V2I 기반의 VANET 환경에서 안전한 차량 통신을 위한 세션 키 교환 기법

(A Session Key Exchange Scheme for Secure Vehicle Communication in V2I-based VANET Environments)

유 승 호 † 정 수 환 ††
(Seungho Ryu) (Souhwan Jung)

요 약 본 논문에서는 VANET 환경에서 차량과 인프라 간의 신뢰성 있는 통신을 제공하기 위한 V2I 간의 세션 키 교환 기법을 제안한다. 기존의 VANET에서는 V2I간의 안전한 통신을 위해 IEEE 802.11i와 PKI 기반의 보안 메커니즘을 사용하고 있다. 그러나 차량의 고속 이동과 네트워크 환경이 자주 변하는 특성을 가진 VANET에서 짧은 시간에 IEEE 802.11i 또는 PKI 방식을 이용한 V2I 세션 키 교환은 어려움이 있다. 제안하는 기법에서는 빠르게 움직이는 차량과 인프라 간의 세션키 교환을 위해 LR (Local Router)을 새롭게 정의하였으며, LR과 OBU 사이의 랜덤 값에 기반 한 XOR 연산을 통해 새로운 세션키를 빠르게 생성하고 교환할 수 있게 하였다. 때문에 제안하는 기법은 VANET 환경에서 AAA 서버 도움 없이도 빠르게 세션키를 교환할 수 있는 이점이 있다.

키워드 : 텔레매틱스, 차량이동 통신, 지능형 교통 시스템

Abstract This paper proposes a session key exchange scheme for providing secure communication between Vehicles and Infrastructure in VANET. In the current VANET environment, IEEE 802.11i or PKI based mechanism is used to provide secure communication between V2I. However, since the vehicles and the frequent changes of network topology, VANET nodes have some difficulties to exchange the session key using IEEE 802.11i or PKI method. In the proposed scheme, Local Router is newly defined for exchanging the session key between moving vehicles and infrastructure. A session key is generated by XOR operation based on the random values between Local Router and OBU. As a result, the proposed scheme has a noticeable advantage on the fastness of key exchange by exchanging session keys between LR and OBU.

Key words : Telematics, V2I Communication, ITS

1. 서 론

최근 국내외적으로 ITS (Intelligent Transportation System : 지능형 교통 시스템)와 IT 기술을 지능형 차량 통신에 적용시키기 위한 연구가 활발하게 이루어지고 있다[1,2]. ITS의 핵심 기술로 부상하고 있는 VANET(Vehicular Ad-hoc Network)은 지능형 차량 사이의 무선 통신을 지원하기 위한 IEEE 802.11 기반의 무선 네트워크 기술로 MANET(Mobile Ad-hoc Network)[3], NEMO(Network Mobility)[4], MANEMO (MANET and NEMO), Mobile IPv6(MIPv6, FMIPv6, HMIPv6)[5-7] 등과 같은 다양한 IT 기술들이 융합된 기술이다. VANET은 지능형 차량을 이용한 V2V(Vehicle-to-Vehicle), V2I(Vehicle-to-Infrastructure) 간의 무선 통신을 지원함으로써 사회적으로 문제가 되고 있는 심

· 이 논문은 2007년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원과(No.R01-2007-000-11504-0), 숭실대학교 교내 연구비 지원에 의해 수행되었음

† 학생회원 : 숭실대학교 정보통신전자공학부
ihappysig@naver.com
†† 종신회원 : 숭실대학교 정보통신전자공학부 교수
souhwanj@ssu.ac.kr
(Corresponding author임)

논문접수 : 2007년 12월 21일
심사완료 : 2008년 5월 22일

정보과학회논문지 : 정보통신 제35권 제4호(2008.8)

각한 교통 문제 해결, 인터넷 접속을 통한 다양한 서비스 제공 등을 기본 목표로 하고 있다. 이미 미국과 유럽을 포함한 선진국에서는 지능형 차량을 이용한 ITS 기술 연구가 활발하게 진행되고 있으며 고속도로 통행 요금의 전자 결제, 위성정보를 이용한 네비게이션 서비스 등은 이미 상용화 되고 있다.

