VANET에서 프라이버시 보호를 위한 대칭키 기반의 인증 프로토콜*

임원우[1], 오희국[1], 김상진[2]
[1]한양대학교 컴퓨터공학과
[2]한국기술교육대학교 컴퓨터공학부
e-mail: wonwoo@infosec.hanyang.ac.kr

Symmetric Key-based Authentication Protocol to Preserve Privacy in VANET

Wonwoo Rhim[1], Heekuck Oh[1], Sangjin Kim[2]
[1]Dept of Computer Science and Engineering, Hanyang University
[2]Dept of Computer Science and Engineering, Korea University of Technology and Education

요 약

VANET은 V2V, V2I 통신을 통해 다양한 서비스를 제공하며, 차량은 여러 가지 서비스를 제공받아 안전하고 효율적인 운행을 할 수 있다. 다양한 서비스를 제공하고 이용하기 위해 안전하고 신뢰성 있는 V2V, V2I 통신이 보장되어야 하며, 이를 위해 많은 연구들이 진행되었다. 기존의 대부분의 연구들은 공개키 기반 암호시스템을 이용하였다. 하지만 VANET의 DSRC 프로토콜에 의하면 한 차량에서 짧은 순간에 매우 많은 메시지를 확인해야 하며, 따라서 매우 큰 연산량이 발생하게 된다. 또한 DSRC를 사용할 경우 서버와의 통신을 항상 보장할 수 없다. 본 논문에서는 이를 해결하기 위해 다른 통신 메커니즘의 사용을 고려한 대칭키 기반 인증 프로토콜을 제안한다.

1. 서론

VANET(Vehicular Ad-hoc NETwork)은 V2V (Vehicular to Vehicular), V2I(Vehicular to Infrastruc-ture) 통신을 통하여 차량의 운행에 도움이 되는 서비스를 제공하고, 차량들은 여러 가지 서비스를 제공받아 안전하고 효율적인 운행을 할 수 있다. 그러한 서비스의 정보가 조작 및 악용되지 않도록 하는 것이 매우 중요하며, 안전하고 신뢰성 있는 V2V, V2I 통신이 보장되어야 한다. 이를 위해 많은 연구들이 진행되었다.

2007년 Raya와 Hubaux의 기법[1], Lin 등의 GSIS[2], 2008년 Lu 등의 ECPP[3] 등을 포함한 대부분의 연구들은 공개키 기반 암호시스템을 이용하고 있다. VANET의 DSRC(Dedicated Short Range Communication) 프로토콜에 의하면 차량에서 메시지는 100-300ms의 주기로 송신된다[4]. 한 차량에서 짧은 순간에 매우 많은 메시지를 확인해야 하며, 공개키 기반 인증을 이용하여 메시지를 확인할 경우 매우 큰 연산량이 발생하게 된다. 따라서 대칭키 기반 인증 방법이 필요하다.

기존의 대칭키 기반 연구들로는 2008년 Lin 등의 TSVC[5], Zhang 등의 RAISE[6], Plößl과 Federrath의 기법[7] 등이 있다. Lin 등의 기법과 Zhang 등의 기법은 차량이 메시지를 수신하고 인증하기까지 시간지연이 발생하며, 이는 차량이 빠른 속도로 이동하며 짧은 순간에 메시지를 인증해야 하는 환경에 적합하다고 할 수 없다. Plößl과 Federrath의 기법은 대칭키의 사용기간을 고려하지 않았으며, 차량의 키 갱신요구를 관찰하는 것으로 차량이 추적될 수 있다.

