VANET 상에서의 차량간 통신을 위한 인증 프로토콜†

(Authentication Protocol for Inter-Vehicle Communication in Vehicular Ad Hoc Networks)

박 영 호*, 나 진 한**, 문 상 재***
(Young Ho Park, Jin Han Na, Sang Jae Moon)

요 약 VANET 환경에서는 차량이 고속으로 이동하므로 차량간 긴급 데이터 전송이 일방향으로 이루어지는 것이 바람직하며 위험 정보를 후방의 차량들에게 전송 시 목적지가 정해지지 않은 브로드캐스트로 전송하는 것이 요구된다. 제안한 인증 프로토콜은 디지털 서명 방식을 사용하여 경로상의 노드를 인증하며 이는 위장 공격이나 메시지 위조 공격을 막을 수 있다. 또한, 제안한 프로토콜은 경로의 중간노드를 인식하기 위하여 노드 리스트를 사용하며 이 노드 리스트, 시간 및 난수는 재사용 공격을 막을 수 있다.

핵심주제어 : 차량 ad hoc 네트워크, 인증 프로토콜, 차량간 통신

Abstract In VANET, it is required one-way broadcast transmission because vehicles move at high speed and warning messages need to broadcast. Our protocol employs digital signatures to authenticate nodes along the path. This prevents impersonation attacks and message modification attacks. Our protocol also employs the node list to recognize intermediate nodes of the path. The node list, the time, and the nonce can prevent replay attacks.

Key Words : vehicular ad hoc network, authentication protocol, inter-vehicle communication

1. 서 론

최근 국내외적으로 ITS(intelligent transportation system)를 위한 연구가 활발히 이루어지고 있으며 ITS의 핵심기술로 부상하고 있는 VANET (vehicular ad hoc network)은 지능형 차량에 무선통신 기술을 지원하기 위하여 IEEE802.11 [1] 기반의 기술을 사용하고 있다. [2]

VANET 환경에서는 차량간 잘못된 정보의 전송이 교통 혼잡 뿐 아니라 치명적인 사고를 일으킬 수 있으며 과금에 관련된 사기의 위험이 발생할 수 있고 통신 정보를 추적하여 운전자의 프라이버시를 침해할 수 있다. 따라서 VANET 환경에서 응용들이 안전하고 신뢰성 있게 제공되기 위해서는 VANET 환경에서 발생할 수 있는 보안 위협 및 공격 유형을 정확하게 분석하여 이를 대처할 수 있는 방안들을 연구하는 것이 필요하다. VANET은 정보가 쉽게 노출될 수 있는 이동 차량 통신 환경이라 보안이 더욱 중요하며 정보보호 기술의 개발이 이러한 문제를 해결하는 최선의 방법이라 할 수 있다. [3,4]

† 이 논문은 2009년도 경북대학교 학술연구비에 의하여 연구되었음
* 경북대학교 이공대학 산업전자전기공학부 교수
** 경북대학교 전자전기컴퓨터학부 석사과정
*** 경북대학교 전자전기컴퓨터학부 교수

VANET 환경에서의 응용들이 안전하고 신뢰성 있게 제공되기 위해서는 가입자 인증과 전송 데이터의 인증 및 보호와 같은 보안성 확보가 필수적으로 해결되어야 한다. 특히, VANET 환경에서 도로상의 사고, 위험물, 노면결빙, 응급차량 등의 정보를 신속하게 다른 차량에게 전달해야 하며 이 경우 잘못된 정보의 전달로 치명적인 사고를 유발할 수 있으므로 차량간 전송 데이터의 인증이 필요하다.

VANET에서의 차량간 인증 프로토콜에 관련된 연구는 최근 국내외에서 이루어지고 있다. IEEE1609.2 [5] 에서는 안전한 차량 통신을 지원하기 위하여 WAVE(wireless access in vehicular environments)를 위한 PKI 기반의 보안기술 연구가 진행 중에 있다. 대칭키 방식을 사용한 인증은 속도 측면에서는 빠르고 효율적이나 VANET 상에서 동적으로 세션 키를 할당 및 관리하는 것이 어렵다. 최근 VANET 상에서 동적으로 세션 키를 그룹으로 분배하는 연구가 [6] 이루어지고 있으나 이러한 세션키를 안전하게 관리하는 것이 여전히 문제이다. 따라서 VANET 상에서의 차량간 인증을 위하여 공개키 기반의 디지털 서명을 사용하는 것을 권고하고 있다. [2]

본 논문에서는 VANET에서의 차량간 일방향 브로드캐스트 인증 프로토콜을 제안한다. 제안한 인증 프로토콜은 디지털 서명 방식을 사용하여 전송 데이터의 인증을 수행하도록 하며 신뢰된 인증서버에서 배부한 인증서를 사용하여 통신 노드들이 송신 노드의 공개키를 알기 위하여 인증서버에 접속해야 하는 시간을 줄이도록 하였다. 또한, 중간 노드들의 경로를 알 수 있도록 노드 리스트를 항목을 사용하며 중간 노드의 부하를 줄이기 위하여 이전 노드의 서명값이 맞으면 이전 노드의 서명값을 제거하고 현재 노드의 서명값을 첨가해서 패킷을 브로드캐스트 하도록 제안한다.