VANET에서는 기존의 무선 환경에서 존재하는 보안 위협과 차량의 고속 이동 및 네트워크 환경의 급격한 변화 때문에 발생하는 다양한 보안 위협이 존재한다[8]. 뿐만 아니라 차량의 이동 정보가 쉽게 노출 될 수 있는 문제점이 있어 개인의 프라이버시가 침해될 수 있다. 따라서 위와 같은 문제를 해결하기 위한 보안 기술 연구가 필요하다. V2I 간의 무선 환경에 존재하는 보안 문제를 해결하기 위해미국과 유럽을 비롯한 선진국에서는 IEEE 802.11i 무선랜 보안 표준과 기존의 PKI(Public Key Infrastructure) 방식을 차량 통신에 적용한 차량용 PKI 보안 기법을 연구하고 있다[9,10].

그러나 IEEE 802.11i와 PKI 방식은 차량의 빠른 이동성을 고려하지 못한다. 우선 IEEE 802.11i에서는 V2I 간의 세션 키 교환을 위하여 IEEE 802.1X의 사용자 상호 인증과 4-단계 핸드쉐이크를 통한 일대일 세션 키 교환 과정을 수행하여야 한다. 그러나 VANET에서는 차량이 빠르게 이동하기 때문에 짧은 시간 안에 사용자 인증과 4-단계 핸드쉐이크 과정을 수행하기에는 시간적 어려움이 있다. 또한 PKI의 경우 보안 서비스 제공을 위해 국가 차원의 교통통신망 인프라 구축, 개인 인증서 갱신 및 관리가 필요하며, 응급 상황 시 전달되는 메시지를 빠르게 처리하기 위한 고성능의 장비가 필요하다. 그렇지 못한 경우 메시지 처리로 인한 전송 지연 등의 문제가 발생 가능하다[11,12]. 본 논문에서는 앞에서 언급한 VANET 환경에서의 IEEE 802.11i와 PKI 기반의 보안 기술의 문제점을 개선하기 위한 새로운 V2I 세션 키 교환 기법을 제안한다. 제안 기법에서는 LR(Local Router)을 새롭게 정의하고 OBU(On Board Unit)와 LR 간에 세션 키를 교환하도록 한다. V2I 간의 세션 키 교환을 위하여 두 번의 메시지 전송과 한 번의 XOR 연산만을 수행함으로써 OBU와 LR 간 신속하고 효율적인 세션 키 교환이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서는 VANET 환경에서의 보안 위협 분석 및 관련 연구에 대해 살펴본다. 3장에서는 본 논문에서 제안하는 V2I 구조 및 V2I 세션 키 전달 기법을 설명한다. 4장에서는 제안 기법의 성능 및 안전성을 분석한다. 마지막으로 5장에서 결론을 맺는다.

2. VANET의 보안 위협 분석 및 관련 연구

VANET에서의 차량 통신에 사용되는 응급 메시지 전송, 위치 정보 서비스 등은 차량의 ID 및 위치 정보가 포함되어져 있다. 차량 통신에 사용되는 이러한 정보들은 쉽게 네트워크에 노출될 수 있으며, 노출된 차량 정보를 이용한 개인 프라이버시 침해가 발생할 수 있다. 따라서 개인의 재산과 정보 보호를 위해 V2I 간의 안전한 통신은 필수사항이며, VANET의 무선 네트워크 환경을 고려한 보안 솔루션이 필요하다. 다음은 VANET 환경에서 발생 가능한 보안 취약성 및 이를 해결하기 위한 기존의 연구 기술에 대한 설명이다.

2.1 VANET의 보안 취약성

• 전파방해 공격(Jamming Attack)

DoS 공격의 일종으로, 일정 네트워크 영역 내에서 다른 차량의 통신에 장애를 초래하는 신호를 발생시켜 네트워크 통신을 마비시키는 공격이다.

• 위조 공격(Forgery Attack)

거짓 정보를 발생하는 공격 차량에 의해 일정네트워크 영역 내에서 다른 차량들을 거짓 정보로 오염시키는 공격이다.

• 트래픽 위변조 공격(In-transit Traffic Tampering)

고속 주행 중 메시지를 전달하는 과정에서 공격 차량에 의한 메시지 삭제 및 변조를 통해 차량 통신을 방해하는 공격이다.