본 논문에서는 공개키 기반 인증을 이용하여 메시지를 확인할 경우 연산량이 매우 크다는 문제점을 해결하기 위해, Plößl과 Federrath의 기법을 개선한 대칭키 기반 인증 프로토콜을 제안한다. 대칭키 기반 인증은 브로드캐스트 인증을 제공하지 못한다. 따라서 TRH (Tamper Resistant Hardware)의 사용을 고려하며, 그룹 내의 차량에 동일한 대칭키를 유지하고, 이를 TRH를 통해 보호함으로써 브로드캐스트 인증을 제공한다. 발급된 대칭키는 안전성을 위해 주기적으로 갱신되어야 한다. 갱신을 위해 서버와의 통신이 필요하지만, DSRC를 사용할 경우 서버와의 통신이 항상 이루어진다고 보장할 수 없다. 따라서 대칭키 발급 및 갱신 과정에 다른 통신 메커니즘의 사용을 고려한다.

본 논문은 다음과 같이 구성된다. 2장에서는 제안하는 프로토콜의 환경을 정의하고, 3장에서 제안하는 프로토콜을 기술한다. 4장에서는 제안하는 프로토콜의 안전성을 분석하고, 5장에서 결론은 맺는다.

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2011-C1090-1111-0010).
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. 2011-0000189).

2. 환경 구성

이 장에서는 제안하는 프로토콜에서 사용하는 그룹과 키 갱신을 위한 방법들을 비교하고, 제안하는 프로토콜에 적합한 환경을 구성한다.

2.1 그룹 구성

그룹을 구성하는 형태로는 전체를 하나의 단일 그룹으로 구성하는 방법과 여러 그룹으로 나누어 구성하는 방법이 있다. 제안하는 프로토콜에 적합한 그룹을 구성하기 위해 두 방법 사이에 비교해야할 사항으로는 키 발급 및 갱신을 위한 통신비용, 키가 노출이 되었을 경우 위험 범위, 차량 철회 등이 있다.

전체를 하나의 단일 그룹으로 구성할 경우에는 모든 차량이 같은 그룹이기 때문에 그룹의 가입 및 탈퇴에 따른 키 발급 요구가 발생하지 않는다. 또한 그룹에 가입하여 키를 발급받은 이후 정해진 규칙에 따라 갱신을 위한 통신만 발생하게 된다. 하지만 그룹키가 노출이 될 경우 위험 범위가 모든 차량에 미치게 되며, 모든 차량의 그룹키를 변경하여야 한다. 차량 철회는 대상 차량을 구분하여 다른 차량들의 그룹키를 갱신하는 방법으로 철회가 가능하다. 여러 그룹으로 구성하는 방법도 그룹에 가입하여 키를 발급 받은 이후 정해진 규칙에 따라 갱신을 위한 통신이 발생한다. 하지만 차량의 이동에 따라 그룹의 가입 및 탈퇴가 발생하게 되며, 따라서 추가적인 통신이 필요하게 된다. 그룹키가 노출될 경우에는 해당 그룹만 영향이 있으며, 그룹키가 노출된 그룹의 차량들만 그룹키를 변경해 준다. 차량 철회는 단일 그룹일 때와 같이 대상 차량을 구분하여 다른 차량들의 그룹키를 갱신하는 방법으로 가능하며, 추가적인 방법으로 그룹장들 사이에 철회리스트를 공유하고 그룹 이동 시 그룹키를 발급하지 않는 방법으로 차량 철회가 가능할 수 있다.

위의 비교를 통해 전체를 하나의 단일 그룹으로 구성하였을 때는 보다 효율성이 높으며, 여러 그룹으로 나누어 구성하였을 때는 보다 안전성이 높다는 것을 알 수 있다. VANET의 보안 프로토콜은 안전성만 고려해야할 것이 아니라 효율성까지 고려해야 한다. 하지만 제안하는 프로토콜은 대칭키를 기반으로 하여 효율성을 높이는 것을 고려하고 있기 때문에 여러 그룹으로 구성하는 것이 안전성과 효율성을 고려한 보다 적합한 방법이라고 할 수 있다. 따라서 제안하는 프로토콜은 여러 그룹으로 나누어 그룹을 구성하는 환경을 사용한다.

