VANET 환경에서 위치 프라이버시를 제공하는 보안 라우팅 프로토콜

김효*, 오희국*, 김상진**
*한양대학교 컴퓨터공학과
**한국기술교육대학교 인터넷미디어공학부
e-mail: hkim@infosec.hanyang.ac.kr, hkoh@hanyang.ac.kr, sangjin@kut.ac.kr

A Secure Routing Protocol to Provide Location Privacy in VANET

Hyo Kim*, Sangjin Kim**, Heekuck Oh*
*Dept of Computer Science and Engineering, Hanyang University
**School of Internet Media Engineering, Korea University of Technology and Education

요 약

VANET(Vehicle Ad-hoc Network) 환경은 도로위의 차량을 노드로 하여 구성하는 애드혹 네트워크로써 최근 들어 그 연구가 활발히 진행되고 있는 분야이다. 일반적인 애드혹 환경과 마찬가지로 VANET 환경에서도 보안적인 문제가 중요한 이슈로 대두되고 있다. VANET 환경에서 가장 중요하게 요구되는 보안요소는 차량의 익명성을 통한 위치 프라이버시와 협력 운전(cooperative driving) 단계에서 사용되는 메시지에 대한 인증, 무결성, 부인방지 등이다. 본 논문에서는 익명 아이디(pseudonym), 그룹화 등을 통해 차량의 위치 프라이버시를 제공하고 또한 이를 이용해 VANET 환경에서 사용할 수 있는 라우팅 프로토콜을 제안하고자 한다. RA(Registration Authority)에서 발급되는 익명 아이디의 집합과 차량의 전송 범위를 고려해서 구성되는 그룹화는 그룹에 속한 차량에 대해 익명성을 제공하고, 또한 그룹리더에 의해 생성되는 그룹키를 통해 효율적인 협력 운전 메시지 전달을 할 수 있게 된다. 그리고 각각의 그룹리더를 라우터로 이용해 전달되는 라우팅 프로토콜은 노드가 매우 유동적으로 움직이는 VANET 환경에서 효과적으로 메시지를 전달할 수 있도록 해줄 것이다.

1. 서론

최근 ITS(Intelligent Transport System)의 연구 개발이 활발히 진행되면서 지능형 차량에 대한 연구 역시 가속화되고 있다. VANET은 이러한 지능형 차량을 통해 이용할 수 있는 하나의 서비스로써 도로 위의 차량을 노드로 하여 구성하는 애드혹 네트워크라고 할 수 있다. VANET에서 운전자에게 제공할 수 있는 서비스는 각 차량이 안전에 관한 정보가 담긴 메시지(위치, 속도, 가속도, 방향 등)를 주기적으로 , 주변 차량에 알리는 협력 운전, RSU(Road Side Unit)에서 무선망을 통해 차량으로부터 정보를 수집해 다른 차량에게 도로 상황이나 흐름 등을 알려주는 차량 정보 수집(Probe vehicle data) 서비스, 차량의 요청을 받아 위치에 관련된 서비스를 제공하는 위치 기반 서비스(LBS; Location Based Service) 등 여러 가지가 있다. 현재는 거의 모든 지역에서 차량의 사용이 필수적이므로 VANET 환경을 이용한 응용 서비스는 앞으로도 계속 개발될 전망이다.