• 위장 공격(Impersonation Attack)

이웃 차량의 정보를 자신의 상태정보로 변경하여 다른 차량으로 하여금 잘못된 차량 인식을 하도록 하는 공격이다.

• 개인 정보 침해(*Privacy Violation*)

시간, 위치, 차량 ID, 이동 정보 등 차량과 관련된 개인 정보가 노출되어 프라이버시 침해가 발생 가능하다.

• On-board 위변조 공격(On-board Tampering)

속도, 위치, 차량 전장 부분의 상태, 각종 센싱 정보 등과 같은 차량 내부의 정보에 대해 위변조 공격을 함으로써 속도나 위치 등의 센서 정보를 악의적으로 수정하여 부정확한 정보를 제공 하는 것을 말한다.

이러한 공격들은 실제 도로상황에서 차량들 간의 정확한 정보교환을 방해하여 교통사고를 유발 시킬 수 있으며, 잘못된 차량 운행을 유도할 수 있다. 따라서 차량 통신과 관련된 메시지는 상호 인증 및 보안 기술을 통해서 반드시 보호되어야 한다.

2.2 VANET 보안 기술

VANET의 V2I 무선 구간에서 존재하는 다양한 보안 위협들로부터 안전한 차량 통신을 지원하기 위해 WAVE (Wireless Access in Vehicular Environments)에서는 PKI 기반의 보안 기술 연구가 IEEE P1609.2를 통해 진행 중에 있다. CALM(Continuous Air Interface for

Long and Medium Range)에서는 IEEE 802.11i 기반의 보안 기술을 VANET 환경에 적용시키기 위한 연구가 진행 중에 있다. 그러나 IEEE P1609.2의 PKI와 IEEE 802.11i 보안 기법은 차량과 RSU(Road Side Units) 간 세션 키 교환과정에서 큰 오버헤드가 발생하기 때문에 차량의 빠른 이동성을 가진 VANET 환경에 적용하기 부적절하다.

본 절에서는 앞서 설명한 WAVE와 CALM에서 연구되고 있는 PKI와 IEEE 802.11i의 무선 구간 보안 기법과 VANET에서 차량의 빠른 이동성을 지원할 수 있는 WLAN 환경의 Proactive 방식, 이동성 예측 방식, Proactive 방식과 이동성 예측 혼합 방식의 핸드오버 세션 키 전달 기법에 대하여 알아본다.

2.2.1 WAVE 및 CALM 보안 기술

IEEE P1609.2에서는 차량 통신 메시지에 대한 인증 및 프라이버시 제공을 위해 기존의 PKI 방식을 VANET에 적용한 보안 기법을 연구하고 있다[10]. 그러나 VANET에서는 사전에 인증서를 발급받을 수 있는 인프라 환경의 구축과 인증서 갱신에 관한 해결책이 명확하게 정해지지 않은 문제점이 있다. 또한 전달 받은 세션 키에 대한 전자서명 및 검증을 위해서는 많은 계산량과 시간이 필요하기 때문에 차량의 빠른 이동성을 가지는 VANET 환경에 적용하는데 문제점이 있다.

CALM에서는 V2I의 무선구간 메시지 보호를 위해 IEEE 802.11i의 보안 표준을 따르고 있다[9]. 그러나 PKI 기반의 보안 기법과 마찬가지로 차량의 빠른 이동성을 가지는 VANET 환경에서 V2I 간의 신속하고 연속적인 세션 키 교환은 어려움이 있다.

2.2.2 빠른 이동성 지원을 위한 V2I 간 세션 키 전달 기법

WLAN 환경에서의 Proactive 방식은 AAA(Authentication, Authorization, and Accounting) 서버가 이동 노드의 핸드오버 마스터키를 주변 N개의 AP(Access Point)들에게 미리 분배하는 기법으로, 이동 노드가 실제 핸드오버 하는 시점에서 핸드오버 마스터 키 교환 과정을 수행하지 않아도 되기 때문에 인증 지연 시간을 단축시킬 수 있다[14]. 그러나 차량의 고속 이동과 빈번하게 네트워크 환경이 변하는 VANET에서는 PMK (Pairwise Master Key) 생성을 위한 AAA 서버와 차량 간의 지속적인 보안 통신이 어렵다. 또한 AAA 서버를 통한 PMK 생성이 이루어짐으로써 메시지 전송지연이 발생할 경우, V2I 간의 신속한 세션 키 전달이 어렵게 된다.