2. 보안 위협

VANET 환경에서 보안서비스를 제공하기 위해서는 VANET 환경에서 발생하는 보안 위협과 공격 유형을 분석하는 것이 필요하다. 본 장에서는 이러한 VANET 환경에서의 일반적인 보안 위협과 공격 유형을 분석 기술한다. VANET 환경에서 발생하는 보안 위협은 크게 안전한 메시지에 관련된 공격, 과금에 기초한 공격 및 프라이버시 공격으로 세가지로 분류할 수 있다. 안전한 메시지에 관련된 공격은 VANET 구축 후 차량 간 안전한 메시지 교환에 관련된 위협으로 중요한 문제이다. 이러한 공격 결과는 교통혼잡 뿐 아니라 치명적 사고로 생명에 영향을 줄 수도 있다. 과금에 기초한 공격은 VANET에서 toll 징수, 위치기반 서비스 과금, 보험 등의 금전적 처리가 필요하며 이는 금전적 사기의 위험이 있을 수 있다. 프라이버시 공격은 VANET의 중요한 문제 중 하나로 개인의 프라이버시에 관련된 문제이다. VANET에서는 서로간의 통신을 통하여 운전자를 추적할 수 있으며 이는 운전자의 프라이버시를 침해할 수 있다.

VANET 환경에서 구체적인 공격 유형은 위조 정보 공격, 네트워크 동작 중단, ID나 속도 혹은 위치 정보를 속이는 방법, ID 노출 공격 등이 있을 수 있으며 그 의미는 다음과 같다. [3]

2.1 위조 정보 공격

이 공격은 공격자가 다른 운전자의 결정에 영향을 주기위하여 차량 네트워크에 그릇된 정보를 유포하는 경우이다. 예를 들어 여러 운전자가 결탁하여 그들의 목적지에 빨리 도착하도록 도울 수 있다. 앞선 운전자가 길이 혼잡하다는 정보를 뒤의 차들에게 보내면 뒤 따르던 차들은 그들의 경로를 변경할 것이고 결탁된 뒤의 운전자는 목적지에 빨리 도착할 수 있을 것이다. 반대로 잘못된 정보로 특정한 길을 혼잡하게 만들 수도 있다. 이 공격은 안전한 메시지에 관련된 공격 위협의 한 유형이다.

2.2 네트워크 동작 중단

이 공격은 안전에 관련된 기능을 수행하는 네트워크를 막는 것이다. 잘못된 결과를 가질 메시지를 보내거나 무선채널 방해신호(DoS 공격)를 보냄으로 차량이 안전 메시지를 교환하지 못하게 한다. 예를 들어 악의의 공격자가 야간운전 시 두 차량에 서로 다른 메시지를 보낸다. 한 차량은 앞에 혼

잡이 있다는 경고 메시지를 받으면 속도를 줄이고 뒤따르는 다른 차량은 도로사정이 좋다는 메시지를 받아 속도를 높이면 극단적인 경우 두 차가 충돌할 수 있다. 다른 예는 무선채널상의 재밍과 같이 DoS 공격을 하여 안전에 관련되거나 과금에 관련된 정보를 주고받지 못하게 할 수 있다.

2.3 ID나 속도 혹은 위치 정보를 속이는 방법

이 공격은 신뢰에 기반 한 것으로 운전자는 어떤 시간에 차의 위치에 관련된 정보를 속이고 싶어질 수도 있다. 예를 들어 한 차량이 사고가 났을 때 차가 사고가 난 그 위치에 있지 않았다고 주장하고자 위치와 속도 정보를 변조할 수 있다. 또한, 다른 사람의 ID를 사칭하여 과금에 관련된 공격을 할 수도 있다.

2.4 ID 노출 공격

이 공격은 Big Brother 시나리오로 볼 수 있다. 글로벌 감시자는 목적된 차량의 경로와 어떤 목적의 데이터를 사용하는지 감시할 수 있다. 이를 위하여 글로벌 감시자는 목적지 부근의 차량이나 노변 구조물을 이용할 수 있다. 예를 들어, 목적지 주변에 바이러스를 퍼뜨리고 요구된 데이터를 수집할 수 있다.

