情報保護學會論文誌
第20卷 第4號, 2010. 8

VANET에서 프라이버시를 보호하는 효율적인 경로 추적 방법*

이 병 우,[1†] 김 상 진,[2‡] 오 희 국[1†]
[1]한양대학교, [2]한국기술교육대학교

A Privacy Preserving Efficient Route Tracing Mechanism for VANET*

Byeongwoo Lee,[1†] Sangjin Kim,[2‡] Heekuck Oh[1†]
[1]Hanyang University, [2]Korea University of Technology and Education

요 약

차량 애드혹 네트워크에서는 차량의 프라이버시를 보장하지만 문제를 일으킨 차량을 식별할 수 있는 조건부 익명성이 제공되어야 한다. 이를 위해 제안된 기존 기법들은 개별 메시지의 익명성을 철회할 수 있는 기능을 제공하고 있다. 만약 차량의 운행 경로를 파악할 수 있다면 사고에서 책임소재 규명과 범죄 수사에 유용하게 사용될 수 있다. 기존 메시지 철회 기능을 이용하여 차량의 운행 경로를 파악할 수 있지만 대상 차량뿐만 아니라 다른 차량의 익명성도 철회가 되는 문제점이 있다. 본 논문은 대상 차량을 제외한 다른 차량의 프라이버시를 침해하지 않으면서 차량의 운행 경로를 파악할 수 있는 효율적인 기법을 제안한다. 제안한 방법은 기존에 사용되는 메시지 인증 기법과 독립적으로 추가하여 사용할 수 있으며, 신뢰기관의 권한 남용을 방지하기 위한 메커니즘을 포함하고 있다.

ABSTRACT

In VANETs (Vehicular Ad hoc NETwork), conditional anonymity must be provided to protect privacy of vehicles while enabling authorities to identify misbehaving vehicles. To this end, previous systems provide a mechanism to revoke the anonymity of individual messages. In VANET, if we can trace the movement path of vehicles, it can be useful in determining the liability of vehicles in car accidents and crime investigations. Although route tracing can be provided using previous message revocation techniques, they violate privacy of other vehicles. In this paper, we provide a route tracing technique that protects privacy of vehicles that are not targeted. The proposed method can be employed independently of the authentication mechanism used and includes a mechanism to prevent authorities from abusing this new function.

Keywords: VANET, route tracing, privacy

I. 서 론

VANET(Vehicle Ad hoc Network)은 무선 통신 기능을 지원하는 지능형 차량들로 이루어진 애드혹 네트워크 환경이다. VANET의 통신 형태는 차량간 통신인 V2V(Vehicle to Vehicle)와 차량과 기반 시설과의 통신인 V2I(Vehicle to Infrastructure), 두 종류가 있다. VANET에 참여하는 차량들은 이와 같은 통신 기법을 사용해서 여러 가지 응용 서비스를 제공받아 안전하고 쾌적한 운행을 할 수 있

* 접수일(2009년 12월 7일), 수정일(1차: 2009년 2월 10일, 2차: 2009년 3월 20일), 게재확정일(2009년 3월 26일)
* 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2008-313-D01024).
* 본 연구는 지식정제부 및 정보통신산업진흥원 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. (NIPA-2009-C1090-0902-0035)
† 주저자, hong@paper.hankook.ac.kr
‡ 교신저자, sangjin@kut.ac.kr

다[1,2]. 그러나 한 번의 사고가 큰 재해로 이어지는 VANET 환경의 특성상, 어플리케이션에서 활용되는 정보가 조작 및 악용되지 않도록 보안 사항을 만족시켜주는 것이 매우 중요하다. VANET에서 요구되는 보안요소에는 메시지 인증, 무결성, 부인방지, 프라이버시 보호 등이 있다. 특히, 일반 차량의 프라이버시는 보호하면서 문제를 일으킨 차량이나 사고 책임자를 식별할 수 있는 조건부 익명성은 반드시 제공되어야 한다[3].

경로 추적이란 문제 차량이나 범죄에 사용된 차량의 이동 경로를 파악하는 기능을 말한다. 현재 범죄 수사에서는 도로에 설치된 방범용 CCTV(Closed-Circuit TV)를 통해 범죄 당시 현장 근처에 운행된 차량을 파악하게 된다. VANET 서비스가 도입된 경우에는 이와 같은 CCTV 대신에 VANET 메시지를 수집하여 범죄에 사용된 후보 차량을 보다 쉽게 파악할 수 있다. 더욱이 본 논문에서 제공하고자 하는 운행 경로 파악 기능이 있다면 범죄 수사에 중요한 역할을 할 수 있을 것으로 기대된다. 뿐만 아니라 교통사고에 있어서 사고의 책임 소재를 규명하기 위해서는 사고에 포함된 각 차량의 운행 경로를 파악하면 보다 명확하게 규명이 가능해진다. 이처럼 VANET의 메시지를 통해 차량의 운행 경로를 파악할 수 있다면 여러 가지 순기능에 활용될 수 있다. 하지만 운행 경로 파악을 남용할 수 있다면 프라이버시에 심각한 침해가 되므로 남용될 수 없도록 기술적, 법적 조치가 반드시 필요하다.