VANET은 그 서비스의 특성상 애드혹과는 달리 통신의 종류를 V2V(Vehicle to Vehicle)와 V2I(Vehicle to Infrastructure)의 두 가지로 분류하고 있다. 말 그대로 V2V는 앞서 언급되었던 협력 운전과 같이 차량과 차량 사이의 통신을 말하며, V2I는 차량 정보 수집, LBS처럼 차량과 도로 주변의 기반 시설들과의 통신을 말한다. VANET 환경에서 차량을 운전하는 사용자는 이와 같은 서비스들을 통해 보다 안전하고 편리하게 이동할 수 있다. 그러나 한 번의 사고가 큰 재해로 이어지는 환경의 특성상 VANET의 서비스들은 조금이라도 잘못된 정보가 오고 갈 시, 자칫 돌이킬 수 없는 상황을 만들어낼 수도 있다. 즉, 차량과 차량 사이, 혹은 차량과 기반 시설 사이의 통신에서 메시지가 조작되거나 악용되어 사용되지 않도록 보안을 만족시켜주는 것이 매우 중요하다. 현재 국내외적으로 이를 위해서 다양한 보안 기술을 연구 및 개발하고 있지만, 대부분 아직 초기 단계에 머물러 있다[1].

본 논문에서는 익명 아이디(pseudonym), 차량의 그룹화를 이용해 VANET 환경에서 중요한 보안 요소인 위치 프라이버시를 보장하는 보안 라우팅 프로토콜을 제안하고자 한다. 본 논문은 다음과 같이 구성된다. 2장에서는 VANET 환경에서의 보안 위협과 보안 요소에 관해 알아보도록 하

* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성・지원사업의 연구결과로 수행되었음.

† 주저자, hkim@infosec.hanyang.ac.kr
hkoh@hanyang.ac.kr
‡ 교신저자, sangjin@kut.ac.kr

고, 3장에서는 제안하는 프로토콜의 시스템 모델을 설계하도록 한다. 4장에서는 제안하는 보안 라우팅 프로토콜에 대해 자세히 설명하고, 5장에서는 제안하는 프로토콜의 보안 분석을 한 후에 6장에서 결론을 맺고 마치도록 한다.

2. VANET 환경에서의 보안

2.1. VANET 공격 모델

VANET 환경은 최근 연구되고 있는 기술이 접목된 새로운 환경인만큼, 새로운 공격 모델이 계속 제안되고 있다[2][3].

(1) 정보 위조: 협력 운전 등의 응용에서 가짜 정보를 주변에 확산시켜 다른 운전자들의 이동에 영향을 주는 공격이다. 예를 들어 다른 도로의 소통이 잘 되고 있다는 거짓 정보를 흘려 현재 공격자가 있는 도로의 소통을 원활하게 만들어 공격자가 이동을 편하게 할 수 있도록 한다.

(2) 센서 정보 조작: 다른 차량이나 RSU의 정보를 조작해 다른 차량이 현재 공격자의 위치, 속도, 방향 등을 잘못 인식하도록 만드는 공격. 이는 후에 사고가 일어났을 때 책임회피로 이어질 수 있다.

(3) 신원 노출: 특정 신원 차량의 위치를 파악해 추적한다. 이 공격은 위치 프라이버시를 위협하는 공격으로써 사용자의 납치, 차량 도난 등의 범죄로 이어질 수 있다.

(4) 숨겨진 차량 공격(Hidden vehicle): 이 공격은 VANET 환경에서 차량의 메시지 전송이 브로드캐스트 된다는 점을 이용한 공격이다. VANET 환경에서 차량은 사고가 발생했을 때 주변으로 위험 메시지를 보내게 되는데, 메시지를 받은 공격자가 뒤따라오는 차량에 메시지를 전달하지 않아서 2차, 3차의 사고를 초래한다.

(5) 기타 애드혹 네트워크의 공격 모델: VANET은 기본적으로 애드혹 네트워크를 기반으로 하기 때문에 애드혹 네트워크에서 알려진 공격 모델을 거의 적용할 수 있다.

2.2. VANET 보안 요구사항

VANET에서는 다음과 같은 보안 요구사항이 존재한다[2].

(1) 인증: 메시지의 원천지를 인증하고 타당한 원천지일 경우에만 그에 따른 반응을 한다.

