 사용된다. V2V 구조의 차량간 통신 모델을 VANET(Vehicular Ad hoc NETwork) 구조로 정의된다.

VANET 에서 통신은 다양한 고유 특성으로 인하여 보안위협에 쉽게 노출된다. 무선매체 본래의 보안 취약성과 더불어, 고속으로 운행되는 차량들은 상호 위상변화가 심하고, 노드의 밀도가 수시로 변화한다. 또한 차량간에는 미리 설정된 관계나 보안신뢰를 가정할 수 없다. 특히 통신이 공공영역에서 이루어짐으로 인하여 Jamming, 메시지 변조, 차량의 추적등의 보안위협이 상대적으로 쉽고, 정보화 사회에 미치는 영향도 크다.

프라이버시 측면에서 현재는 차량의 번호, 모델, 색, 주행방향, 속도 등의 시각적으로 관측에 한정되어 있다. 즉, 해당 차량의 목적지, 경로, 탑승객의 이름이나 취향등을 가시적 한계로 인하여 추적이 매우 제한적이다. 반면에 교통안전 통신이 적용되면 다수 차량의 정확한 위치와 식별자, 경로 등의 프라이버시 정보를 다중 위치에서 획득, 분석이 가능해진다. 특정 차량의 추적 예는 다음과 같다.

① 10:20 분 서울기점 하행 25km 지점을 지남
② 10:30 분 서울기점 하행 40km 지점에서 인터넷으로 호텔예약
③ 10:50 분 천안 톨게이트 통과

통신 과정은 통신장치 혹은 사용자의 식별자가 필연적으로 요구되며, 식별자 노출은 특정 차량 혹은 사용자의 추적이 가능하여 교통안전 통신의 정착에 큰 걸림돌로 인식되고 있다. 교통안전 응용 정보에는 차량의 위치, 시간, 응용 서비스 등 운전자의 행위와 선호도 등의 개인정보가 포함되어 프라이버시에 큰 위협이 된다. 따라서 통신 정보는 암호화되어야 함은 물론 식별자의 익명성이 보장되어야 한다.

한편, 식별자의 익명화는 불법 행위자로 하여금 불법 사실을 은닉하는 심리적 기회를 제공한다. 특히 교통환경으로 다변화로 인하여 뺑소니등 불법행위 차량은

이 연구에 참여한 연구자는 2 단계 BK21 사업의 지원비를 받았음

사회적으로 큰 문제가 되고 있다. 즉 공공환경에서 사용되는 식별자는 법이 허용하는 범위에서 불법 행위자를 밝힐 수 있는 수단이 익명성과 동시에 제공되지 않으면 않된다. 이러한 교통안전 통신에서 사용되는 식별자의 이중적 특성을 조건부 익명성(Conditional Anonymity)라고 한다[4]. 즉, 교통안전 통신은 불특정 다수에 의해서 식별이 가능한 식별자는 최대한 익명성을 보장하되, 필요한 경우에는 특정 차량을 식별할 수 있는 수단이 제공되어야 프라이버시를 보장하는 공공안전 기술이 될 수 있다.

3. 프라이버시 확보 방안

인터넷 기반 통신구조에서 통신 주체간에 유일한 식별자는 IP 주소와 MAC 주소로 알려져 있다. 또한 차량은 차량번호와 VIN(Vehicle Identification Number) 그리고 소유자/사용자 이름 등이 차량 식별자로 사용될 수 있다. 프라이버시 확보를 위해서 본 논문에서는 통신 식별자는 필명(Pseudonym)으로 대치시키고, 차량 식별자는 암호화 함으로써 조건부 익명성에 접근을 제시한다.

교통안전 통신은 안전에 관한 정보를 전달하는 관계로 가능한 빨리 불특정 다수에게 전달되어야 한다. 따라서 브로드케스트 형태의 데이터 전달이 기본 통신 방법론으로 사용된다. 긴급상황 알림 메시지 등의 브로드케스트는 응답이 필요치 않는 통신 페러다임으로 송신자의 IP 주소와 MAC 주소는 필명의 적용이 가능하다. 필명은 지속적으로 사용하게 되면 정확한 식별자의 노출은 막을 수 있지만 동일한 통신장치를 사용한 차량으로 추정이 가능하다. 따라서 통신 식별자는 주기적으로 혹은 새로운 메시지를 전달할 때마다 새로운 갱신하여 사용해야 한다. VSCC(VSC Consortium) 규격에서도 익명성이 VSC 적용의 사회적 수용에 결정적인 요인으로 정의하고 MAC 주소의 주기적인 갱신을 권고하고 있다[5].