강한 프라이버시를 지원하기 위해서는 불관찰성(unobservability)과 불연결성(unlinkability)이 모두 제공되어야 한다. 불관찰성이란 개별 메시지에 대해 해당 메시지를 전송한 차량을 식별할 수 없어야 한다는 것을 말하며, 불연결성이란 같은 차량이 보낸 두 메시지를 서로 연결할 수 없어야 한다는 것을 말한다. 불연결성은 특정 메시지의 익명성이 노출되었을 때 그 파급 효과를 해당 메시지로 제한할 수 있다. 무조건적 불관찰성이 제공되면 사용자들이 남용할 수 있으므로 필요할 경우 개별 메시지의 불관찰성을 철회할 수 있는 조건부 불관찰성을 제공한다. 하지만 본 논문에서 제공하고자 하는 운행 경로 추적에 있어 VANET 시스템이 불연결성은 제공하지 못하고 조건부 불관찰성만 제공하면 연결성을 이용하여 다른 차량의 프라이버시에 영향을 주지 않고 운행 경로를 파악할 수 있다. 따라서 본 논문에서는 모든 개별 메시지가 조건부 불관찰성 및 불연결성이 제공되는 VANET 환경을 가정한다. 이와 같은 환경에서 개별 메시지 익명 철회 기능을 이용하면 특정 차량의 이동 경로를 파악할 수 있지만 대상 차량뿐만 아니라 다른 모든 차량의 프라이버시가 침해되는 심각한 문제가 발생한다. 따라서 다른 차량의 프라이버시에 영향을 주지 않고 대상 차량의 운행 경로를 파악할 수 있는 기법이 필요하다.

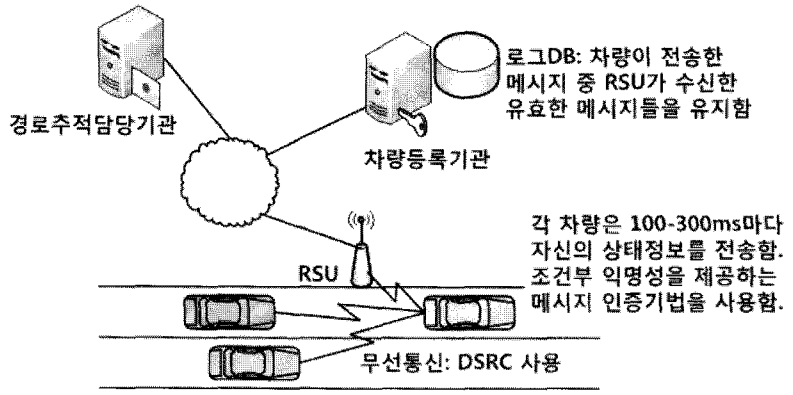
본 논문에서는 TRH(Tamper-Resistant Hardware)를 활용하여 다른 차량의 프라이버시를 침해하지 않으면서 대상 차량의 이동 경로를 파악할 수 있는 방법을 제안한다. 지금까지 VANET에서 경로 추적 기능을 제공하여 그것의 순 기능을 활용하고자 하는 연구는 없었으며 오히려 대부분의 연구는 차량의 이동 경로를 추적하지 못하도록 하는 것에 초점이 맞혀져 있었다. 제안된 시스템에서 차량들은 메시지를 전송할 때 제안된 인자들을 메시지에 추가하며, 신뢰기관은 개별 메시지에 대한 익명철회 과정 없이 특정 차량의 이동 경로를 파악할 수 있다. 지수 연산을 사용하는 방법과 MAC(Message Authentication Code)을 사용하는 방법을 제안하고 각 방법에 대한 안전성과 효율성 분석을 통해 가장 효율적인 방법을 제시한다. 제안하는 방법은 기존에 사용되고 있는 메시지 인증 기법과 독립적으로 메시지에 추가해서 사용할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구에 대해 소개하고, 3장에서는 제안하는 시스템을 자세히 설명한다. 4장에서 제안된 기법을 분석하고, 5장에서 결론과 향후 연구 방향을 제시한다.

II. 관련연구

VANET에서는 지금까지 경로 추적을 제공하는 연구는 없었지만, 다음과 같이 익명성을 제공하는 그룹 서명기법에 추적 기능을 제공하는 연구는 있었다. Kiayias 등은 기존의 그룹 서명 기법에서 신뢰 기관이 메시지의 익명성을 철회하는 기능만으로는 프라이버시 보호가 충분하지 못하다는 점을 보완하기 위해 추적가능 서명기법(traceable signature)을 제안했다[4]. 이 서명 기법은 추적 연산을 추가해서 익명철회 없이 신원이 알려진 사용자의 모든 메시지를 추적할 수 있는 기법이다. 모든 메시지에 대한 익명철회가 필요 없기 때문에 추적 대상이 아닌 사용자의 프라이버시는 침해되지 않는다.

Choi 등은 짧은 추적 가능 서명기법을 제안했다[5]. 이들은 Boneh 등이 제안한 그룹 서명 기법[6]



〔그림 1〕 시스템에서 가정하는 VANET 통신 모델

에 Kiayias 등이 제안한 추적기능을 추가하였다. Kiayias 등의 방법과 비교했을 때, 타원곡선 기반 군 환경을 사용하기 때문에 서명의 길이가 상대적으로 작다. 이 방법도 추적을 원하는 사용자의 신원을 알고 있을 경우, 메시지의 익명성을 철회할 필요 없이 추적 연산을 통해서 해당 메시지가 추적하고자 하는 사용자의 메시지인지 여부를 알 수 있는 방법이다.