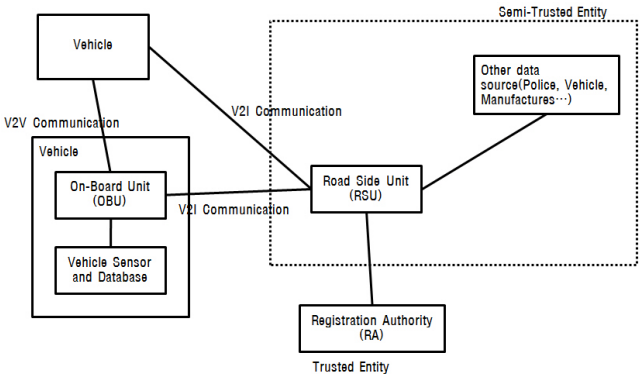
(2) 무결성: 데이터가 중간에 조작되지 않았는지 확인할 수 있어야 한다.

(3) 부인방지: 사고 차량 등이 보낸 책임 관련 메시지는 부인방지가 필요하다. 이 요구사항이 보장되지 않는다면 후에 책임 회피로 이어질 수 있다.

(4) 위치 프라이버시: VANET에 참여하는 차량에 대해 특정 차량의 위치를 알 수 없도록 보장되어야 한다. 또한 유사시 권한을 가지는 기관에서 차량의 위치에 대한 확인이 가능해야 한다.

3. 시스템 모델

일반적으로 VANET 환경에서 차량은 OBU(On-board Unit)을 탑재한다[4]. 이는 다른 차량 혹은 기반 시설과의 통신을 위한 장비이다. 또한 각 차량은 RA에 차량을 등록하고 전자 번호판을 부여받는다. 이는 ID와 같은 역할을 한다. RSU는 도로 주변에 있는 신호등, 도로 표지판 등과 같은 곳에 장치되어 차량에 서비스를 제공하며 모든 RSU는 RA에 유선으로 연결된다. 그림 1은 차량과 RSU, 그리고 RA의 연관 관계를 도식화 한 것이다.



(그림 1) 시스템 모델

4. 제안하는 방법

4.1. 가정

본 논문에서 제안하는 프로토콜은 다음과 같은 가정을 갖는다.

(1) 각 차량은 RA에 등록되어 있으며, RA에게 부여받은 공개키와 자신이 생성한 개인키를 갖는다. 공개키는 VANET에 참여하는 모든 차량이 공유하고 있다.

(2) 각 차량은 RA에게 부여받은 익명 아이디의 집합을 갖는다.

4.2. 표기법

표 1은 본 논문에서 사용되는 표기법을 설명하고 있다.

<표 1> 표기법

표기	설명
M	메시지
P_n	n번째 익명 아이디(pseudonym)
T_a	a가 생성한 타임스탬프
N_a	a가 생성한 난스(nonce)
$\{\}_K$	키 K로 암호화
$h()$	일방향 해쉬 함수
$MAC_K()$	키 K로 확인할 수 있는 MAC함수
K	대칭키
$+K_a$	a의 공개키
$-K_a$	a의 개인키
V	차량
V_{GL}	그룹리더차량
RA	RA(Registration Authority)

4.3. 제안하는 보안기법

4.3.1. 그룹화

차량은 익명성을 통한 위치 프라이버시의 보장을 위해 그룹화를 하게 된다. 그룹은 차량의 전송가능범위보다 작은 수를 반지름으로 하는 원형의 셀로 구분하며 그룹을 대표하는 그룹리더 V_{GL}을 갖는다. 그룹리더는 주기적으로 그룹키 K_G를 생성하여 RA에 등록하고 그룹에 속한 차량들에게 분배한다. 그 방법은 다음과 같다.

