VANET에서 대칭키 기반의 개선된 메시지 인증 기법*

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

Enhanced Message Authentication Scheme in VANET based on Symmetric Key*

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

VANET에서 V2V, V2I 통신을 통해 다양한 서비스를 이용하기 위해서는 안전하고 신뢰성 있는 통신이 보장되어야 한다. 이를 위해 다양한 연구들이 진행되었으며, 기존 연구들 중 대칭키를 사용한 방법으로는 RAISE가 있다. RAISE는 대칭키를 기반으로 하였기 때문에 다른 연구들 보다 낮은 통신 및 연산 비용을 가진다. 하지만 메시지에 대한 인증을 즉시 제공하지 못하며, RSU가 불능이 되거나 존재하지 않는 환경에서는 차량이 서비스를 제공받지 못한다는 문제점이 있다. 본 논문에서는 이러한 문제점을 해결하기 위해 대칭키 기반의 그룹키와 식별자를 사용하여 메시지 인증을 제공하고, 메시지 인증 과정에서 RSU에 비의존적인 인증 프로토콜을 제안한다.

1. 서론

차량과 인프라 간 통신은 물론 차량 간에 통신으로 형성된 애드혹 망을 차량 애드혹 네트워크(VANET, Vehicular Ad hoc NETwork)라 한다. VANET은 차량과 RSU(Road-Side Infrastructure Units)로 구성되어 있다.

VANET의 통신 형태는 차량과 차량 간의 통신(V2V, Vehicular to Vehicular)과 차량과 기반시설 간의 통신(V2I, Vehicular to Infrastructure)이 있다. 차량이 V2V, V2I 통신을 통해 다양한 서비스를 이용하기 위해서는 안전하고 신뢰성 있는 V2V, V2I 통신이 보장되어야 하며, 이를 위해 많은 연구들이 진행되었다.

2007년 Raya와 Hubaux는 차량의 프라이버시를 보호하기 위해 신뢰기관으로부터 다량의 익명인증서를 발급받아서 사용하는 방법을 제안하였다[1]. 차량이 다량의 익명인증서를 발급받고 저장해야한다는 문제점을 개선하기 위해, 2007년 Lin 등은 V2V 통신에 그룹 서명을 사용한 방법인 GSIS를 제안하였고[2], 2008년 Lu 등은 RSU가 차량에 단기간 익명인증서를 발급해주는 방법인 ECPP를 제안하였다[3]. 2008년 Zhang 등은 낮은 통신비용을 위해 HMAC을 사용하는 방법인 RAISE를 제안하였고[4], 같은 해에 Zhang 등은 복잡한 인증서 관리 문제를 해결하기 위해 신원기반 암호시스템을 적용한 방법을 제안하였다[5].

위의 연구들 중 대칭키를 사용하는 방법으로는 RAISE가 있다. RAISE는 대칭키를 기반으로 하였기 때문에 기존의 공개키를 기반으로 한 다른 연구들보다 낮은 통신 및 연산 비용을 가진다는 장점이 있다. 하지만 메시지를 즉시 인증하지 못하며, 인증 과정이 RSU에 의존적이고, 차량 철회를 지원하지 않는 등 몇 가지 문제점을 가지고 있다. 본 논문에서는 RAISE가 가지는 문제점을 해결하기 위해 대칭키 기반의 그룹키와 식별자를 사용하며 메시지 인증을 제공하고, 메시지 인증 및 키 발급 등의 과정에서 RSU에 비의존적인 인증 프로토콜을 제안한다.

본 논문의 2장에서는 관련 연구인 RAISE에 대해서 살펴보고 문제점을 파악한다. 3장에서는 제안하는 프로토콜을 소개하며, 4장에서는 제안하는 프로토콜이 보안 요구사항을 만족하는지에 대한 안전성 분석을 한다. 그리고 5장에서 결론을 맺는다.

2. 관련연구

이 장에서는 RAISE가 제공하는 방법에 대해서 살펴보고, RAISE가 가지는 문제점에 대해서 파악한다. 그리고 문제점에 대한 개선점을 도출한다.

