VANET 환경에서 안전한 통신을 위한 차량 등록 프로토콜†

(Vehicle Registration Protocol for Secure Communication in VANET Environment)

박 영 호*
(YoungHo Park)

요 약 VANET 응용을 안전하게 활용하기 위해서는 가입자를 확인하고 메시지 변조를 일으킬 수 있는 악의적인 가입자를 막는 인증이 필요하다. 본 논문에서는 VANET 환경에서 차량 등록을 위한 효율적인 인증 프로토콜을 제안한다. VANET은 차량이 고속으로 이동하는 빠르게 변하는 망이기 때문에 연산 부하가 적은 인증 프로토콜을 사용하는 것이 필요하다. 따라서, 제안한 프로토콜에서는 일방향 함수와 EOR 연산을 이용하여 차량 등록 인증을 수행한다.

핵심주제어 : 차량 ad hoc 네트워크, 차량 등록 프로토콜, 일방향 해쉬 함수

Abstract To operate safely VANET applications, authentication is necessary to identify valid participants and prevent malicious parties from modifying messages. This paper proposes an efficient authentication protocol for the vehicle registration in VANET environment. The topology of VANET changes rapidly due to high-speed movement of vehicles, thus it is need to reduce the computational burden of the authentication protocol. Therefore, this protocol uses only one-way hash functions and EOR operations to register vehicles.

Key Words : vehicular ad hoc network, vehicle registration protocol, one-way hash function

1. 서 론

최근 국내외적으로 IT 기술을 차량 통신에 적용시킨 지능형 교통시스템(ITS: intelligent transportation system)에 관한 연구가 활발히 이루어지고 있다. ITS는 점점 가속화되고 있는 정보화 사회에 알맞은 신속, 안전, 쾌적한 차세대 교통체계를 구현하는데 목적을 두고 있다. ITS의 핵심기술로 부상하고 있는 VANET (vehicular ad hoc network)은 지능형 차량에 무선통신 기술을 지원하기 위하여 IEEE802.11 [1] 기반의 기술을 사용하고 있다. [2-4]

VANET 환경에서의 응용들이 안전하고 신뢰성 있게 제공되기 위해서는 데이터 보호와 같은 보안성 확보가 필수적으로 해결되어야 한다. VANET은 정보가 쉽게 노출될 수 있는 이동 차량 통신 환경이라 더욱 중요하게 연구되어야 하며 정보보호 기술의 개발이

† 이 논문은 2010학년도 경북대학교 학술연구비에 의하여 연구되었음
* 경북대학교 산업전자전기공학부

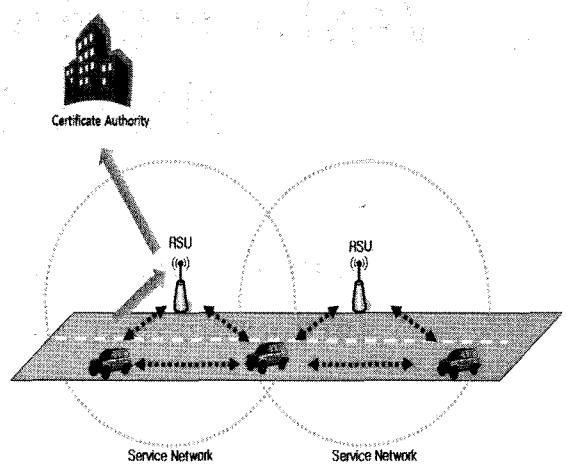
이러한 문제를 해결하는 최선의 대안이라 할 수 있다. VANET은 전파를 통한 무선 환경으로 제한된 대역폭을 사용해야 하며 이동 단말기의 계산 능력의 한계, 이동성과 다양한 부가 서비스 기능의 제공 등 많은 제약 요인과 특수성이 고려되어야 한다. 또한 이동 차량과 노변장치 간의 통신뿐만 아니라 가입자와 부가 서비스 제공자간의 통신도 고려해야 하므로 기존의 보안 프로토콜 및 알고리즘을 그대로 사용할 수 없다. 따라서 무선 환경 및 차량단말기 처리능력, 그리고 사용자와 부가 서비스 제공자간의 통신을 고려한 보안 프로토콜 및 알고리즘 개발이 이루어져야 한다. [2-5]

VANET에서의 보안기술에 관련된 연구는 최근 국내외에서 이루어지고 있다. IEEE 1609.2 [6] 에서는 안전한 차량 통신을 지원하기 위하여 WAVE(wireless access in vehicular environments)를 위한 보안기술 연구가 진행 중에 있다. IEEE 1609.2에서는 데이터 암/복호를 위해서 AES-CCM(advanced encryption standard - counter with CBC-MAC) [7] 알고리즘과 키를 암호화하기 위하여 ECIES(elliptic curve integrated encryption scheme) [6,8] 알고리즘을 사용하도록 권고하고 있으나 그 외 안전한 통신을 위한 구체적인 시나리오와 프로토콜은 없는 실정이다.