Kiayias 등이 제안한 방법이나 Choi 등이 제안한 방법을 그대로 VANET에 적용을 한다면 VANET의 보안 요구 사항을 만족시키면서 본 논문에서 제안하는 경로 추적 기능의 요구사항도 만족시킬 수 있다. 그러나 매 100-300ms마다 메시지를 전송하는 VANET 환경의 특성상, 이와 같이 공개키 연산을 사용하는 것과 메시지 크기 증가 측면에서 차량에게 부담이 될 것이다. 현재 VANET의 연구 동향이 조건부 익명성을 만족하면서 효율성을 높이는 것임을 생각해 볼 때 〔7-11〕 추적 서명 기법을 그대로 VANET에 적용하는 것은 기능 하나를 추가하기 위해 차량에 큰 부담을 지우는 것으로 현재의 연구 동향과 동떨어진 결과가 될 것이다. 본 논문은 이런 문제점을 감안해서 추적가능 서명기법을 사용하지 않고 기존의 조건부 익명성을 보장하는 VANET 통신 기법과 독립적으로 경로 추적 기능을 추가해서 사용을 할 수 있는 효율적인 방법을 제안하고자 한다.

III. 제안하는 시스템

3.1 시스템 모델

3.1.1 TRH(Tamper-Resistant Hardware)

Raya와 Hubaux〔7〕는 TRH를 사용해서 차량에서 유지되는 암호키들의 안전성을 높이고자 하였고, Zhang 등〔8〕과 김상진 등〔9〕은 TRH에 신원 기반 시스템의 개인키 발급자의 마스터키를 저장하여 차량 자체에서 익명공개키를 생성하는 방법을 사용했다. 차량은 비용 측면에서 TRH를 충분히 사용할 수 있으며 안전성 측면에서 TRH의 사용은 권장되어야 한다. 본 논문에서도 TRH를 사용하며 다음을 가정한다.

- 가정 1. TRH 내부에는 암호모듈이 구축되어 있고, 이 모듈의 동작은 외부에서 영향을 줄 수가 없다.
- 가정 2. TRH 내부의 비휘발성 메모리에 저장된 정보는 외부에서 획득할 수 없다.

본 논문에서 TRH를 사용하는 가장 큰 이유는 가정 1를 활용하기 위함이다. 즉, 경로 추적 기능에 사용되는 값들이 정해진 규칙에 따라 생성됨을 보장하기 위해 TRH를 사용하고 있다. 만약 TRH를 사용하지 않으면 영지식 증명과 같은 기법을 사용하여 사용된 값의 유효성을 보장해야 한다. 하지만 이 경우 값을 생성하는 측과 확인하는 측에게 모두 부담이 된다.

3.1.2 통신모델

본 논문에서는 〔그림 1〕과 같이 VANET의 노드들인 차량과 도로에 설치된 RSU(Road-Side Unit)는 무선 통신 표준으로 DSRC(Dedicated Short-Range Communication)〔12〕을 사용한다고 가정한다. DSRC에 의하면 각 차량은 100-300ms 마다 자신의 상태 정보(현재시간, 방향, 위치, 속도, 가속도 등)를 방송한다. 차량들은 이 정보를 수신하여 차량 진행 방향의 교통상황을 미리 파악할 수 있다. 전송되는 주기는 차량의 속도에 좌우되며, 사용되는 전력은

메시지의 종류에 따라 다르지만 앞서 언급한 상태 정보는 전송 반경이 최대 400m이다. VANET이 완전히 도입된 시점에서는 RSU가 도로 곳곳에 설치되어 있지만 아주 조밀하게 설치되어 있지 않으므로 차량에서 전송된 모든 메시지가 한 홉 통신으로 RSU로 전달될 수 없다. 다중 홉 방식을 사용하더라도 홉 거리 제한과 무선 통신의 특성 때문에 모든 메시지가 RSU에 전달된다고 보장하기 어렵다. 따라서 RSU의 통신 반경 내에서 전송된 메시지와 응용의 요구에 의해 일정한 홉 수로 전달된 메시지들 중 일부만 RSU가 수신하게 된다.

본 논문에서 제공하고자 하는 차량 이동 경로 추적 기능은 이렇게 RSU로 전달되어 중앙서버에 보관된 메시지를 이용하여 이루어지게 된다. 물론 통신 모델에 의해 일부 손실되거나 수신하지 못하는 메시지가 있지만 RSU가 충분히 설치되어 있다면 차량의 대략적인 이동 경로는 충분히 파악할 수 있다.

3.1.3 VANET 환경에 대한 가정

본 논문에서는 VANET 환경에 대해 다음을 가정한다.

- 가정 1. 모든 차량은 시스템에서 발급한 TRH를 내장하고 있다.
- 가정 2. 모든 차량은 GPS(Global Positioning System), 네비게이션 시스템, 차량블랙박스 등과 같은 장치들이 설치되어 있는 지능형 차량이다.
- 가정 3. RSU가 도로에 충분히 설치되어 있다.
- 가정 4. RSU는 차량으로부터 수신한 메시지들을 차량등록기관에 전달하며, 이 기관은 이 메시지들을 로그DB에 유지한다.

가정 1, 2, 3에 의해 이 연구는 VANET이 완전하게 서비스되는 환경을 고려하고, VANET의 초기 도입 단계에 대한 고려는 하지 않는다.