* 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).

<표 1> RAISE에서 사용하는 표기법

표기법	내용
K_i	차량 V_i와 RSU R 간의 대칭키
VID	V_i에 발급된 익명 ID
SK_U	U의 개인키
$\{\ \}_{SK_U}$	U의 개인키를 이용한 서명
$H()$	일방향 해쉬 함수
$HMAC()$	해쉬 된 메시지 인증 코드

2.1 RAISE

RAISE는 RSU를 사용한 메시지 인증 방법으로, 대칭키 확립, 해쉬 통합, 검증의 3단계로 나뉜다. RAISE에서 사용된 표기법은 <표 1>과 같다.

2.1.1 대칭키 확립

RSU와 차량 사이에 사용할 대칭키를 확립하고, RSU가 차량에 익명 ID를 발급하는 단계이다. RSU와 각 차량 사이에 서로 다른 대칭키를 확립하게 되며, 익명 ID는 K-ANONIMITY 방법[6]을 사용하여 여러 차량에 동일한 ID를 중복해서 발급받는다.

2.1.2 해쉬 통합

RSU가 차량들이 보낸 메시지를 식별 및 검증하여 방송하는 단계이다. 차량은 메시지 $VID\|M_i\|HMAC(VID\|M_i)$를 방송한다. RSU는 차량의 메시지를 식별 및 검증한 후, 통합하여 $HAggt = H(VID\|M_1)\|\cdots\|H(VID\|M_n)$를 생성한다. 그리고 주기적으로 $HAggt\|\{HAggt\}_{SK_R}$를 방송한다.

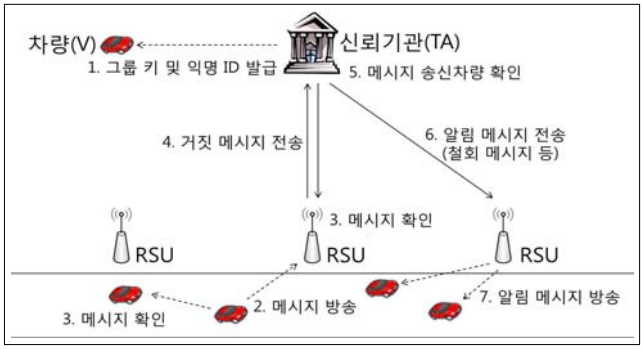
2.1.3 검증

차량이 주변 차량에서 받은 메시지와 RSU로부터 받은 메시지를 비교하여 검증하는 단계이다. 차량은 주변 차량에서 받은 메시지의 VID와 M_i으로 $H(VID\|M_i)$를 계산하여 저장한다. 그리고 $H(VID\|M_i)$가 RSU로부터 받은 $HAggt\|\{HAggt\}_{SK_R}$에 있는지 확인하여 메시지를 검증한다.

2.2 RAISE의 문제점

RAISE에서 차량들은 RSU로부터 주기적으로 수신한 메시지에 주변 차량들로부터 수신한 메시지가 포함되어 있는지 확인하여 메시지를 검증한다. 따라서 차량은 메시지를 수신한 즉시 인증할 수 없다. 또한 RSU가 메시지를 식별 및 검증하기 때문에 RSU가 불능이 되거나 존재하지 않는 구간에서는 RSU로부터 확인된 메시지를 수신하지 못하기 때문에, 메시지를 검증하지 못한다.

이러한 RAISE의 문제점을 해결하기 위하여, 본 논문에서는 차량이 수신한 메시지를 바로 검증할 수 있도록, 그룹키와 식별자를 이용하여 메시지에 대한 인증을 제공한다. 그리고 RSU가 존재하지 않는 구간에서도 유연하게 메시지를 인증하기 위해, 그룹키 발급 및 메시지 인증에 RSU가 관여하지 않도록 하였다. 또한 하위 그룹을 설정하여 문제를 일으킨 차량에 대한 철회를 제공하였다.