(1) RA에 그룹키 K_G 등록

$$V_{GL} \rightarrow RA : \{K_G, N_{GL}, P_{n+1}\}_{+K_{RA}}$$

$$RA \rightarrow V_{GL} : \{N_{GL}+1\}_{K_G}$$

그룹리더는 그룹키와 난스, 그리고 자신의 현재 익명 아이디의 다음 익명 아이디를 RA의 공개키로 암호화해서 RA에게 보낸다. 메시지를 받은 RA는 이를 복호화 하고 익명 아이디를 통해 그룹리더가 보냈음을 인증한다. 그 후 얻은 그룹키 K_G를 이용해 난스를 암호화 한 뒤 그룹리더에게 확인 메시지를 전송한다.

(2) 그룹에 속한 차량들에게 갱신된 그룹키 K_{G+1} 분배

$$V_{GL} \rightarrow RA : \{K_{G+1}, N_{GL}, P_{n+1}\}_{+K_{RA}}$$

$$RA \rightarrow V_{GL} : \{\{\{K_{G+1}, T_{RA}\}_{K_G}\}_{-K_{RA}}, N_{GL}\}_{+K_{GL}}$$

$$V_{GL} \rightarrow * : \{\{K_{G+1}, T_{RA}\}_{K_G}\}_{-K_{RA}}$$

그룹리더는 RA에게 갱신된 그룹키를 난스, 다음 익명 아이디와 함께 RA의 공개키로 암호화해서 보낸다. RA는 익명 아이디를 통해 그룹리더가 보냈음을 인증하고 다음 그룹키, 타임스탬프를 이전 그룹키로 암호화 한 메시지에 자신의 개인키로 서명한 것과 그룹리더가 보낸 난스를 함께 그룹리더의 공개키로 암호화 한 후 보낸다. 메시지를 받은 그룹리더가 그 내용을 확인한 뒤 RA의 서명이 된 부분을 그룹에 속한 차량들에게 브로드캐스트 한다.

(3) 협력 운전

그룹에 속한 차량은 그룹 안에서 협력 운전에 관한 메시지를 브로드캐스트 하며, 그 메시지 내용은 다음과 같다.

$$V \rightarrow * : \{M, P_n, T_v\}_{K_G}, MAC_{K_G}(M, P_n, T_v), h(P_{n+1})$$

협력 운전에서 필요한 보안 요소는 메시지 인증과 무결성, 그리고 부인방지이다. 그룹에 속한 차량들은 그룹키를 이용해 자신이 그룹에 속한 정식 일원임을 인증하고 MAC값을 통해 무결성을 보장한다. 다음 익명 아이디를 해쉬한 값은 후에 부인방지를 보장하게 된다. 익명 아이디는 메시지를 전송하고 나면 다음 익명 아이디로 갱신한다. n개의 익명 아이디를 RA에게 받았을 경우 현재 익명 아이디가 $n-1$번째일 때 RA에게 새로운 익명 아이디 집합을 부여받는다.

(4) RSU의 정보 수집

RSU는 도로의 정보를 수집하고 분석하기 위해 차량에 현재 도로의 정보를 요청한다. 여기에는 모든 차량이 답하지 않고 그룹리더만이 요청에 응하게 된다. 요청에 응하는 방법은 다음과 같다.

$$RSU \rightarrow V_{GL} : \{request\_message, N_{RSU}\}_{K_G}$$

$$V_{GL} : K_{RL} = F(K_G \,||\, P_{n+1})$$

$$V_{GL} \rightarrow RSU : \{M, N_{RSU}\}_{K_{RL}}, MAC_{K_{RL}}(M, N_{RSU})$$

RSU가 그룹리더에게 요청을 하면 그룹리더는 RA와 그룹리더의 세션키 K_{RL}을 생성한 후, 이 세션키를 이용해 도로 정보를 암호화해서 보내게 된다.