여러 그룹으로 나누어 그룹을 구성할 때, 동적인 그룹을 적용할 것인지, 지역적으로 정적인 그룹을 구성할 것인지를 고려해 볼 수 있다. 동적인 그룹을 구성할 때는 각 차량 간의 속도 차이로 인하여 예상하지 못한 그룹의 가입과 탈퇴가 빈번하게 발생할 수 있다. 이는 차량에서 그룹키 발급을 위한 통신요구가 빈번하게 발생하여 효율성을 악화시킨다고 볼 수 있다. 따라서 제안하는 프로토콜에서는 지역적으로 고정된 여러 그룹을 사용하여 그룹을 구성한다.

2.2 키 갱신 방법

대칭키의 안전성을 강화하기 위해 요구되는 키 갱신은 각 차량 별로 서로 다른 시간에 갱신을 하는 방법과 전체 차량이 같은 시간에 갱신하는 방법으로 나누어 볼 수 있다. 제안하는 프로토콜에 적합한 키 갱신 방법을 적용하기 위해 두 방법 사이에 비교해야할 사항으로는 차량 철회를 제공하는 것과 그룹 내의 모든 차량에 동일한 그룹키를 제공하는 것이 있다.

각 차량 별로 서로 다른 시간에 갱신을 할 때, 그룹장은 철회리스트에서 각 차량을 확인하여 그룹키를 발급하는 방법으로 차량 철회를 제공할 수 있다. 하지만 차량 별로 서로 다른 시간에 갱신이 이루어지기 때문에 그룹 내의 모든 차량이 동일한 그룹키를 소유하지 못하게 된다. 앞으로 사용할 키를 미리 발급받는 방법으로 모든 차량에 동일한 그룹키를 제공할 수 있지만, 이는 키를 미리 발급받고 그룹에서 탈퇴를 하였을 때 키의 안전성을 훼손할 수 있다. 전체 차량이 같은 시간에 갱신하는 방법도 그룹장이 철회리스트에서 각 차량을 확인하여 그룹키를 발급하여 차량 철회를 제공할 수 있다. 또한 같은 시간대에 모든 차량에서 키 갱신이 일어나므로 동일한 그룹키가 제공된다. 하지만 같은 시간대에 모든 차량에서 키 갱신이 요구된다는 점에서 통신 요청의 병목현상이 발생할 수 있다.

위의 비교를 통해 각 차량 별로 서로 다른 시간에 갱신을 할 때는 통신량의 병목현상은 발생하지 않지만 안전성이 훼손되며, 전체 차량이 같은 시간에 갱신을 할 때는 안전성은 훼손되지 않지만 통신량의 병목현상이 발생하는 것을 알 수 있다. 각 차량 별로 서로 다른 시간에 갱신하는 방법은 키 갱신으로 인하여 키가 노출될 수 있고 안전성을 제공하지 못하기 때문에 제안하는 프로토콜에서 고려될 수 없다. 같은 시간에 갱신하는 것으로 발생하는 통신량의 병목현상은 어느 정도 완충 시간대를 두고 그 시간대 내에 랜덤하게 분산하는 것으로 보완할 수 있다. 따라서 제안하는 프로토콜은 키 갱신 방법으로 모든 차량이 같은 시간대에 갱신하는 방법을 사용한다.

3. 제안하는 프로토콜

이 장에서는 제안하는 프로토콜에 대해서 설명한다. 제안하는 프로토콜은 차량 등록 과정, 그룹키 요청 과정, 그룹키 갱신 과정, 메시지 인증 과정, 신원 확인 과정으로 이루어진다. 사용한 표기법은 <표 1>과 같다.