(그림 1) 제안하는 프로토콜의 전체 구성과 과정

3. 제안하는 프로토콜

이 장에서는 제안하는 프로토콜에 대해서 설명한다. 제안하는 프로토콜은 시스템 설정 단계, 차량 등록 단계, 메시지 전송 단계, 메시지 확인 단계, 신원 확인 단계, 차량 철회 단계로 나뉜다. 전체 시스템의 기본적인 구성과 과정은 (그림 1)과 같으며, 제안하는 프로토콜에서 사용한 표기법은 <표 2>와 같다.

3.1 시스템 설정 단계

신뢰기관(TA, Trusted Authority)은 VANET에서 사용할 암호 알고리즘과 일방향 해쉬 함수를 선정한다. 그리고 TA는 Q_S와 q_S를 선택하고, C_S를 생성한다. 각 차량은 Q_V와 q_V를 선택하고, C_V를 TA로부터 발급받는다.

3.2 차량 등록 단계

차량이 TA에 신원을 등록하고, 사용할 인자를 발급받는 단계이다. TA는 차량의 신원정보를 저장하기 위해 <표 3>과 같은 차량리스트를 관리한다.

1) 차량 V_i는 TA에 Q_{V_i}와 C_{V_i}를 보낸다.

2) TA는 V_i에게 발급할 VID_i와 R_i를 생성한다.

3) TA는 VID_i와 R_i, G_1ID, G_2ID를 그룹키 K로 암호화하고, K는 공개키로 암호화하여 V_i에 보낸다. 즉, $C_S, \{\{K\}_{-Q_S}\}_{+Q_V}, H(K), \{VID_i, R_i, G_1ID, G_2ID\}_K$를 V_i에 보낸다.

4) V_i는 메시지를 복호화한 후, $VID_i, R_i, K, G_1ID, G_2ID$를 TRH(Tamper Resistant Hardware)에 저장한다.

<표 2> 제안하는 프로토콜의 표기법

표기법	내용
$Q_S/\ q_S/\ C_S$	서버의 공개키 / 개인키 / 인증서
$Q_V/\ q_V/\ C_V$	차량의 공개키 / 개인키 / 인증서
VID_i / R_i	차량 i에 발급되는 익명ID / 랜덤값
G_1ID / K	모든 차량에 발급되는 그룹ID / 그룹키
G_2ID	차량이 속하게 되는 하위 그룹ID
$H()$	일방향 해쉬 함수
$\{\ \}_{-A}$	개인키 A를 이용한 서명
$\{\ \}_{+A}$	공개키 A를 이용한 암호화
$\{\ \}_A$	대칭키 A를 이용한 암호화

<표 3> 신뢰기관에서 관리하는 차량리스트

그룹	차량 ID	차량 인증서
G_2ID_1	VID_1	C_1
G_2ID_1	VID_2	C_2
G_2ID_1	VID_3	C_3
G_2ID_2	VID_4	C_4
G_2ID_2	VID_5	C_5
⋮	⋮	⋮

차량 등록 단계는 K의 갱신을 위해 각 차량마다 일정 주기마다 다시 거친다. 이 과정에서 새로운 K를 발급하며, 철회 대상 차량에 대해서는 발급하지 않는다. 그리고 TRH의 정보는 손상되지 않는다고 가정한다.

3.3 메시지 전송 단계

V_i는 TA로부터 발급받은 $VID_i, R_i, K, G_1ID, G_2ID$를 사용하여 메시지를 구성한다. 교통관련 정보 및 이벤트 정보를 포함하는 M에 대한 메시지 생성과정은 다음과 같다.

1) V_i는 메시지 수신 차량에서 M을 인증하기 위한 인자 $G_2ID, \{G_1ID, VID_i \bullet R_i\}_K, M, H(M \| VID_i \bullet R_i)$를 생성한다.

2) V_i는 M에 대해 TA에서 메시지 송신 차량을 확인하기 위한 $\{R_i\}_{+Qs}, \{\{M \| VID_i\}_{-Q_V}\}_{+Qs}$ 를 생성한다.