3.1.4 신뢰기관의 권한 남용 방지

추적 기능의 남용은 VANET 사용자의 프라이버시를 침해할 수 있기 때문에, 신뢰 기관에 의한 추적 기능의 사용도 제한되어야한다. 본 논문에서 제공하는 기법의 경우 특정 차량의 경로를 추적하기 위해서는 경로 추적 기능에 사용된 특정 차량의 식별자를 알아야 한다. 이 식별자는 개별 메시지의 불관찰성 철회에 사용되는 식별자와 독립적인 식별자이며 차량 등록 과정에서 TRH에서 생성되어 암호화된 상태로 차량 추적 기능을 담당하는 신뢰기관에 전달된다. 따라서 이 신뢰기관이 특정 차량의 경로를 추적하기 위해서는 암호화된 식별자를 먼저 복호화해야 한다. 이 과정을 제어함으로써 경로 추적 기능의 남용을 방지할 수 있다. 가장 간단한 방법은 TRH에 (t,n) 임계방식(threshold-based)[13]으로 생성된 개인키에 대응하는 공개키를 포함하고 이 공개키로 식별자를 암호화하도록 하는 것이다. 여기서 (t,n) 임계방식 공개키시스템이란 공개키로 암호화된 암호문을 복호화기 위해서는 전체 n홍콩기명 중 t명 이상의 협조가 필요한 시스템을 말하며, 이를 위해 공개키에 대응되는 개인키는 n명이 비밀공유한다. 이 때 중앙서버가 각 사용자의 몫(share)을 만들어 분배하지 않고 분산비밀공유 방식을 사용할 수 있다. 이 방법을 사용하면 여러 신뢰 기관의 협력 없이는 복호화가 가능하지 않아 남용을 막을 수 있다.

3.2 제안하는 방법

3.2.1 표기법

[표 1]에 제시된 표기법을 이용하여 제안하는 방법을 설명한다.

3.2.2 추적 기능

문제 차량이나 범죄에 사용된 차량의 경우, 수사 기관에서 그 운행 경로를 알아야 할 필요가 있다. 이 경

[표 3] 표기법

표기	의미
T	추적값
r	차량이 생성한 랜덤값
t	타임스탬프
K_{id}	차량의 TRH 비밀키
v_{id}	차량의 고유 id
x_{id}	경로 추적에 사용되는 차량의 익명 id
$H_q : \{0,1\}^* \rightarrow Z_q^*$	충돌회피 해쉬함수
$H_k : \{0,1\}^* \rightarrow \{0,1\}^k$	충돌회피 해쉬함수
$MAC.K(m)$	대칭키 K를 이용한 메시지 m에 대한 MAC값

우 기존의 조건부 익명성을 만족하는 VANET 통신 시스템에서 제공하는 메시지 익명철회 기능을 통해서 파악 할 수도 있다. 그러나 이는 모든 메시지의 익명성을 철회 시켜야 가능하며 앞서 말한 바와 같이 이는 추적 대상이 아닌 차량의 프라이버시가 침해될 수 있다. 본 논문에서 제안하는 경로 추적 기능은 이런 문제점을 해결한다. 따라서 제안하는 경로 추적 기능은 다음과 같은 4가지 요구사항을 만족해야 한다.

- 요구사항 1. 신뢰기관만 특정 차량의 이동 경로를 파악할 수 있어야 한다.
- 요구사항 2. 신뢰기관은 경로 추적 기능을 남용할 수 없어야 한다.
- 요구사항 3. 경로 추적 과정에서 대상 차량 외에 다른 차량의 프라이버시는 침해되지 않아야 한다.
- 요구사항 4. 경로 추적 기능을 위해 메시지에 추가된 요소는 프라이버시를 보장해야 한다.

위에 나열한 요구사항을 충족시키는 이동 경로 추적 기능을 제공하기 위해서는 다음과 같은 두 종류의 함수가 필요하다. 첫째, $f:(x_{id},r)\rightarrow T$와 같은 형태로 각 VANET 메시지에 추가될 값을 생성하는 함수가 필요하다. 여기서 r은 매번 다른 T값이 생성되도록 사용되는 랜덤 값이다. 이것은 요구사항 4의 불연결성을 충족하기 위해 필요하다. 둘째, x_{id}가 주어졌을 때 메시지에 포함된 T값이 주어진 x_{id}를 이용하여 생성된 값인지 확인할 수 있는 $g:(T,x_{id})\rightarrow\{0,1\}$와 같은 형태의 함수가 필요하다. g 함수는 T가 x_{id}를 이용하여 계산된 값이면 1을 아니면 0를 출력해야 한다.

추적기능 요구사항 1과 4를 만족하기 위해 f 함수는 해쉬함수처럼 일방향성 특성을 가지고 있어야 한다. 즉, T로부터 그것을 생성할 때 사용된 x_{id}를 계산할 수 없어야 한다. 요구사항 2을 만족하기 위해서는 x_{id}가 보호된 상태로 유지되어야 하며, 일정한 수의 신뢰기관의 동의가 있어야 얻을 수 있도록 만들어야 한다. 이 기능을 제공하는 가장 일반적인 방법은 임계방식의 암호기법[13]을 사용하여 x_{id}를 암호화하여 유지하는 것이다.

요구사항 3을 만족하기 위해 g 함수는 0과 1외에 T를 계산할 때 사용된 x_{id}에 대한 어떤 추가적인 정보도 노출시키지 않아야 한다. 요구사항 4의 경우 요구사항 1과 3이 만족되면 불관찰성이 기본적으로 제공되며, 같은 x_{id}이지만 다른 r를 이용하여 계산된 두 개의 T값이 같은 x_{id}로 계산된 것인지 연결할 수 없어야 불연결성까지 제공된다.