교통안전 응용 측면에서 VIN 은 차량의 고장등 차량관리 측면에서 사용되며, 소유자/사용자의 이름은 응용 프로그램에서 사용된다. 이들의 프라이버시 보호를 위해서는 적절한 암호화 기법의 적용이 필요하다. 통신 식별자와 유사하게 동일한 암호문을 지속적으로 사용하는 경우에 동일 차량을 추정하는 단서가 된다. 따라서 암호문 작성에 사용되는 키는 익명성을 갖도록 자주 갱신되어야 한다. 익명 키는 한번 사용되면 폐기되거나, 짧은 시간만 유효한 형태로 사용되어야 한다. 이를 위한 방안으로 통신이 발생할 때마다 임시 키를 생성하여 사용하거나, 미리 키 풀에 다수의 키를 확보하여 순서적으로 사용할 수 있다. 이때, 차량 정비업체나 응용 서버에서 임시키나 키 풀의 익명키를 해득할 수 있어야 한다. 공개 키 암호화 기법을 이용하는 경우에 키들은 CA(Certificate Authority)에 인증을 거쳐서 사용한다.

차량번호는 차량의 등록과정에서 부여된 공인된 유일한 차량 식별자이다. 따라서 법적인 범위에서 불법행위 차량을 식별하는 수단으로 사용될 수 있다. 참고문헌 [2]에는 전자번호판을 제시하고 있다. 전자번호판은 Public Key 암호화 기법에서 인증서와 유사한 것으로 차량의 등록시 부여되며, 경찰서와 같은 기관에서만 해독이 가능하다. 전자번호판이 가장 유효하게 적용되는 시나리오는 뺑소니 차량의 검거를 들 수 있다. 각 차량은 주기적으로 자신의 전자번호판을 브로트케스트해야 하며, 또한 주변에서 송출되는 전자번호판을 기록하는 의무를 지닌다. 따라서 불법행위 차량 주변의 차량들은 자연스럽게 익명성 감시(Anonymous Watchdog)을 수행하여 추후에 불법행위의 검증에 유효하게 사용될 수 있다.

<표 1> VSC 프라이버시 확보 방안

계층	익명성 요소	확보 방안	적용
응용	전자번호판	공인인증서	식별자확인
	VIN, 사용자	익명키 암호	익명성확보
라우팅	IP 주소	임시주소	익명성확보
MAC	MAC 주소	임시주소	익명성확보

<표 1>은 VSC 에서 프라이버시 확보를 위해 적용되는 익명서 요소와 확보방안을 보이고 있다. 통신 프로토콜 계층 구조에서 MAC 과 라우팅 계층은 장치의 식별자로 사용될 수 있다. 응답이 요구되지 않는 브로드케스트 통신에서는 식별자로써 의미가 없으므로 임시주소를 사용한다. 응용 계층은 공공 환경에서 불법행위자를 감시와 차량관리 및 정보서비스와 같은 인터넷 응용으로 구분될 수 있다. 이들은 기반구조를 전제로 구성되므로 공개키 암호화 기법의 틀 범위에서 프라이버시를 보호하는 방안이 유효할 것이다.

4. 결론

현재 혹은 미래 생활에서 교통환경은 중요한 공공안전의 기저를 이룰 것으로 예상된다. 교통안전에 무선통신 기술의 적용은 프라이버시 보호에 새로운 해석과 방안이 필요하다. 본 논문에서 교통안전 통신에 유효한 프라이버시 보호를 위한 기본 방향을 제시하고 있으며, 추후에 구체적인 방법론의 체계화가 필요하다.

참고문헌

[1] 유석대, 조기환, “교통사고 방지를 위한 차량간 통신기술,” 한국통신학회 학회지, 23 (2), pp. 79-90, 2006. 2.

[2] J. Hubaux, S. Capkun and L. Luo, “The Security and Privacy of Smart Vehicles,” *IEEE Security & Privacy*, pp. 49-55, May 2004

[3] T. Leinmuller, *et al*., “Intrusion Detection in VANETs,” *Proc. on SEVECOM* June 2006

[4] M. Raya, P. Papadimitratos, J. Hubaux, “Securing Vehicular Communications,” *IEEE Wireless Comm. Magazine,* 13(5), pp. 8-15, Oct. 2006

[5] M. Zimmer, “Personal Information and the Design of Vehicle Safety Communication Technologies : an Application of Privacy as Contextual Integrity,” *Ph.D proposal in New York Univ.,* Apr. 2005