<표 1> 제안하는 프로토콜의 표기법

표기법	내용
VID	차량의 실제 ID
PID	차량의 익명 ID
T	타임스탬프
K_G	그룹키
K_V	개별 차량키
$HMAC_K()$	K를 사용한 $HMAC()$

<표 2> GTA에서 저장하는 정보

차량	실제 ID	익명 ID	개별 차량키
V_1	ID_1	PID_1	K_{v1}
V_2	ID_2	PID_2	K_{v2}
V_3	ID_3	PID_3	K_{v3}
⋮	⋮	⋮	⋮

3.1 차량 등록 과정

차량이 시스템이 등록하는 과정으로 최초에 1번 수행된다. 최초 차량의 TRH에는 차량의 실제 ID와 개별 차량키가 저장되어 있으며, 차량은 GTA(Geographically Trusted Authority)에 ID를 등록하고 익명 ID, 그룹키를 발급받아 차량의 TRH에 저장한다. GTA에 저장되는 정보는 <표 2>와 같으며, 과정은 (그림 1)과 같다.

3.2 그룹키 갱신 과정

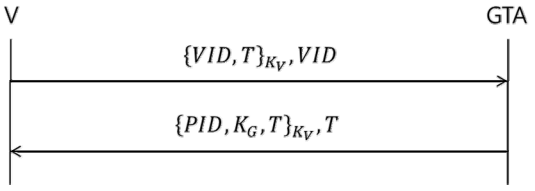
차량이 발급받은 그룹키를 갱신하는 과정이다. 모든 차량이 주기적으로 같은 시간대에 갱신하며, 갱신 시간은 정책적으로 12시간이나 24시간 주기로 결정할 수 있다. 갱신 시간 전에 완충 시간대를 두어 그 기간 사이에 차량에서 임의의 시간을 선택하여 갱신 요청을 하도록 한다. 갱신된 키는 3.1절의 차량 등록 과정과 같이 차량의 TRH에 저장된다. 과정은 (그림 2)과 같다.

3.3 그룹키 요청 과정

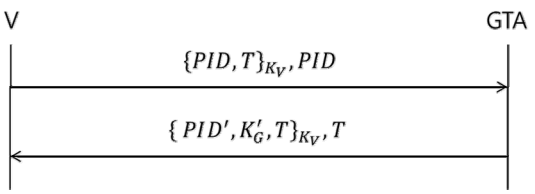
차량이 그룹을 이동할 때 그룹키를 요청하는 과정으로, 새로운 그룹으로 이동할 때는 3.1절의 차량 등록 과정을 수행하며, 등록된 그룹으로 이동할 때는 3.2절의 그룹키 갱신 과정으로 그룹키 갱신을 요청한다.

3.4 메시지 인증 과정

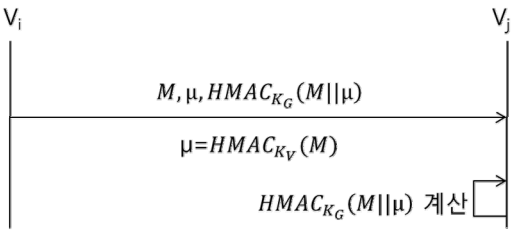
차량 간에 메시지를 송신하고, 수신하여 메시지를 인증하는 과정이다. 수신된 메시지에 포함된 인자인 M과 $HMAC_{K_V}(M)(=\mu)$를 메시지를 수신한 차량에서 그룹키로 $HMAC()$한 후, 메시지에 포함된 인자 $HMAC_{K_G}(M||\mu)$과 비교를 하여 같은 그룹 내의 차량에서 송신된 메시지인지 확인한다. 과정은 (그림 3)과 같다.



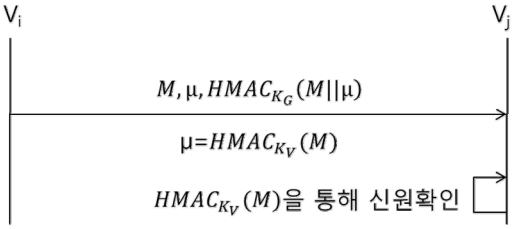
(그림 1) 차량 등록 과정



(그림 2) 그룹키 갱신 과정



(그림 3) 메시지 인증 과정



(그림 4) 신원 확인 과정

3.5 신원 확인 과정

차량에 발급된 개별 차량키로부터 메시지를 송신한 차량의 신원을 확인하는 단계이다. 문제를 일으킨 차량이나 사고 책임자는 GTA에 의해 메시지의 익명성을 철회하여 차량의 신원을 확인할 수 있어야 한다. GTA는 메시지에 포함된 M을 <표 2>에 저장하고 있는 개별 차량키를 이용해 $HMAC()$한 후, 메시지에 포함된 인자 $HMAC_{K_V}(M)$과 비교하여 차량의 신원을 찾는다. 그 후, 철회 대상 차량의 확인된 ID를 철회리스트에 추가한다.

