VANET 환경에서 위치 프라이버시를 보장하는 보안 프로토콜†

김효*, 오희국*
*한양대학교 컴퓨터공학과
e-mail: hkim@infosec.hanyang.ac.kr, hkoh@hanyang.ac.kr

A Security Protocol Providing Location Privacy in VANET

Hyo Kim*, Heekuck Oh*
*Dept of Computer Science and Engineering, Hanyang University

요 약

VANET(Vehicle Ad-hoc Network)은 통신 기능을 지원하는 지능형 차량들로 이루어진 애드혹 네트워크 환경으로써 최근 들어서 그 연구가 매우 활발하게 진행되고 있는 분야이다. VANET은 원활한 교통 소통, 사고 방지 등 여러 가지 편리한 기능들을 제공하지만, 그 기반을 애드혹 네트워크에 두고 있기 때문에 애드혹 네트워크에서 발생할 수 있는 보안 문제가 그대로 발생하며, 또한 그 환경적 특성에 따라 추가적인 보안 요구사항 역시 존재한다. VANET 환경에서 가장 중요하게 요구되는 보안요소는 협력 운전(cooperative driving) 시 메시지 인증, 무결성, 부인방지 등과 특정 차량에 대한 추적을 할 수 없도록 하는 위치 프라이버시 보호이다. 그러나 이 가운데 사용자의 위치 프라이버시는 조건적으로 신뢰기관에 의한 추적 역시 가능해야 한다는 조건을 포함한다. 본 논문에서는 L. Martucci 등이 제안한 자체적으로 생성하고 인증하는 pseudonym 기법[1]을 이용하여 이러한 보안 요구사항들을 만족시키는 방법을 제안하고자 한다. 제안하는 기법은 최초 차량 등록 시 받은 비밀 인자를 이용하여 보안 통신을 하며 추가적으로 신뢰 기관으로의 통신이 필요하지 않는 효율적인 보안 기법이다. 또한 기존 연구에서 발생했던 저장 공간의 문제, RSU(Road Side Unit) 접근 문제 등을 해결한다.

1. 서론

최근 ITS(Intelligent Transport System)의 연구가 각 분야별로 활발하게 진행됨에 따라 차량에 통신 기능을 추가한 지능형 차량에 대한 연구 역시 여러 연구기관 및 기업들을 주축으로 심도 있게 논의되고 있다. VANET은 이러한 지능형 차량들을 이용하여 구축된 애드혹 네트워크로써 여러 방향으로 활용될 수 있는 가능성을 갖고 있다. 이 가운데 대표적인 어플리케이션으로 차량들이 주기적으로 자신의 운행 정보(방향, 속도, 가속도, 차량 위치 등)을 주변에 전파하여 도로에서 발생할 수 있는 사고 등을 예방하는 협력 운전을 들 수가 있다. 또한 이 외에도 RSU에서 무선망을 통해 차량으로부터 정보를 수집하고 이 수집한 정보를 통해 주변 도로의 상황을 다른 차량에 알려 도로 소통을 원활하도록 하는 차량 정보 수집(Probe vehicle data) 서비스, 현재 위치에 관련된 정보를 제공하게 되는 위치 기반 서비스(LBS, Location Based Service) 등이 VANET 환경의 주요 어플리케이션으로 연구되고 있다.

† 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성·지원사업의 연구결과로 수행되었음.

VANET은 기본적으로 통신의 종류를 차량 간 통신인 V2V(Vehicle to Vehicle)와 차량과 기반 시설과의 통신인 V2I(Vehicle to Infrastructure)로 나누고 있다. VANET에 참여하는 차량들은 이와 같은 통신 기법을 이용하여 여러 응용 서비스를 제공받아 안전하고 쾌적한 운행을 할 수 있다. 그러나 한 번의 사고가 큰 재해로 이어지는 환경의 특성상 VANET의 서비스들은 조금이라도 잘못된 정보가 교환될 시, 자칫 돌이킬 수 없는 상황을 유발할 수도 있다. 즉, V2V 및 V2I 통신에서 참여 노드들의 정보가 조작되거나 악용되지 않도록 보안 사항을 만족시켜주는 것이 매우 중요하다. 현재 국내외적으로 이를 위해서 다양한 연구가 진행되고 있지만, 대부분 아직 시작 단계에 머물러 있는 실정이다[2][3].