본 논문에서는 VANET 환경에서 인증센터가 차량을 인증하는 단방향 차량 등록 인증 프로토콜을 제안한다. V2I(vehicle to infrastructure)의 확장된 개념으로 차량이 노변장치인 RSU(road side unit)를 거쳐 CA(certificate authority)와 통신하여 통신상에 필요한 차량 인증을 제공한다. 차량과 인증 센터간의 공유된 키 검증자를 통해 CA가 생성한 세션 키의 안전한 분배가 이루어지게 되고 세션 키를 통해 생성한 인증 값과 차량의 인증 결과 값을 비교 검증하여 동일한 값일 경우 차량 등록 인증하게 된다.

2. VANET 환경에서의 차량 등록 프로토콜 시나리오

그림 1은 VANET 환경에서 정보보안 시스템의 시나리오를 나타낸 것이다. V2V(vehicle to vehicle) 및 V2I 통신에서 데이터를 암/복호하기 위하여 IEEE 1609.2에서는 데이터 암호화 알고리즘인 AES-CCM 방식을 권고하고 있으며 이 암호화 알고리즘에 사용할 키를 분배



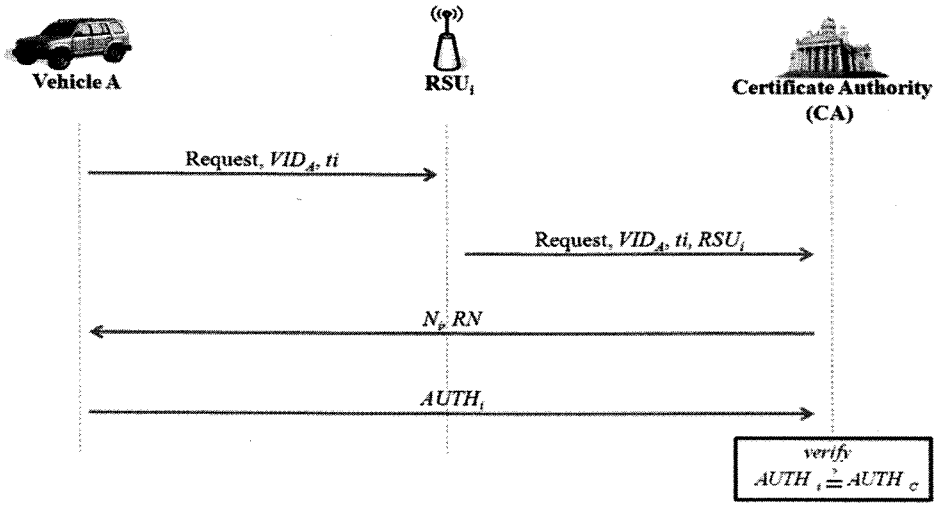
<그림 1> VANET 환경에서의 차량 등록 프로토콜 적용 시나리오.

하기 위하여 IEEE 1609.2에서는 키를 암호화하는 알고리즘인 ECIES의 사용을 권고하고 있다. 그러나 VANET 망에서의 과금 등의 서비스에 활용될 차량 인증 프로토콜에 관해서는 구체적인 연구결과가 없는 실정이다. 따라서 본 논문에서는 VANET 환경에서 인증센터가 차량을 인증하는 단방향 차량 등록 인증 프로토콜을 제안한다. 그림 1에서와 같이 차량이 노변장치인 RSU를 거쳐 CA와 통신하여 통신상에 필요한 차량 인증을 제공한다. 차량과 CA간의 공유된 키 검증자를 통해 인증 센터가 생성한 세션 키의 안전한 분배가 이루어지게 되고 세션 키를 통해 생성한 인증 값과 차량의 인증 결과 값을 CA에서 비교 검증하여 동일한 값일 경우 차량 등록 인증하게 된다.

3. VANET 에서의 차량 등록 프로토콜

VANET 환경은 통신상의 다수 차량들 간의 안전메시지 교환이나 다양한 응용서비스 제공 측면에서 안전하고 신뢰성 있게 제공되기 위해서는 가입자의 인증 및 데이터의 보호와 같은 보안성 확보가 필수적으로 해결되어야 한다.