지역별로 구성되어 있는 GTA 간에는 철회리스트를 공유하며, GTA들의 상위 계층으로 TA(Trusted Authority)를 구성하여 철회 정보를 공유할 수 있다. 공유된 철회리스트를 통해 3.1절의 차량 등록 과정에서 그룹키 발급 요청을 거부할 수 있으며, 3.2절의 그룹키 갱신 과정에서 그룹키 갱신 요청을 거부할 수 있다.

3.6 다른 통신 메커니즘 적용

앞서 언급했듯이, 차량에서 그룹키의 발급 및 갱신을 위해서는 서버와의 통신이 필요하다. 하지만 DSRC를 사용할 경우 서버와의 통신이 어디서든지 항상 이루어진다고 보장할 수 없다. 따라서 GTA와 통신 과정에 다른 장거리 통신 메커니즘을 적용하는 것을 고려해 볼 수 있다.

위성통신, 이동통신, WiBro 등 여러 가지 장거리 통신망이 있지만, 구축상태 및 사용비용을 고려하였을 때, 이동통신이 가장 적합하도고 할 수 있으므로 제안하는 프로토콜에서는 이동통신의 사용을 고려한다.

이동통신이 적용된 시나리오는 먼저 차량이 이동통신망을 이용하여 GTA에 차량을 등록한다. 그 후, DSRC를 사용하여 차량 및 RSU(Road-Side infrastructure Units)와 통신하고, GTA와의 그룹키 갱신은 다시 이동통신망을 사용하여 수행한다. 그룹키 요청 과정 또한 3.1절 차량 등록 과정과 3.2절 그룹키 갱신 과정을 수행하므로 이동통신망을 이용한다. 여기서 이동통신망의 사용비용은 정책적으로 결정될 부분이기 때문에 고려하지 않는다.

4. 안전성 분석

이 장에서는 제안하는 프로토콜의 안전성에 대해 분석한다. 분석에 앞서 VANET의 보안 요구사항들에 대해 살펴본 후, 제안하는 프로토콜이 보안 요구사항들을 만족하는 지에 대해 분석한다.

4.1 보안 요구사항

VANET에서 안전하고 신뢰성 있는 통신을 보장하기 위해서는 다음과 같은 보안 요구사항들을 만족해야 한다.

- 메시지 인증(Message Authentication): 메시지 수신 차량은 자신이 수신한 메시지가 VANET 시스템에 등록된 정당한 차량에 의한 것인지 확인할 수 있어야 한다.
- 무결성(Integrity): 메시지 수신 차량은 자신이 수신한 메시지가 전송 중간에 위/변조 되었는지 확인할 수 있어야 한다.
- 부인방지(Non-repudiation): 사고와 같은 분쟁이 발생할 경우, 책임 회피를 방지하기 위해 자신이 보낸 메시지에 대해 부인할 수 없어야 한다.
- 조건부 익명성(Conditional Anonymity): 익명성이 보장된 차량의 신원확인이 필요할 경우, 차량의 신원은 신뢰기관에 의해 확인될 수 있어야 한다.

위의 보안 요구사항을 바탕으로 강한 프라이버시를 보장하기 위해서는 다음 두 가지 요구사항을 만족해야 한다.

- 불관찰성(Unobservability): 개별 메시지에 대해 해당 메시지를 방송한 차량을 식별할 수 없어야 한다.
- 불연결성(Unlinkability): 같은 차량이 송신한 두 메시지를 서로 연결할 수 없어야 한다.