본 논문에서는 차량이 자체적으로 생성하고 인증하는 pseudonym을 통해 VANET에서 필요한 보안 요구사항을 만족하는 방법을 제안한다. 본 논문은 다음과 같이 구성된다. 2장에서는 VANET 환경의 보안 요구사항과 그에 따라 기존에 제안된 기법들과 그 문제점을 살펴보고, 3장에서는 본 논문에서 제안되는 기법에 사용될 pseudonym 자체 생성 기법을 설명한다. 4장에서는 이를 VANET에 적용한 보안 기법을 제안하고 이어서 5장에서는 제안된 기법의 보안 분석을 한다. 그리고 6장에서 결론을 맺으며 마치도록 한다.

2. 관련 연구

2.1. VANET 보안 요구사항

VANET 환경에서는 다음과 같은 보안 요구사항이 존재한다[2][4].

·인증: 메시지의 원천지를 인증하고 타당한 원천지일 경우에만 그에 따른 반응을 한다.

·무결성: 데이터가 중간에 조작되지 않았는지 확인할 수 있어야 한다.

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

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

2.2. 기존에 제안된 방법

VANET 환경의 보안 요구사항을 만족시키기 위한 방법으로 여러 가지 기법이 소개되었다. 이 기법들은 크게 pseudonym의 집합을 이용하는 방법, 신원기반 공개키 암호화 기법을 이용하는 방법, 그룹서명 기법을 이용하는 방법 등 세 가지로 나눠볼 수 있다.

2.2.1. Pseudonym의 집합을 이용한 방법

[5][6]에서는 VANET에 참여하는 차량이 신뢰 기관으로부터 pseudonym의 집합과 그에 따른 개인키 및 인증서의 집합을 부여받아 사용하는 방법을 소개하고 있다. 이들 방법에서 차량은 pseudonym을 이용해 익명성을 보장받고 그에 따른 개인키로 메시지의 인증 문제를 해결한다. 차량은 pseudonym을 메시지마다 갱신하여 사용하고 소진 시 다시 신뢰기관에 접속하여 새로운 집합을 부여받는다.

2.2.2. 신원기반 공개키 암호화 기법을 이용한 방법

[7][8]은 차량의 최초 등록 시 신뢰기관으로부터 인자를 부여받아 신원기반 공개키 암호화 기법을 이용하여 메시지 인증 및 위치 프라이버시를 보호하는 방법을 소개한다.

2.2.3. 그룹서명 기법을 이용한 방법

[9][10]은 그룹서명 기법을 이용한 VANET 보안 프로토콜을 제안한다. 그룹서명은 사용자 각자의 그룹서명키와 그룹이 갖는 하나의 그룹공개키를 이용하여 메시지에 대한 서명 및 확인을 할 수 있는 기법으로 익명성을 보장하면서 서명을 확인할 수 있다는 장점을 갖는다.

2.3. 기존 방법들의 문제점

기존에 발표된 방법들은 모두 VANET 환경의 보안 요구사항인 인증, 데이터 무결성, 부인방지, 위치 프라이버시 등을 보장하고 있다. 그러나 VANET이라는 환경의 특수성에 의해 각각의 방법들이 문제점을 갖는다.

2.2.1에서 설명한 방법은 모든 노드에게 pseudonym의 집합과 그에 따른 개인키 및 인증서의 집합을 저장할 저장 공간이 필수적으로 필요하게 된다. 또한 신뢰 기관 역시 이 집합들과 노드의 매핑 정보를 갖고 있어야 유사시 차량 추적을 할 수 있으므로 추가적인 저장 공간이 필요하다. 그리고 차량은 pseudonym의 보충을 위해 RSU에 접근해야 하는 일이 발생하는데, 설치에 많은 비용이 소모되는 RSU는 차량이 필요로 할 때마다 통신 반경 안에 있을 것이라는 보장이 없기 때문에 이 기법 자체는 현실적이지 못하다. 2.2.2에서 설명한 신원기반 공개키 암호화를 이용한 기법은 pseudonym의 집합을 이용하는 기법과 마찬가지의 문제점이 존재한다. 어차피 신원기반 공개키 암호화를 하더라도 익명성을 위해 pseudonym을 사용해야 하며, 이를 위해서는 저장 공간 및 RSU 접근이 필요하게 된다. 2.2.3에서 설명한 그룹서명 기법을 이용한 방법은 익명성을 보장하면서도 조건적인 위치 프라이버시 보장이 가능하며, 비연결성, 무결성, 인증 등이 제공된다는 점에서 이론적으로 VANET 환경에 알맞은 방법이라고 생각할 수 있다. 그러나 그룹서명의 가장 큰 문제인 탈퇴 노드의 제어 문제와 수많은 차량이 하나의 그룹공개키를 사용한다는 점에서 범위 설정의 문제점이 존재한다.