본 논문에서 제안하는 VANET에서의 차량 등록 인증 프로토콜은 차량을 차량이 노변상의 RSU를 거쳐 CA와 통신을 통해 인증이 이루어지게 된다. 이때 인증 요청 차량의 키인 K_i의 검증자 $v_i = H[K_i]$는 차량과



<그림 2> VANET에서의 차량 등록 프로토콜.

인증 센터 간에 공유되었다고 가정한다. 본 프로토콜에 사용된 표기는 표 1과 같다.

VANET에서의 차량 등록 프로토콜은 그림 2와 같이 진행된다. 인증 대상 차량이 자신이 운행 중인 VANET 내의 RSU$_i$에게 인증 요청 메시지와 차량의 ID인 VID_i, 그리고 타임스탬프 t_i를 전송한다. 이 메시지를 받은 RSU는 인증 요청 차량이 보내 메시지에 RSU의 고유 식별 번호인 RSU$_i$을 포함시켜 CA에게 전송한다.

<표 1> 차량 등록 프로토콜 표기

VID_i	차량 i의 ID
t_i	차량 i의 타임스탬프
RSU_i	노변장치 RSU의 고유 식별 번호
RN	난수
v_i	차량 i의 키 검증자 ($H[K_i]$)
K_s	세션 키
$H[]$	해쉬 함수

CA에서는 식 (1)과 같이 N_i와 $AUTH_C$ 의 연산이 이루어진다. N_i는 공유된 인증 차량의 키 검증자 v_i와 타임스탬프 값으로 연산되기 때문에 인증 요청 차량이 안전하게 세션 키를 확인 할 수 있게 되고, $AUTH_C$는 임의의 난수과 인증 요청 차량의 ID를 세션 키로 해쉬하여 $AUTH_C$를 연산한다.

$$N_i = H[v_i \oplus t_i] \oplus K_s \qquad (1)$$
$$AUTH_C = H_{K_s}[RN \| VID_i]$$

CA는 계산한 $AUTH_C$ 값을 저장하고 난수 RN과 연산값 N_i을 인증 요청 차량의 서비스 지역 내 RSU를 통해 차량에게 전송하게 된다. 인증 요청 차량은 CA로부터 전송 받은 난수 RN과 연산값 N_i을 이용하여 식 (2)와 같이 세션 키를 알아내고 받은 난수값 RN과 자신의 ID를 세션 키로 해쉬하여 $AUTH_i$를 연산하여 CA에게 전송한다. CA는 이전에 계산한 $AUTH_C$와 전송받은 $AUTH_i$를 비교 검증하여 그 값이 일치할 경우 차량을 인증하게 된다.

$$N_i \oplus H[v_i \oplus t_i] = K_s \qquad (2)$$
$$AUTH_i = H_{K_s}[RN \| VID_i]$$

4. 안전성 및 성능 분석

제안한 VANET 환경에서의 차량 등록 프로토콜의 안전성 분석은 다음과 같다.

① 위장 공격

통신상에 공격자가 정상 차량으로 위장하여 인증하기

위해 임의의 ID와 타임스탬프 정보를 보내고 응답메시지인 N_i 값이 도청 당하더라도 인증 요청 차량과 인증 센터간의 공유된 키 검증자를 통해 인증 센터에서 생성한 세션 키의 분배가 이루어지므로 세션키의 노출을 방지한다. 세션 키 노출 방지를 통해 공격자는 올바른 AUTH 값을 생성하지 못하므로 공격자의 인증 시도는 실패하게 된다.

② 재전송 공격

재전송 공격을 막기 위해 타임스탬프와 난수를 사용하고 있다. 먼저 타임스탬프는 RSU에서 인증 요청시 CA로 전송되는 파라메터로 차량 인증 요청의 적시성을 판단한다. 그리고 세션키 분배에 사용되는 N_i 생성에 사용함으로서 차량 자신이 CA와 공유하고 있는 키 검증자와 인증 요청시 사용한 타임스탬프를 통해 분배된 세션키 확인할 수 있게 된다. 난수는 CA가 생성하여 $AUTH_C$를 생성하고 인증 요청 차량에게 난수를 전송하여 AUTHi 값 생성에 사용되므로 동일한 차량 아이디와 난수 값으로 생성되었는지 확인함으로서 재전송 공격을 막을 수 있다.