WLAN 환경에서의 이동성 예측 기반의 인증 방식은 FHR(Frequent Handoff Region) 선택 알고리즘을 사용하여 초기 부팅 인증 과정보다 인증 시간을 50% 단축시킬 수 있다[15]. FHR 선택 알고리즘은 이동 노드의 이동 패턴을 분석하는 알고리즘으로 Proactive 키 분배 방식과 달리 새로운 개념의 AP들을 정의하였다. 그러나 VANET은 차량이 도로 위를 이동하는 특성 때문에 FHR와 같은 복잡한 계산과정이 불필요하다. 또한 AAA 서버는 이동 노드가 이동 하게 될 각각의 AP들에게 PMK를 생성하여 전송하게 됨으로 AAA 서버의 오버헤드와 메시지 전송 지연이 발생할 수 있다.

Proactive와 이동성 예측 기반의 혼합 방식은 WLAN 환경에서 AAA 네트워크의 트래픽 오버헤드를 줄이기 위해 Proactive 키 분배 방식과 이동 노드의 이동성 예측성을 조합한 기법이다[16]. Proactive와 이동성 예측 혼합 방식은 기존 기법들보다 AAA 네트워크의 인증 트래픽 양을 줄이고 인증 지연 시간을 단축시켰으나 VNAET 환경의 특성상 차량의 이동 방향이 정해져 있어 이동성 예측 알고리즘이 필요하지 않다. 또한 AAA 서버가 각 AP들의 토폴로지 상태를 유지해야 하는 오버헤드와 OBU와 AAA 서버 간의 메시지 전송 지연 발생 시 신속한 세션 키 교환이 어려운 문제점이 있다.

3. 제안 구조 및 V2I 세션 키 전달 기법

3.1 V2I 세션 키 교환을 위한 구조

VANET 환경에서 지능형 차량이 지속적이고 안전한 네트워크 서비스를 보장 받기 위해서는 지능형 차량이 이동하게 되는 모든 RSU 간에 연속적인 세션 키 교환이 이루어져야 한다.

본 논문에서는 OBU와 RSU 간의 세션 키 교환횟수를 줄이기 위하여 그림 1과 같이 다수의 RSU를 관리하는 LR을 포함한 계층적 구조를 제안한다. LR은 자신의 영역에 속한 RSU에게 OBU와의 안전한 통신을 위한 세션 키를 계층적으로 전달한다. OBU는 동일한 LR의 영역에 속한 RSU를 이동할 경우 사전에 생성된 OBU와 RSU 간의 세션 키를 사용하여 안전한 통신을 할 수 있다. 이렇게 함으로써 기존의 방식에 비해 세션 키 교환 횟수 및 세션 키 교환을 위한 오버헤드를 줄일 수 있다.

제안 기법에서 OBU는 RSU와 EAP-TLS를 통해 세션 키를 공유하고 RSU는 세션 키를 안전한 채널을 통해 LR에게 전달함으로써 OBU와 LR 간에는 세션 키를 공유할 수 있다. 또한 그림 2에서와 같이 RSU와 LR 간, LR과 LR 간에는 TLS 또는 IPSec과 같은 보안 프로토콜을 사용하여 안전한 채널이 형성될 수 있다.

3.2 OBU와 LR 간의 세션 키 전달 기법

OBU의 처음 부팅과정에서 그림 2와 같이 OBU와 LR_A 간의 세션 키 교환을 위해 IEEE 802.1x를 사용하여 상호 인증 및 4-단계 핸드쉐이크 과정을 수행한다.