추적값이 메시지와 무관한 값일 경우에는 추적값을 재사용하거나 교체하여 사용 할 수 있기 때문에 추적값은 메시지에 바인딩되어야 한다. 이를 위해 추적값 생성 함수인 f의 인자로 메시지를 사용하거나, 메시지를 인증하는 방법에 T값을 추가할 수 있다. 본 논문에서는 T값을 메시지를 인증하는 방법에 추가한다고 가정을 한다. 즉, 메시지 내용이 m이고 조건부 익명성을 제공하는 서명기법 $AnonSig(m)$을 사용한다고 가정하면, 경로추적 기능의 추가로 전체 메시지는 m, T, $AnonSig(m\|T)$로 변경된다.

3.2.3 방법 1: 지수 연산을 사용하는 방법

3.2.3.1 시스템 설정 및 차량 등록

차량등록기관은 p가 소수일 때, 위수가 소수 q인 Z_p^*의 부분군 $G=<g>$를 생성한다. 경로추적담당기관은 임계방식의 분산비밀공유기법[13]을 사용하여 공개키 $y=g^s$를 생성한다. 즉, 경로추적담당기관은 개인키 $s\in Z_p^*$의 몫만 가지고 있다. 차량 v_{id}가 등록을 원하면 차량등록기관은 공개키 y가 저장되어 있는 TRH를 차량의 OBU(On-Board Unit)에 설치한다. TRH가 동작을 시작하면 추적기능에 사용될 차량의 익명 id인 $x_{id}\in_R Z_q^*$를 생성한 다음 ElGamal 공개키 시스템[14]을 이용하여 공개키 y로 x_{id}를 암호화한 $v_{id},(g^{w_1},y^{w_1}g^{w_2}),H_q(g^{w_2})\oplus x_{id}$를 경로추적담당기관에 전달한다. 여기서 $w_1,w_2\in Z_q^*$는 암호화를 위해 선택한 랜덤요소들이다. 익명 id를 사용하는 것은 x_{id}가 노출되더라도 차량의 실제 신원을 알 수 없도록 하기 위함이다.

3.2.3.2 추적값 생성 및 추적

차량이 메시지를 전송할 때마다 차량의 TRH는 $r\in_R Z_p^*$를 선택하고 $\alpha=g^r$, $\beta=x_{id}\cdot r$을 계산한 뒤, 메시지를 전송할 때 $T=<\alpha,\beta>$를 포함한다. 여기서 T값은 메시지와 바인딩하기 위해 사용하는 메시지 인증 기법의 입력 중 하나로 사용해야 한다. 예를 들어 메시지를 항상 전자서명하여 전달할 경우에는 T값은 전자서명 메시지에 포함되어야 한다.

만약 차량 v_{id}에 대한 경로 추적이 필요할 경우, 도로 곳곳에 설치된 RSU로부터 수집되어 보관 중인 메시지들 중에 지역과 시간 기준으로 검색할 집합을 분류한 후에 다음과 같은 과정을 통해 이루어진다.

- 단계 1. 경로추적담당기관은 다른 기관들의 협조

를 얻어 데이터베이스에 저장된 암호문을 복호화하여 대상 차량의 x_{id}를 얻는다.

- 단계 2. 검색 집합의 각 메시지에 대해 $\alpha^{x_{id}}$와 g^{β}를 계산한 다음 두 값이 같은 메시지들을 메시지에 포함된 타임스템프를 이용하여 정렬한다. 정렬된 메시지들의 위치정보를 관찰하면 차량의 이동경로를 파악할 수 있다. T값이 x_{id}를 이용하여 생성된 값이라면 $\alpha^{x_{id}}(=g^{rx_{id}})$이고 $g^{\beta}(=g^{x_{id}r})$이므로 두 값이 같으며, 아니라면 $\alpha^{x_{id}}(=g^{rx_{id}})$이고 $g^{\beta}(=g^{x'_{id}r})$이므로 서로 다르다. x_{id}는 Z_q^*에서 임의로 선택된 값이므로 서로 다른 두 차량이 선택한 익명 id가 같을 확률은 매우 작다.

만약, T값이 규칙대로 생성되지 않았다면 경로 추적 기능이 올바르게 동작할 수 없지만 TRH 가정 2에 의해서 이와 같은 상황은 발생하지 않는다. 경로 추적 대상이 된 차량은 x_{id}가 노출되었으므로 차량등록과정을 반복하여 x_{id}를 갱신하여야 한다.

방법 1은 간단하게 타원곡선 기반 덧셈군 환경($\alpha=rP$, $\beta=r \cdot x_{id}$, 여기서 P는 타원곡선 기반 군의 생성자)으로 바꿀 수 있으며, 이 경우 T 값의 크기를 줄일 수 있다. 곱셈군 기반 방법 1은 각 메시지마다 한 개의 지수연산이 필요하다. 이 지수연산을 제거하기 위해 $\alpha=r$, $\beta=H(x_{id} \cdot r)$로 계산하고, 대상 차량의 익명 id가 x'_{id}이면 $H(x'_{id} \cdot \alpha)$와 β를 비교하여 경로 추적을 할 수 있다. 여기서 β는 x_{id}를 알고 있는 사용자만 계산할 수 있는 해쉬값이므로 MAC과 같은 효과를 가지고 있으며, 이 방법은 기존 방법 1에 비해 계산 효율성이 높다. 이에 다음 절의 방법을 제안한다.