(5) 그룹 참여 및 탈퇴

최초에 그룹에 속하지 못한 차량은 자신의 주변으로 그룹 참여 의사를 브로드캐스트 한다. 일정 시간이 지나도 응답이 돌아오지 않으면 그 차량이 하나의 그룹리더가 되어 또 다른 차량의 참여를 기다리게 된다. 주변에 그룹이 존재해 응답이 돌아오면 참여를 원하는 차량은 다음의 과정을 통해 그룹에 참여하고 그룹키를 받는다.

$$V \rightarrow V_{GL} : join\_request \,||\, P_n$$

$$RA \rightarrow V : \{\{K_G, T\}_{-K_{RA}}\}_{+K_V}$$

요청을 받은 그룹리더가 이를 RA에 전달하면 RA는 익명 아이디를 확인하고 이 차량이 정상적인 참여자임을 그룹리더에게 알린다. 그 후 RA는 참여 차량의 공개키로 그룹키를 암호화 해 참여 차량에게 전달하게 된다.

그룹에 속한 차량이 그룹의 범위를 벗어나 탈퇴를 하게 되면 그룹리더는 그룹키를 갱신하고 이를 RA와 그룹에 속한 차량들에게 재분배한다.

4.3.2. 라우팅

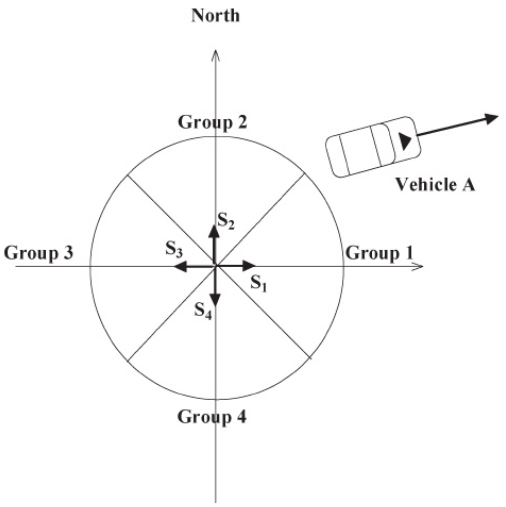
VANET 환경에서 라우팅은 가장 많이 연구되고 있는 분야 중 하나이다. VANET을 구성하는 노드의 특성상 라우팅 경로가 매우 유동적으로 바뀔 수 있으므로 그에 알맞은 라우팅 프로토콜이 필요하기 때문이다. 본 절에서는 T. Taleb 등이 제안한 VANET 환경에서의 라우팅 프로토콜[5]에서 경로 탐색 방법을 설명하고 이를 적용한 보안 라우팅 프로토콜을 제안한다.

4.3.2.1. 위치벡터를 이용한 그룹화 기법

그림 2는 [5]의 그룹화 기법을 도식화 한 것으로, 2차 평면에서 각 방향의 단위벡터와 차량의 위치벡터를 내적해서 그 스칼라 값이 가장 큰 방향의 번호를 그룹 번호로 하고, 그룹 번호가 같은 차량을 같은 그룹으로 보는 방법을 설명하고 있다. 즉, 위치벡터가 다른 차량들은 차량이 향하는 방향이 달라 라우팅 경로가 깨질 확률이 높으므로 방향이 비슷한 차량들끼리 그룹으로 묶어 라우팅 경로를 구성한다는 것이 [5]의 주된 내용이다.

4.3.2.2. 보안 라우팅 프로토콜

본 논문의 그룹화는 셀 단위로 이루어지고, 그룹 안에서의 메시지 전달은 그룹키를 통해 안전하게 진행된다. 그



(그림 2) 벡터를 통한 차량 그룹화

러나 그룹키는 그룹 내에서만 사용되므로 서로 다른 그룹에 있는 차량들의 통신은 어렵다. 따라서 그룹 간 통신의 경우, [5]의 방법에 따라 라우팅 그룹을 나누고, 그룹리더를 통해 목적 차량에 메시지를 전송할 수 있는 방법을 제안한다.