3. 제안한 인증 프로토콜

VANET 환경에서 도로상의 사고, 위험물, 노면결빙, 응급차량 등의 정보를 신속하게 다른 차량에게 전달해야 하며 이 경우 잘못된 정보의 전달로 치명적인 사고를 유발할 수 있으므로 차량간 전송 데이터의 인증이 필요하다. VANET 환경에서는 차량이 고속으로 이동하므로 차량간 데이터 전송이 일방향으로 이루어지는 것이 바람직하며 위험정보를 후방의 차량들에게 전송시 목적지가 정해지지 않은 브로드캐스트로 전송하는 것이 필요하다. 따라서, 본 논문에서는 이러한 조건을 만족하는 차량간 일방향 브로드캐스트 인증 프로토콜을 제안한다.

본 인증 프로토콜은 신뢰된 인증서버(CA)를 사용하며 CA의 공개키는 모든 노드에 알려진다. 각 노드는 VANET에 들어가기 전 인증서버로부터 인증서를 요구해야 하고 인증서버는 노드의 실체를 인증한 후 인증서를 배부한다. 한 노드 S는 다음과 같이 인증서버로부터 인증서를 수신한다.

$$CA \rightarrow S : Cert_s = [S, K_{S+}, t, e]K_{CA-}$$

여기서 S는 시작노드의 주소, K_{S+}는 S의 공개키, t는 인증이 이루어진 timestamp이고 e는 인증서가 만료되는 시간이다. 이러한 인증서를 사용하면 통신 노드들이 송신 노드의 공개키를 알기 위하여 인증서버에 접속해야하는 시간을 줄일 수 있으며 VANET과 같이 고속으로 인증이 이루어져야 하는 경우에는 유용하게 활용될 수 있다.

$$S \rightarrow broadcast$$
$$[(S,*,N,t,cert_S,M)_{K_{S-}}]$$
$$A \rightarrow broadcast$$
$$[(\ (S,*,N,t,cert_S,M)_{K_{S-}}(A),cert_A)_{K_A}\ ]$$
$$B \rightarrow broadcast$$
$$[(\ (S,*,N,t,cert_S,M)_{K_S}(A,B),cert_B)_{K_{B-}}]$$
$$C \rightarrow broadcast$$
$$[(\ (S,*,N,t,cert_S,M)_{K_{S-}}(A,B,C),cert_C)_{K_{C-}}]$$

<그림 1> 차량간 인증 프로토콜.

그림 1은 VANET에서의 차량간 인증 프로토콜을 나타낸 것이다. 차량간 인증을 하기 위하여 시작노드 S는 난수 N, timestamp t, 시작노드의 인증서 $cert_S$ 그리고 메시지 M을 포함하는 서명된 패킷을 방송한다. *는 방송용임을 나타내며 목적지가 있을 경우 *값 대신 목적지 주소를 사용하면 되고 N과 t는 네트워크에서 패킷이 새로운 것임을 나타낸다. 노드 B는 A의 인증서 값 $cert_A$를 확인하여 서명값을 검사한다. B는 시작노드 S의 인증서 $cert_S$를 확인하고 수신된 경로요구 패킷의 서명값을 확인하기 위하여 인증서 내의 키를 사용한다. 만약, 서명값이 맞으면 이전 A의 서명값을 제거하고 노드 리스트에 자신의 주소 B를 첨부하고 B의 서명값을 첨가해서 패킷을 방송한다. 노드 리스트는 패킷의 경로를 알 수 있으며 필요시 중간 노드의 경로 수를 제한하여 패킷의 존속경로를 정

할 수 있다.

4. 안전성 분석

본 장에서는 제안한 VANET에서의 차량간 인증 프로토콜을 네트워크 측면에서 발생할 수 있는 위장 공격 및 메시지 위조 공격, DoS 공격과 재전송 공격의 측면에서 안전성을 분석한다.

4.1 위장 공격 및 메시지 위조 공격

제안한 프로토콜에서 공격자는 위장하거나 메시지를 위조할 수 없다. 만약, 공격자가 메시지를 위조하여 다른 차량에 보낼 경우 서명이 검증되지 않으므로 공격이 되지 않으며 최초 메시지를 보낸 차량의 비밀 키를 알 수 없으므로 최초의 발신자로 위장할 수도 없다. 만약, 중간 노드로 위장하더라도 최초 발생된 메시지에 접근할 권한이 없으므로 공격에 대처할 수 있다.