3.2.4 방법 2: MAC값을 사용하는 방법

3.2.4.1 시스템 설정 및 차량 등록

방법 1과 시스템 설정 부분은 동일하다. 이 방법에서 차량 v_{id}가 등록을 원하면 차량등록기관은 공개키 y가 저장되어 있는 TRH를 차량의 OBU에 설치한다. TRH가 동작을 시작하면 추적 기능에 사용될 MAC 키 K_{id}를 생성한 다음 이것을 y로 암호화한 $v_{id}, (g^{w_1}, y^{w_1}g^{w_2}), H_k(g^{w_2}) \oplus K_{id}$를 경로추적담당기관에 전달한다.

3.2.4.2 추적값 생성 및 추적

차량이 메시지를 전송할 때마다 차량의 TRH는 $T=MACK_{id}(t)$를 계산하여 메시지에 포함한다. 여기서 t는 메시지에 포함된 타임스템프이다. 이 T값도 메시지와 적절하게 바인딩하여야 한다. 차량 v_{id}에 대한 경로 추적은 다음과 같은 과정을 통해 이루어진다.

- 단계 1. 경로추적담당기관은 다른 기관들의 협조를 얻어 데이터베이스에 저장된 암호문을 복호화하여 대상 차량의 K_{id}를 얻는다.
- 단계 2. 검색 집합의 각 메시지에 대해 $MACK_{id}(t)$를 계산하여 T와 비교하여 두 값이 같은 메시지들을 메시지에 포함된 타임스템프를 이용하여 정렬한다. K_{id}가 128 비트이고, 랜덤하게 선택한다면 서로 다른 차량이 동일한 키를 선택할 확률은 매우 작다. 또 $K_{id} \neq K'_{id}$일 때 $MACK_{id}(t) = MACK'_{id}(t)$일 확률은 MAC의 충돌회피성 때문에 확률적으로 매우 낮다.

이 기법은 별도의 랜덤값을 생성하지 않고 메시지에 포함된 타임스템프를 사용하기 때문에 3.2.3에 설명된 해쉬함수를 이용한 기법보다 메시지에 추가되는 값의 크기가 작다.

3.2.5 제안한 경로추적 기법의 추가 고려사항

방법 1이나 방법 2에서 경로추적담당기관이 특정 차량에 대한 차량추적 권한을 얻어 차량의 익명 id나 MAC 키를 확보하면 지속적으로 다른 기관의 협조없이 차량을 추적할 수 있게 된다. 이 문제를 극복하기 위해 다음과 같은 조치들이 추가로 필요하다.

- 메시지를 수집하는 기관과 차량추적을 시행하는 기관을 분리하여 경로추적담당기관이 불필요한 메시지에 대한 접근을 차단하여야 한다. 경로추적담당기관이 경로추적을 하기 위해서는 법원으로부터 영장을 받아야 하며, 영장에는 대상 차량, 추적 기간, 대상 지역 등을 포함한다. 따라서 영장에 제시된 기간과 지역에 해당하는 메시지들만 접근이 가능하도록 해야 하며, 최초 접근은 메시지 id, 타임스템프, T값에 대해서만 접근을 허가하고 현재 추적하는 차량에 해당하는 메시지로 판정된 경우에만 위치정보와 같은 메시지 내용에 대해서 접근을 허가해야 한다.
- 차량은 정기적으로 경로추적에 사용되는 id 또는 키값을 변경한다. 이를 통해 경로추적담당기관이 id나 키를 확보하였을 때 이들을 이용하여 경로추적할 수 있는 기간을 제한한다.

IV. 분석

이 장에서는 본 논문에서 제안한 두 가지 경로 추적 방법의 안전성과 효율성을 비교 분석한다.

4.1 안전성 분석

이 절에서는 네 가지 요구사항의 충족 여부에 대해 분석한다. 방법 1과 관련하여 p는 512비트 이상이고 q는 160비트 이상이라고 가정한다. 즉, 군 G에서 이산대수 문제를 해결하는 것은 계산적으로 불가능하다고 가정한다.

(1) 신뢰기관만 특정 차량의 이동 경로를 파악할 수 있어야 한다.

방법 1의 경우 $\alpha=g^r$, $\beta=x_{id}\cdot r$로부터 x_{id}를 계산하기 위해서는 α로부터 r를 계산하거나 x_{id}를 추측하는 전사(brute-force)공격을 시도해야 한다. 전자는 이산대수 문제이므로 계산적으로 불가능하며, x_{id}는 Z_q^*에서 랜덤으로 선택한 값이므로 후자는 x_{id}의 범위 때문에 계산적으로 가능하지 않다. x_{id}를 계산할 수 있다고 가정하더라도 x_{id}는 랜덤 값이므로 이 값이 어떤 차량에 해당되는지 알 수 없다. 방법 2의 경우 $T=MACK_{id}(t)$로부터 K_{id}를 계산할 수 있어야 한다. 하지만 사용하는 MAC 함수가 안전하면 이것은 가능하지 않다. 방법 1과 마찬가지로 K_{id}를 계산할 수 있더라도 이 키가 어떤 차량의 키인지 알 수 없다.

(2) 신뢰기관은 경로 추적 기능을 남용할 수 없어야 한다.