4.2 보안 요구사항 분석

앞서 살펴본 VANET의 보안 요구사항을 제안하는 프로토콜이 만족하는지에 대해 안전성을 분석한다.

- 메시지 인증: 각 차량은 메시지에 포함된 인자들과 발급받은 그룹키를 사용하여 계산을 한 후, 메시지에 포함된 인자 $HMAC_{K_G}(M\|\mu)$와 비교를 한다. 계산된 값과 메시지에 포함된 값이 같을 경우 같은 그룹에 등록된 차량에 의한 메시지인지 확인할 수 있다.
- 무결성: 메시지 수신 차량은 메시지에 포함된 M과 $HMAC_{K_V}(M)(=\mu)$을 사용하여, $HMAC_{K_G}(M\|\mu)$를 계산하기 때문에, 메시지의 세 인자 중 어떤 값이 위/변조 될 경우에도 확인할 수 있다.
- 부인방지: 차량에 발급된 개별 차량키는 TRH에 의해 위/변조 될 수 없으며, 안전하게 저장된다. 차량은 발급된 개별 차량키를 사용한 $HMAC_{K_V}(M)$을 메시지에 포함하게 되며, 메시지 송신을 부인할 수 없다.
- 조건부 익명성: GTA는 차량의 신원확인이 필요할 경우, 메시지의 익명을 철회하여 신원확인이 필요한 차량의 신원을 확인할 수 있다. GTA에 저장된 개별 차량키로 메시지에 포함된 M을 $HMAC()$한 후, 메시지에 포함된 $HMAC_{K_V}(M)$과 비교하여 차량의 신원을 확인할 수 있다.
- 불관찰성: 차량이 송신한 메시지는 $M, HMAC_{K_V}(M)(=\mu), HMAC_{K_G}(M\|\mu)$로 구성되어 있다. 메시지 필드 내에는 차량의 신원을 나타내는 인자가 포함되어 있지 않으므로 메시지의 송신 차량을 식별할 수 없다.
- 불연결성: 메시지 필드 내에 포함된 인자는 모두 M과 M의 연산으로 생성되는 값들이다. M은 속도, 방향, 사고정보 등을 포함하기 때문에 메시지마다 서로 다른 값을 가지며, M으로 생성되는 인자들도 메시지마다 서로 다른 값을 가지게 된다. 따라서 같은 차량에서 보낸 메시지들을 연결시킬 수 없다.

5. 결론

본 논문에서는 대칭키를 사용한 인증 프로토콜을 제안하였다. 제안하는 프로토콜은 공개키 기반 인증의 매우 큰 연산량을 해결할 수 있으며, 차량과 서버간의 통신을 어디서든지 보장할 수 있다. 하지만 키 갱신의 주기에 따라 철회 대상 차량이 어느 정도 VANET을 이용할 수 있다는 단점이 있다. 향후 연구에서는 제안하는 프로토콜의 단점을 개선하며, 시뮬레이션을 통한 효율성 분석을 진행할 계획이다.

참고문헌

[1] M. Raya and J. P. Hubaux, "Securing Vehicular Ad hoc Networks," Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007.

[2] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications," IEEE Transaction on Vehicular Technology, Vol. 56, No. 6, pp. 3442-3456. 2007.

[3] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," Proceedings - IEEE INFOCOM, pp. 1903-1911, 2008.

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

[5] X. Lin, X. Sun, X. Wang, C. Zhang, P. Ho, and X. Shen, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving" IEEE Transaction on Wireless Communications, Vol. 7, No. 12, pp. 4987-4998, 2008.

[6] C. Zhang, X. Lin, R. Lu, and P. Ho, "RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks," IEEE International Conference on Communications, art. no. 4533317, pp. 1451-1457, 2008.

[7] Klaus Plößl and Hannes Federrath, "A Privacy aware and Efficient Security Infrastructure for Vehicular Ad hoc Networks," Computer Standards and Interfaces, Vol. 30, No. 6, pp. 390-397, 2008.