4.2 재전송 공격

재전송 공격은 가장 가능성이 높은 공격 중 하나이며 제안한 프로토콜에서는 재전송 공격을 방지하기 위하여 시간과 nonce를 사용하였다. 본 프로토콜에서는 랜덤 값 N을 충분히 큰 수를 사용하며 전송 패킷에 포함된 시간과 각 노드에서 약속된 패킷의 폐기시간을 이용한다. 예를 들어 공격자가 이전에 수신한 패킷을 다른 차량에게 전송한다면 패킷 내에 있는 시간과 인가된 폐기시간을 확인하여 인증이 실패되었음을 알 수 있다.

4.3 DoS 공격

DoS 공격에는 네트워크 트래픽을 이용하거나 차량에 과다한 연산을 수행하도록 하여 성능을 떨어뜨리는 경우가 있다. 네트워크 트래픽을 이용한 DoS 공격은 무차별적으로 대량의 메시지를 보내기 때문에 근본적으로 차단하는 것이 어렵다. 그러나 인증을 수행하는 연산량을 줄임으로써 DoS 공격에 대응할 수 있다. 본 프로토콜에서는 패킷 인증을 위하여 공개키 기반 디지털 서명을 사용하나 중간노드에서 최대한 연산량을 줄이도록 중간노드에서 서명이 검증된 노드는 노드리스트에 그 노드를 첨부하고 검증된 노드의 서명값을 제거하도록 하였다. 또한, 수신 패킷이 발신자나 노드 리스트에 있는 동일 차량노드로부터 전송되는 경우 이를 제거함으로써 DoS 공격에 대응할 수 있다.

5. 결 론

VANET 환경에서 도로상의 사고, 위험물, 노면결빙, 응급차량 등의 정보를 신속하게 다른 차량에게 전달해야 하며 이 경우 잘못된 정보의 전달로 치명적인 사고를 유발할 수 있으므로 차량간 전송 데이터의 인증이 필요하다. VANET 환경에서는 차량이 고속으로 이동하므로 차량간 긴급 데이터 전송이 일방향으로 이루어지는 것이 바람직하며 위험 정보를 후방의 차량들에게 전송 시 목적지가 정해지지 않은 브로드캐스트로 전송하는 것이 필요하다. 본 논문에서는 이러한 조건을 만족하는 차량간 일방향 브로드캐스트 인증 프로토콜을 제안하였다. 제안한 인증 프로토콜은 인증서 기반 디지털 서명 방식을 사용하였으며 중간 노드에서 최대한 연산량을 줄이도록 중간노드에서 서명이 검증된 노드는 노드리스트에 그 노드값을 첨부하고 검증된 노드의 서명값을 제거하도록 하였다. 또한, 제안한 인증 프로토콜은 위장 공격 및 메시지 위조 공격, 재전송 공격과 DoS 공격의 측면에서 안전성을 분석하였다.

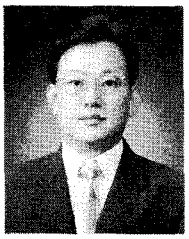
참 고 문 헌

[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.

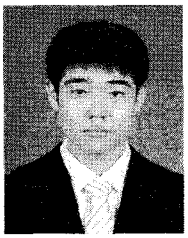
[3] Maxim Raya, Panos P., and Jean-Pierre

Hubaux "Secureing Vehicular Communications," 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] IEEE1609.2, Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE standards, 2006.
[6] Maxim Raya and Jene-Pierre Hubaux "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, Vol.15, pp.39-68, 2007.



박 영 호 (Young Ho Park)

- 종신회원
- 1989년 2월 경북대학교 전자공학과(공학사)
- 1991년 2월 경북대학교 대학원 전자공학과(공학석사)
- 1995년 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 이공대학 산업전자전기공학부 교수
- 관심분야 : 네트워크 보안, 광통신 보안 등



나 진 한 (Jin Han Na)

- 학생회원
- 2008년 2월 상주대학교 전자전기공학부(공학사)
- 2008년 3월 ~ 현재 경북대학교 전자전기컴퓨터학부 석사과정

문 상 재 (Sang Jae Moon)

- 1972년 2월 서울대학교 공과대학(공학사-전자공학)
- 1974년 2월 서울대학교 대학원 (공학석사-전자공학)
- 1984년 6월 미국 U.C.L.A. (공학박사-통신공학)
- 1984년 7월 ~ 1985월 6월 미국 OMNET 회사 컨설턴트
- 1984년 7월 ~ 1985년 6월 미국 U.C.L.A 포스트닥터
- 2001년 2월 ~ 2002년 2월 한국정보보호학회 회장
- 1974년 12월 ~ 현재 경북대학교 전자전기컴퓨터학부 교수
- 관심분야 : 네트워크 보안, 암호학 등

논문접수일 : 2009년 9월 28일
논문수정일 : 2009년 6월 10일
게재확정일 : 2009년 6월 22일