차량의 경로를 추적하기 위해 필요한 식별자 또는 MAC 키는 등록 과정에서 TRH에 의해 암호화 되어서 전송된다. 이것을 복호화하기 위해서는 다른 신뢰기관의 협조가 필요하다. 따라서 경로추적담당기관이 홀로 차량의 이동 경로를 파악할 수 없다. 3.2.5에서 설명한 바와 같이 정기적으로 식별자나 MAC키를 변경하면 경로추적담당기관이 이미 확보한 식별자나 키를 이용하여 권한을 남용할 수 있는 범위를 시간적으로 제한할 수 있다.

(3) 경로 추적 과정에서 대상 차량 외에 다른 차량의 프라이버시를 침해하지 않아야 한다.

방법 1과 2는 모두 요구사항 1의 충족 여부에서 설명한 것처럼 T로부터 직접 x_{id}나 K_{id}를 계산할 수 없다. 방법 1의 경우 T값을 생성할 때 사용된 x_{id}가 아닌 다른 x'_{id}로 확인하면 $g^{x'_{id}\cdot r}\neq g^{x_{id}\cdot r}$이므로 메시지가 x'_{id}와 연관이 없다는 것을 알 수 있다. 하지만 $\alpha(=g^r)$, $\alpha^2(=g^{2r})$, ..., $\alpha^k(=g^{kr})$를 계산한 후에 $(g^\beta/\alpha^{x'_{id}})=g^{x_{id}\cdot r-x'_{id}\cdot r}$와 비교하여 일치하는 값이 있으면 x_{id}를 계산할 수 있다. 즉, T값을 생성할 때 사용된 x_{id}와 이 값을 검증할 때 사용된 x'_{id}의 차이가 크지 않으면 전사공격을 통해 T값에 사용된 x_{id}를 계산할 수 있다. 방법 2의 경우 T값을 생성할 때 사용된 K_{id}가 아닌 다른 K'_{id}로 확인하면 $MACK_{id}(t)\neq MACK'_{id}(t)$이므로 메시지가 K'_{id}와 연관이 없다는 것을 알 수 있다. 하지만 방법 1과 달리 이 비교를 통해 K_{id}에 대한 어떤 정보도 얻을 수 없다.

(4) 경로 추적 기능을 위해 메시지에 추가된 요소는 프라이버시를 보장해야 한다.

제안하는 방법은 기존의 메시지 인증 기법과 독립적으로 메시지에 추가해서 사용할 수 있는 방법이다. 만약 기존 인증 기법이 프라이버시를 보장하였다면 메시지에 추가된 T값도 프라이버시를 보장해야 한다. 요구사항 1과 3이 만족되므로 방법 2의 T값은 불관찰성을 만족한다. 방법 1의 경우 같은 두 개의 T값으로부터 $(\alpha/\alpha')=g^{r-r'}$를 계산한 후에 r과 r'의 차이가 작다면 $r-r'$을 계산할 수 있고, $(\beta-\beta')/(r-r')=x_{id}-x'_{id}$

〔표 4〕 효율성 비교

	방법1			방법2	Choi 등의 방법*
	이산대수	타원곡선	SHA-256	HMAC-SHA1	겹선형사상
메시지에 추가되는 값의 크기	84바이트	40바이트	32바이트	20바이트	104바이트
메시지 생성 비용	1지수승,1곱셈	1타원곡선곱셈 1곱셈	1곱셈,1해쉬	1MAC	2겹선형사상 2지수승 1타원곡선덧셈
경로추적 비용 (메시지마다)	2지수승	2타원곡선곱셈	1곱셈,1해쉬	1MAC	1겹선형사상

* 경로추적과 관련된 요소만 고려하였음

이므로 이 값이 0이면 두 개의 T값은 동일한 x_{id}로 계산된 값인지 알 수 있다. 또한 한 번 사용된 r을 다시 사용하면 두 개의 T값이 같아지므로 불연결성이 제공되지 않다. 방법 2의 경우에는 T값으로부터 K_{id}를 계산할 수 없으면 두 개의 T값이 동일한 K_{id}를 이용하여 계산한 것인지 알 수 없다. 따라서 방법 2는 불관찰성과 불연결성을 모두 제공한다.

따라서 MAC을 이용하는 방법이 안전성 측면에서 우수하다.

4.2 효율성 분석

이 논문에서 제안한 4가지 방법과 Choi 등의 방법을 비교하면 표 2와 같다. 이 비교에서 방법 1의 경우 군 G를 생성할 때 사용한 p가 64 바이트이고 q가 20 바이트라 가정하며, 해쉬함수는 SHA-256을 사용한다고 가정한다. 방법 1의 타원곡선을 이용하는 기법이나 Choi 등의 기법에서 사용되는 타원곡선 기반 군의 경우에는 하나의 타원곡선 점을 표현하기 위해 20 바이트가 필요하고, 겹선형 사상의 결과는 64 바이트가 필요하다고 가정한다. 방법 2의 경우에는 SHA-1 기반의 HMAC을 가정한다. 참고로 최근에 SHA-1의 안전성 문제로 SHA-256의 사용이 권장되고 있지만 HMAC은 이것과 무관하므로 SHA-1 기반의 HMAC을 사용하여도 안전하다. 표를 통해 알 수 있듯이 메시지에 추가되는 값의 크기나 메시지 생성 비용을 고려하였을 때 방법 2가 가장 우수하다.

따라서 방법 2를 도입하면 각 메시지마다 20바이트 크기의 값이 추가되어야 하며, 각 차량은 메시지마다 한 번의 MAC 연산을 추가로 수행하여야 한다. 하지만 일반 차량들은 추가된 MAC 값을 확인할 필요도 없고 확인할 수도 없으므로 수신한 차량에서 메시지 검증 비용은 증가하지 않는다. 차량 경로 추적을 할 경우에는 검사하는 대상 메시지마다 한 번의 MAC 연산을 수행하여야 한다.