3) 생성된 두 인자를 합하여 $G_2ID, \{G_1ID, VID_i \bullet R_i\}_K, M, H(M \| VID_i \bullet R_i), \{R_i\}_{+Qs}, \{\{M \| VID_i\}_{-Q_V}\}_{+Qs}$ 를 방송한다.

메시지에서 R_i는 메시지마다 변경된다. 이에 따라 VID_i는 R_i와 $VID_i \bullet R_i$ 연산을 통해 지속적으로 갱신된다.

3.4 메시지 확인 단계

수신한 메시지가 시스템에 등록된 정당한 차량으로부터 송신된 메시지인지 확인하는 단계이다. 한 차량에서 방송한 메시지를 주변 차량과 RSU가 수신하면, 먼저 M에 포함된 시간 정보로 유효한 시간 내의 메시지인지 확인한다. 그리고 그룹키 및 그룹ID를 통해서 메시지를 인증한다.

1) 수신된 메시지의 $\{G_1ID, VID_i \bullet R_i\}_K$를 공통된 그룹키 K로 복호화 하여, G_1ID와 $VID_i \bullet R_i$를 획득한다.

2) 공통된 그룹ID G_1ID를 확인하여 메시지가 정당한 송신차량으로부터 송신된 메시지인지 확인한다.

3) M과 $VID_i \bullet R_i$를 해쉬한 후, $H(M \| VID_i \bullet R_i)$와 비교하여 메시지의 무결성을 확인한다.

3.5 신원 확인 단계

TA가 차량의 신원확인이 필요할 경우, 송신 차량의 신원을 확인하는 단계이다. 차량과 RSU에서 메시지 확인 단계를 거쳐 유효한 메시지들을 확인하고, 거짓 정보를 담고 있는 메시지가 있으면, TA에 메시지를 전송한다. TA는 다음 과정을 통해 차량의 신원을 확인한다.

<표 4> 신뢰기관에서 관리하는 철회리스트

철회 리스트	기간
C_6	T_1
C_7	T_2
C_8	T_3
⋮	⋮

1) TA는 $\{R_i\}_{+Qs}$를 복호화 하여, R_i을 획득한다.

2) $\{G_1ID, VID_i \bullet R_i\}_K$를 복호화 하여, $VID_i \bullet R_i$를 획득하고, R_i과 연산을 통해 VID_i를 획득한다.

3) VID_i를 <표 3>에서 검색하여, 차량의 신원정보를 확인한다.

3.6 차량 철회 단계

TA에서 철회 대상 차량의 신원이 확인되면, 그 차량을 VANET으로부터 철회하는 단계이다. TA는 철회 차량을 저장하기 위해 <표 4>과 같은 철회리스트를 관리한다. 제안하는 프로토콜의 G_2ID를 사용하여 철회하는 두 가지 방법에 대한 과정은 다음과 같다.

1) 차량의 등록을 갱신하는 방법

a) 철회 대상 차량이 소속된 그룹이 G_2ID_1이라고 하면, TA는 G_2ID_1에 대한 철회 메시지를 RSU에 보내고, RSU는 철회 메시지를 방송한다.

b) 철회 메시지를 수신한 차량은 소속된 그룹이 G_2ID_1일 경우, 차량 등록 단계를 다시 수행하여 새로운 G_2ID를 발급 받는다. 소속된 그룹이 G_2ID_1이 아닐 경우, 메시지를 무시한다.

c) TA는 차량 등록 단계에서 철회리스트에 포함된, 철회 대상 차량에 대해서는 프로토콜을 중지한다.

d) 이후, G_2ID_1이 사용된 메시지는 무시한다.

2) 새로운 G_2ID를 발급하는 방법

a) 철회 대상 차량이 소속된 그룹이 G_2ID_1이라고 하면, TA는 G_2ID_1에 대한 철회 메시지를 RSU에 보내고, RSU는 철회 메시지를 방송한다.

b) 철회 대상을 제외한 G_2ID_1를 사용하는 차량들에게 새로운 G_2ID를 암호화하여 철회 메시지와 함께 보낸다.

$$G_2ID_1, \{\{G_2ID_3\}_{-Qs}\}_{+Q_{V_1}}, \{\{G_2ID_3\}_{-Qs}\}_{+Q_{V_2}}, \cdots$$

c) 철회 메시지를 수신한 차량은 소속된 그룹이 G_2ID_1일 경우, 새로 발급된 G_2ID_3을 G_2ID로 사용한다. 소속된 그룹이 G_2ID_1이 아닐 경우, 메시지를 무시한다.

d) 이후, G_2ID_1이 사용된 메시지는 무시한다.