우리는 이와 같은 문제점을 해결하기 위해 pseudonym을 사용하되, 저장 공간 및 RSU로의 접근이 필요하지 않는 기법을 사용하여 VANET 환경의 보안 요구사항을 충족시키고자 한다.

3. L. Martucci 등의 자체 인증 pseudonym 기법

L. Martucci 등은 노드가 최초 등록 시 부여받은 인자값을 이용해 자체적으로 공개키 및 개인키와 pseudonym을 생성하고 이에 따른 인증서를 발급하여 통신할 수 있는 기법을 제안했다.

3.1. 사용 알고리즘

이 기법에서는 다음과 같은 알고리즘이 사용된다.

·$IKeygen(1^k)$ & $UKeygen(1^k, pk_i)$: 키 발급자 및 사용자의 키쌍인 (pk_i, sk_i), (pk_u, sk_u)를 생성한다.

·$Obtain(pk_i, sk_u)$ & $Issue(pk_u, sk_i)$: 이 인터액션 알고리즘을 통해 사용자는 발급자로부터 토큰 분배자 D를 얻는다.

·$Sign(m, D, pk_i, ctx)$: m에 대한 인증서와 pseudonym을 생성한다. 결국 m의 자리엔 사용자가 생성한 공개키를 입력하게 된다.

·$Verify(m, S, \tau, pk_i, ctx)$: 제시된 pseudonym이 정당한 사용자가 생성한 것인지 판별한다.

3.2. Pseudonym의 자체 생성 및 인증

사용자는 신뢰 기관으로부터 토큰 분배자 D를 발급받고 다음의 과정을 통해 통신하게 된다.

사용자 가운데 임의의 한 사용자가 도메인 컨트롤러가 되어 도메인 ctx를 주변에 브로드캐스트 한다. 이 후, 사용자는 키쌍 $(pk(u, ctx), sk(u, ctx))$를 생성하고 이를 증명받기 위해 $Sign(pk(u, ctx), D, pk_i, ctx)$ 알고리즘을 실행하여 $pk(u, ctx)$에 대한 pseudonym S와 그 인증서 $cert(u, ctx)$를 생성하게 된다. 이렇게 생성된 pseudonym

S 및 인증서는 *Verify(pk(u, ctx), S, cert(u, ctx), pki, ctx)* 알고리즘을 이용하여 모든 사용자가 검증할 수 있게 된다.

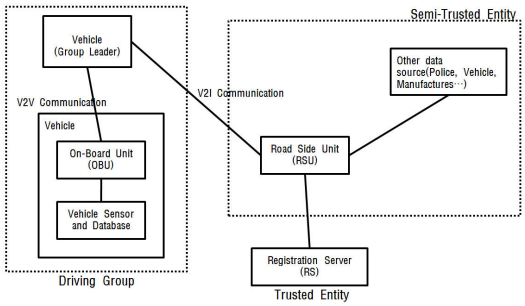
3.3. 효용성

자체 인증 pseudonym 기법은 pseudonym을 노드가 자체적으로 생성하고 인증할 수 있다는 점에서 VANET 환경에 유용하게 사용될 수 있다. Psedonym을 사용하는 VANET 보안 프로토콜은 pseudonym을 이용하여 익명성 및 메시지의 비연결성을 보장하고 무결성, 인증 문제를 해결하지만 pseudonym의 집합을 저장할 공간이 노드와 신뢰 기관 양쪽에 필요하며 덧붙여 신뢰 기관은 집합에 매핑되는 사용자 정보 역시 필요하다는 문제점을 갖는다. 또한 RSU로의 접근이 주기적으로 필요하다는 문제점 역시 존재한다. 그러나 자체 인증 pseudonym 기법을 사용하게 되면, 신뢰 기관은 최초 사용자 등록 시 발급한 비밀 인자와 사용자의 매핑 정보만을 저장하면 그 외의 매핑 정보는 필요 없으며, 사용자는 pseudonym의 집합을 저장할 공간을 필요로 하지 않는다. 또한 사용자 자체적으로 키쌍 및 pseudonym을 생성하므로 RSU에 대한 접근도 필요하지 않게 된다. 따라서 다음 장에서는 이 기법을 이용하여 VANET에서 사용할 수 있는 보안 프로토콜을 설계해보고자 한다.