$$V : K_{VR} = F(K_G \,||\, P_{n+1})$$

$$V \rightarrow V_{GL} : \{M, T_V, P_n, P'_n\}_{K_{VR}}, P_n, P'_n$$

$$V_{GL} \rightarrow V'_{GL} : \{M, T_V, P_n, P'_n\}_{K_{VR}}, P_n, P'_n$$

$$V'_{GL} \rightarrow RA : \{M, T_V, P_n, P'_n\}_{K_{VR}}, P_n, P'_n$$

$$RA \rightarrow V' : \{\{M, T_V, P_n, P'_n\}_{-K_{RA}}\}_{+K_{V'}}$$

위의 방법은 위치 프라이버시를 위해 그룹 멤버 대신 그룹리더가 메시지를 대신 전달하는 방식이다. 메시지를 전송하는 차량은 RA만이 알 수 있는 키를 만들어서 메시지를 보호하므로, 각각의 그룹리더들은 이를 전달하는 역할만 할 수 있을 뿐, 메시지의 내용이나 전송자의 위치 및 신상 정보를 알지는 못한다. 메시지가 대상 차량이 있는 그룹의 그룹리더에게 전달되면 그룹리더는 RA를 통해 메시지를 복호화하고 대상 차량에게 전달하게 된다.

5. 보안 분석

본 논문에서 제안하는 방법은 기본적으로 익명 아이디의 집합을 사용하기 때문에 차량의 위치 프라이버시를 보장하게 된다. 익명 아이디는 익명성을 제공한다는 특징 외에도 앞으로 사용될 아이디를 해당 차량과 RA만이 알고 있다는 특징을 갖는다. 본 논문에서는 이를 이용해 안전한 메시지 교환을 하게 된다. 만일 차량에 사고가 발생하게 되면 협력 운전에 사용된 메시지를 조사할 수가 있는데, 이때 책임을 회피하고자 메시지에 대해 부인하는 경우가 발생할 수 있어서 협력 운전에 사용된 메시지는 부인방지가 필수적인 보안 사항으로 요구된다. 본 논문에서 제안하는 방법은 다음 익명 아이디의 일방향 해쉬 값을 붙여서 이를 보장했다. 또한 RSU의 정보 수집 및 차량 간 라우팅에서는 다음 익명 아이디를 이용해 키를 만들기 때문에 결과적으로 해당 차량과 RA 간에 대칭키를 공유할 수 있도록 했다.

6. 결론

본 논문은 VANET 환경에서 사용될 수 있는 어플리케이션의 보안 요구사항을 분석해 이를 보장하는 방법을 제안했다. 제안하는 방법은 익명 아이디 집합과 차량의 그룹화를 통해 차량의 위치 프라이버시를 보호하고 안전한 통신 및 유사시 메시지의 부인방지를 보장한다. 또한 [5]에서 제안된 방향벡터를 이용한 라우팅 기법을 이용해 안전하게 메시지를 전달할 수 있는 방법을 제안했다. 향후 우리는 설치비용이 큰 RSU를 이용하지 않고 V2V만을 이용한 보안 및 라우팅을 할 수 있는 방법에 대해 연구를 진행할 것이다.

참고문헌

[1] 최병철, 한승완, 정병호, 김정녀, “지능형 차량 보안 기술 동향,” ETRI 전자통신동향분석, vol. 22, no. 1, pp. 114-118, 2007.

[2] M. Raya and J. P. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, vol. 15, pp. 39-68, 2007.

[3] M. Raya, P. Papadimitratos and J. P. Hubaux, "Securing Vehicular Communications," IEEE Wireless Communications, vol. 13, no. 5, pp. 8-15, 2006.

[4] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust Location Privacy Sheme for VANET," IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1569-1589, 2007.

[5] T. Taleb, E. Sakhaese, A. Jamalipour, K. Hashimoto, N. Kato and Y. Nemoto, "A Stable Routing Protocol to Support ITS Services in VANET Networks," IEEE Transaction on Vehicular Technology, vol. 56, no. 6, pp. 3337-3347, 2007.