V. 결 론

본 논문에서는 대상 차량을 제외한 다른 차량의 프라이버시를 침해하지 않으면서 경로를 추적할 수 있는 MAC을 사용하는 새로운 방법을 제안하였다. 이 논문은 VANET에서 이동 경로 추적 기법의 필요성을 처음으로 제시하고 간단하면서 효율적인 방법을 제안한 논문이다. 제안된 기법은 기존 VANET 통신 기법에서 사용하는 메시지 인증 기법과 독립적으로 추가하여 사용할 수 있으며, 경로 추적을 담당하는 기관의 권한 남용을 방지하기 위한 메커니즘을 포함하고 있다. 이 기법은 TRH가 필요하며, 기존 메시지에 MAC 값을 하나만 추가하면 된다. 결과적으로 제시된 기법은 매우 단순한지만 이 논문의 공헌은 경로 추적의 필요성과 유용성을 최초로 제시한 것, 경로 추적에 필요한 요구사항과 함수를 정의하고 이것을 충족하는 간단한 기법을 제시한 것, 제안한 기법은 사용하고 있는 메시지 인증 기법과 독립적으로 추가하여 사용할 수 있다는 것, 경로 추적을 제공할 경우에는 기존 메시지 익명철회 방법에 사용된 id와 다른 id 또는 키를 사용할 필요가 있다는 것 등이 있다.

참고문헌

[1] H. Hartenstein and K. P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks," IEEE Communications Magazine, vol. 46, no. 6, pp. 164 - 171, Jun. 2008.

[2] Y. Toor, P. Mühlethaler, A. Laouiti, and A. Fortelle, "Vehicular ad hoc networks: Applications and related technical issues," *IEEE Communication Survey & Tutorial*, vol. 10, no. 3, pp. 74-88, 2008.

[3] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, B. Ta-Vinh Thong, G. Calandriello, A. Held, A. Kung, and J.-P, Hubaux, "Secure vehicular communication systems: Design and Architecture," IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[4] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable signatures," Advances in Cryptology, Eurocrypt 2004, LNCS 3027, pp. 571-589, 2004.

[5] S.G. Choi, K. Park, and M. Yung, "Short traceable signatures based on bilinear pairings," Proceedings of the 1st International Workshop on Security, IWSEC 2006, LNCS 4266, pp. 88-103, 2006.

[6] D. Boneh, X. Boyen, and H. Shacham,

"Short group signatures," *Advances in Cryptology, Crypto 2004*, LNCS 3152, pp. 41-55, 2004.

[7] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, Jan. 2007.

[8] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks," *Proceedings of the IEEE INFOCOM 2008*, pp. 246-350, Apr. 2008.

[9] 김상진, 임지환, 오희국, "VANET을 위한 차량자체생성 조건부익명 인증시스템," *정보보호학회논문지*, vol. 19, no. 4, pp. 105-114, 2009년 8월.

[10] 김상진, 이병우, 오희국, "VANET을 위한 차량자체 갱신가능 익명ID 시스템," *정보보호학회논문지*, vol. 19, no. 5, pp. 93-103, 2009년 10월.

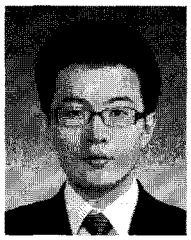
[11] R. Hussain, S. Kim, and H. Oh, "Towards privacy aware pseudonymless strategy for avoiding profile generation in VANET," *Proceedings of the 10th International Workshop on Information Security Applications*, WISA 2009, LNCS 5932, pp. 268-280, 2009.

[12] 오종택, "미국의 5.9GHz 차세대 DSRC 주파수 및 표준화 현황," *TTA Journal*, No. 98, pp. 122-132, 2005년 4월.

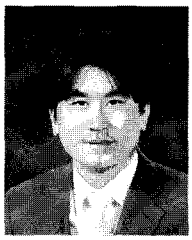
[13] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," *Advances in Cryptology, Eurocrypt 1999*, LNCS 1592, pp. 295-310, 1999.

[14] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," Advances in Cryptology, Crypto 1984, LNCS 196, pp. 10-18, 1984.

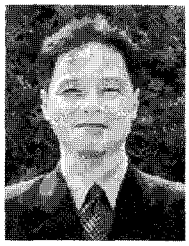
〈著者紹介〉



이 병 우 (Byeongwoo Lee) 학생회원
2008년 2월: 한양대학교 전자컴퓨터공학부(학사)
2009년 2월: 한양대학교 컴퓨터공학과(석사)
〈관심분야〉 네트워크 보안



김 상 진 (Sangjin Kim) 종신회원
1995년 2월: 한양대학교 전자계산학과(학사)
1997년 2월 한양대학교 전자계산학과(석사)
2002년 8월 한양대학교 전자계산학과(박사)
2003년 3월~현재: 한국기술교육대학교 인터넷미디어공학부 부교수
〈관심분야〉 암호기술 응용
URL:http://infosec.kut.ac.kr/sangjin/



오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과(학사)
1989년: 아이오와주립대학 전자계산학과(석사)
1992년: 아이오와주립대학 전자계산학과(박사)
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안
URL:http://infosec.hanyang.ac.kr/~hkoh/