4. 제안하는 방법

4.1. 가정

본 논문에서 제안하는 프로토콜은 다음과 같은 가정을 갖는다.



(그림 1) 시스템 모델

·네트워크는 그림 1과 같은 형태의 모델을 갖는다.

·각 사용자는 VANET에 참여하기 전에 차량에 대한 등록을 하고 신뢰 기관으로부터 통신에 필요한 인자 및 토큰 분배자 *D*를 부여받는다.

·각 차량은 각종 암호화 기법의 계산 및 키생성을 할 수 있다.

4.2. 차량의 그룹화

제안하는 방법에서 VANET에 참여하는 도로 위의 차량들은 그룹을 이루어 이동하게 된다. 그룹은 하나의 그룹 리더 V_L과 그룹에 참여하는 차량들로 구성되며, 다음과 같은 과정으로 생성된다.

(1) 그룹에 속하지 않은 차량은 주변에 참여할 그룹이 없는지 참여 요청 신호를 브로드캐스트 한다.
(2) 만일 그룹에 참여하고 있는 차량이 참여 요청 신호를 받게 되면 이를 그룹 리더에게 알려 요청 차량을 그룹에 참여시킨다.
(3) 참여할 그룹이 나타나지 않으면 요청 차량 스스로가 그룹 리더가 되어 그룹을 생성한다.
(4) 그룹 리더는 주기적으로 바뀌게 되며, 이는 그룹에 참여하는 차량 중에서 랜덤하게 선택된다.

차량의 협력 운전은 그룹 내에서 이루어지게 된다. 주변에 차량이 없을 경우 협력 운전은 의미가 없으므로, 그룹에 참여하는 차량만이 협력 운전을 할 수 있는 것은 문제가 되지 않는다.

<표 1> 표기법

표기	설명
RS	신뢰 기관(Registration Server)
ctx	$\{0, 1\}^n$의 문자열로 이루어진 도메인
pk_i, sk_i	신뢰 기관의 키쌍
V_n	n 번째 차량
V_L	그룹 리더 차량
$+K_n$, $-K_n$	V_n의 키쌍
$+K_{(n,\ ctx)}$, $-K_{(n,\ ctx)}$	ctx에서 생성된 V_n의 키쌍
T_n	V_n이 생성한 타임스탬프
$\{\}_K$	키 K로 암호화
$P_{(n,\ ctx)}$	ctx에서 생성된 V_n의 pseudonym
$cert_{(n,\ ctx)}$	ctx에서 생성된 $P_{(n,\ ctx)}$의 인증서
$h()$	일방향 해쉬 함수

4.3. 프로토콜 설계

그룹에 참여하여 협력 운전을 하고자 하는 차량은 다음과 같은 방법으로 프로토콜을 진행하게 된다.

$V_L \rightarrow *$: ctx
V_i: $+K_{(n,\ ctx)}$, $-K_{(n,\ ctx)}$
V_i: $P_{(n,\ ctx)}$, $cert_{(n,\ ctx)}$
$Vi \rightarrow *$: $\{cooperative\_driving, T_i, P_{(n,\ ctx)}, cert_{(n,\ ctx)}\}-K_{(n,\ ctx)}$, $+K_{(n,\ ctx)}$, $h(cooperative\_driving, T_i, P_{(n,\ ctx)}, cert_{(n,\ ctx)})$

V_i에게 협력 운전 메시지를 받은 차량들은 메시지의 검증을 위해 $Verify(+K_{(n,\ ctx)}, P_{(n,\ ctx)}, cert_{(n,\ ctx)}, pk_i, ctx)$ 알고리즘을 이용하여 메시지를 분석한다. 검증이 성공하면 수신 차량은 *cooperative_driving* 정보를 수집하게 되며, 검증이 실패하면 수신 차량은 이 노드의 pseudonym을 V_L에게 전달하고, V_L은 이를 RS에 보고하게 된다.