4. 안전성 분석

이 장에서는 제안하는 프로토콜의 안전성에 대해 분석한다. 분석에 앞서 VANET의 보안 요구사항들에 대해 설펴본 후, 제안하는 프로토콜이 보안 요구사항들을 만족하는지에 대해 분석한다.

4.1 보안 요구사항

이 절에서는 안전하고 신뢰성 있는 통신을 보장하기 위해 만족해야하는 보안 요구사항들을 정의한다.

- 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): 일반 차량의 프라이버시는 보호하면서 문제를 일으킨 차량의 신원은 신뢰기관에 의해 확인할 수 있어야 한다.

위의 보안 요구사항을 바탕으로 VANET에서 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 보낸 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 차량 등록 단계에서 공통된 그룹키 K와 그룹ID G_1ID를 발급받는다. 메시지를 수신한 차량은 K로 메시지의 $\{G_1ID, VID_i \bullet R_i\}_K$를 복호화한 후, G_1ID를 확인하여 시스템에 등록된 차량에 의한 메시지인지 확인할 수 있다.
- 무결성: 메시지 수신 차량은 $\{G_1ID, VID_i \bullet R_i\}_K$를 복호화 하여 획득한 $VID_i \bullet R_i$와 M을 해쉬하여 무결성을 확인할 수 있다.
- 부인방지: 메시지의 $\{\{M \| VID_i\}_{-Q_V}\}_{+Q_S}$에 포함된 차량의 서명으로 부인방지를 보장할 수 있다.
- 조건부 익명성: TA에서 $\{R_i\}_{+Q_S}$로부터 획득한 R_i와 $VID_i \bullet R_i$의 연산을 통해 각 차량에 발급한 익명 ID VID_i를 확인할 수 있다.
- 불관찰성: 메시지에서 VID_i는 R_i과 연산이 되어 $VID_i \bullet R_i$로 포함된다. 그리고 R_i는 서버의 공개키로 암호화되어 있기 때문에 서버만 확인할 수 있다. 따라서 불관찰성을 만족한다.
- 불연결성: 메시지에 포함된 R_i는 메시지마다 지속적으로 갱신되기 때문에 $VID_i \bullet R_i$는 메시지마다 다른 값을 가진다. 따라서 같은 차량이 보낸 메시지들을 확인할 수 없기 때문에 불연결성을 만족한다.

5. 결론

본 논문에서는 대칭키를 사용한 인증 프로토콜을 제안하였다. 대칭키를 사용한 기존 연구에서 발생하는 메시지 인증 시간의 지연, RSU에 의존적인 환경의 문제를 해결하였으며, 기존 연구에서 제공하지 않았던 차량 철회를 제공하였다. 하지만 제안하는 프로토콜은 차량이 TA로부터 수신한 인자들이 TRH에 저장되어 차량이 임의로 변경할 수 없어야 한다는 조건을 가진다. 그리고 차량의 철회 과정에서 철회 대상이 아닌 몇몇 차량에서도 연산 및 통신이 필요하다는 단점이 있다. 향후 연구에서는 제안한 프로토콜의 단점을 개선하며, 시뮬레이션을 통해 기존 연구보다 효율적임을 보이도록 하겠다.

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] C. Zhang, X. Lin, R. Lu, and P. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," IEEE International Comference on Communications, art. no. 4533317, pp. 1451-1457, 2008.

[5] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," Proceedings - IEEE INFOCOM, pp. 816-824, 2008.

[6] L. Sweeney, " K-ANONYMITY: a model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based System, Vol. 10, No. 5, pp. 557-570, 2002.