③ MITM 공격

CA에 의해 생성된 세션키 K_s 분배에 키 검증자 v_i를 사용하여 분배된 세션 키로 생성한 $AUTH_C$와 $AUTH_i$를 CA가 검증하여 차량을 단방향 인증하게 된다. 이때 키 검증자를 모르는 공격자는 AUTH 값을 생성하기 위한 세션키를 알 수 없으므로 MIMT 공격을 행할 수 없게 된다.

④ 메시지 변조 공격

CA에서 생성된 N_i를 차량으로 전송하는 과정에서 공격자에 의해 $N_i' = N_i \oplus H[v_k \oplus t_k]$로 변조되어 차량에게 전송되면 차량은 $N_i' \oplus H[v_i \oplus t_i] = H[v_k \oplus t_k] \oplus K_s = K_s'(N_k)$를 세션키로 오인하여 잘못된 AUTHi'를 생성하여 전송하므로 인증에 실패한다. 또한, 공격자가 AUTHi' 값에서 인증에 사용된 세션 키를 알 수 없으므로 메시지 변조 공격에 안전하다.

본 논문에서 제안하는 차량 등록 프로토콜은 차량의 연산처리 능력을 고려하여 XOR과 해쉬 연산만을 사용한다. 그림 2의 프로토콜에서 CA에서는 XOR 연산2번, hashing, keyed-hashing 연산이 각각 1번이 이루어지고 차량에서도 동일한 연산이 이루어진다. 이러한 연산 부하는 VANET 환경에서 차량 등록 인증 프로토콜을 구현시 CA와 차량에서 실시간 처리가 가능함을 알 수 있다.

5. 결 론

VANET 환경에서의 응용들이 안전하고 신뢰성 있게 제공되기 위해서는 데이터의 보호와 같은 보안성 확보가 필수적으로 해결되어야 한다. 특히, VANET 환경에서 정당한 사용자의 인증을 위해서는 차량 등록 인증이 이루어져야 한다.

본 논문에서는 VANET 환경에서 CA가 차량을 인증하는 효율적인 단방향 차량 등록 인증 프로토콜을 제안하였다. 차량과 인증 센터간의 공유된 키 검증자를 통해 인증 센터가 생성한 세션 키의 안전한 키 분배가 이루어지게 되고, 세션 키를 통해 생성한 인증 센터와 차량의 인증 결과 값을 CA에서 비교 검증하여 동일한 값일 경우 차량 등록 인증이 이루어지게 된다. 또한, 제안한 프로토콜은 차량의 연산처리 능력을 고려하여 XOR과 해쉬 연산만을 사용하였으며 향후 VANET 보안시스템 구축시 실시간 처리가 가능할 것이다. 본 프로토콜은 VANET 환경상에서 과금 등 다양한 응용서비스에 활용이 가능하다.

참 고 문 헌

[1] IEEE802.11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2007.

[2] Hannes Hartenstein and Kenneth P. Laberteaux "A Tutorial Survey on Vehicular Ad Hoc Networks," IEEE Communication Magazine, pp.164-171, June 2008.

[3] Maxim Raya, Panos P., and Jean-Pierre Hubaux "Secureing Vehicular Communi- cations," IEEE Wireless Comm. Vol.13, No. 5, pp.8-15, 2006.

[4] Maxim Raya and Jene-Pierre Hubaux "Security

Aspect of Inter-Vehicle Communication," Swiss Transport Research Conference, pp.1-14, March 2005.
[5] Yi Qian, and Nader Moder Moayrri, "DESIGN SECURE AND APPLICATION-ORIENTED VANETs", Proceedings of IEEE VTC 2008-spring, Singapore, May 2008.
[6] IEEE1609.2, *Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, IEEE standards, 2006.
[7] NIST, *Announcing the Advanced Encryption Standard(AES)*, FIPS PUB 197, 2001.
[8] IEEE Std 1363a, *IEEE Standard Specification for Public-Key Cryptography-Amenment1 : Additional Techniques*, 2004.

박 영 호 (YoungHo Park)

- 종신회원
- 1989년 2월 경북대학교 전자공학과(공학사)
- 1991년 2월 경북대학교 대학원 전자공학과(공학석사)
- 8월 경북대학교 대학원 전자공학과(공학박사)
- 2003년 8월 ~ 2004년 7월 Oregon State University 방문 교수
- 1996년 3월 ~ 2008년 2월 상주대학교 전자전기공학부 교수
- 2008년 3월 ~ 현재 경북대학교 산업전자전기공학부 교수
- 관심분야 : 네트워크 보안, 광통신 보안, 멀티미디어 보안 등

논 문 접 수 일 : 2010년 11월 02일
1차수정완료일 : 2010년 12월 03일
게 재 확 정 일 :: 2010년 12월 15일