5. 보안 분석

본 논문에서 제안하는 방법은 다음과 같이 VANET 환경의 보안 요구사항을 만족한다.

·인증: 노드가 생성한 개인키를 이용하여 서명된 메시

지는 노드가 생성한 공개키를 이용하여 확인할 수 있다. 노드는 이 공개키의 정당성을 확인하기 위해 해당 ctx에서 생성한 pseudonym과 그 인증서를 메시지에 첨부하는데, 이는 정식으로 신뢰 기관에 등록한 차량만이 생성할 수 있는 정보이므로 메시지의 인증을 가능하게 한다.

·무결성: 노드는 메시지의 무결성을 보장하기 위해 서명된 정보의 해쉬값을 첨부한다.

·부인방지: 노드가 생성하는 pseudonym은 신뢰 기관이 발급한 토큰 분배자 D와 현재 도메인인 ctx를 사용해서 생성할 수 있으며, 신뢰 기관은 이를 역으로 계산하여 pseudonym을 생성한 노드의 신원을 확인할 수 있다. VANET 환경에서 익명성 보장은 중요한 문제이지만, 사고 발생 시 책임 소재 확인 등 조건적으로 익명성이 해제되어야 하는 경우를 고려해야하기 때문에 이러한 부인방지는 반드시 보장되어야 한다.

·위치 프라이버시: 도메인 컨트롤러인 그룹 리더 V_L은 계속해서 ctx를 갱신하며, 그룹에 참여하는 차량들은 이 ctx를 이용하여 자신의 pseudonym을 생성한다. ctx는 계속해서 랜덤으로 바뀌게 되며, 노드의 토큰 분배자 D 역시 $Sign$ 알고리즘을 실행할 때마다 갱신되므로 각 pseudonym 간의 연결성(linkability)은 없다. 따라서 차량의 위치 프라이버시는 RS 이외의 대상에게 완벽하게 보장된다.

6. 결론

본 논문은 VANET 환경에서 사용될 수 있는 어플리케이션의 보안 요구사항을 분석하여 이를 보장하는 방법을 제안했다. 제안하는 방법은 자체 인증 pseudonym 기법을 통해 메시지 인증, 무결성, 부인방지 및 차량의 위치 프라이버시를 보장하고 이에 대한 분석을 통해 정확성을 제고하였다. 또한 기존에 제안되었던 [5][6][7][8][9][10] 등의 문제점인 저장 공간의 필요성, RSU에의 접근 필요성 등을 해결하여 보다 효율적이고 안전하게 VANET 어플리케이션을 활용할 수 있도록 제공한다. 향후 우리는 자체 인증 pseudonym 기법을 개량하여 보다 VANET 환경에 알맞도록 할 것이며, 이에 나아가 VANET 환경의 보안 프레임워크를 구성하여 앞으로 전 세계적으로 활발히 진행될 VANET 환경의 표준화 연구에 대한 우리나라의 입지를 확고히 하는데 기여하고자 한다.

참고문헌

[1] L. Martucci, M. Kohlweiss, C. Andersson and A. Panchenko, "Self-certified Sybil-Free Pseudonyms," ACM Conference on WiSec 2008, pp. 154-159, 2008.

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

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

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

[5] 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.

[6] G. Calandriello, P. Papadimitratos, J. P. Hubaux and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," International Conference on Mobile Computing and Networking, Proceeding of the 4th international workshop on VANET, pp. 19-28, 2007.

[7] S. Jinyuan, Z. Chi and F. Yuguang, "An ID-based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks," IEEE MILCOM 2007, pp. 1-7, 2007.

[8] P. Kamat, A. Baliga and W. Trappe, "An Identity-based Security Framework for VANETs," Proceeding of the ACM 3rd international workshop on Vechicular ad hoc networks, pp. 94-95, 2006.

[9] X. Lin, X. Sun, P. Ho and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," IEEE Transaction on Vehicular Technology, vol. 56, pp. 3442-3456, 2007.

[10] J. Zhang, L. Ma, W. Su and Y. Wang, "Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks," IEEE Conference on ISDPE 2007, pp. 138-142, 2007.