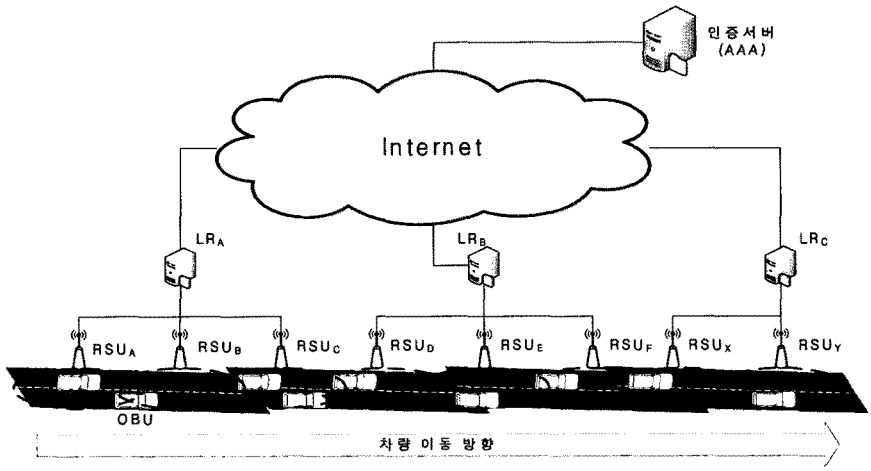

그림 1 세션 키 교환을 위한 구조

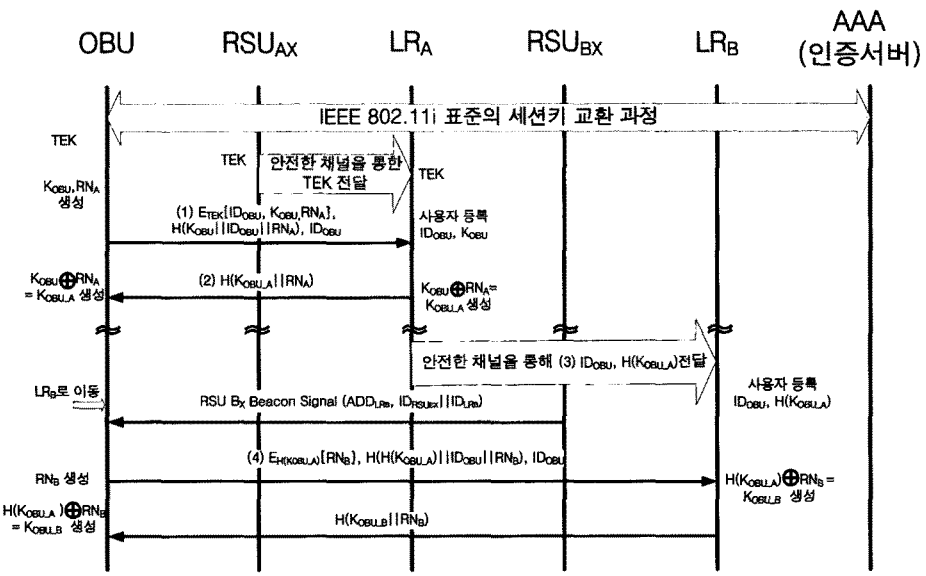

그림 2 OBU와 LR 간의 세션 키 전달 기법

이 과정을 통해 OBU와 RSU_{AX} 사이에 세션 키를 공유한다. 이 후에 RSU_{AX}는 자신이 속한 LR_A에게 OBU와 공유하고 있는 세션 키를 안전한 채널을 통하여 LR_A에게 전달함으로써, OBU와 LR_A는 세션 키를 공유할 수 있다. 또한 LR_A는 그림 2의 메시지 (3)을 통하여 LR_B에게 ID_{OBU}, K_{OBU_A}의 해쉬값을 LR_A와 LR_B간의 안전한 채널을 통해 전달함으로써 LR_B는 자신의 영역으로 이동할 OBU를 사전에 알 수 있다.

OBU는 LR_A과 TEK(Temporary Encryption Key)를 공유한 후 LR_A에 처음 사용자 등록 및 세션 키(K_{OBU_A}) 교환을 수행한다. 우선, OBU는 RSU_{AX}를 통해 자신이 속한 LR_A에 등록 및 세션 키 생성을 위해 ID_{OBU}, K_{OBU}, RN_A를 TEK로 암호화한 값, ID_{OBU}, K_{OBU}, RN_A를 해쉬한 값, 그리고 ID_{OBU}를 그림 2의 메시지 (1)처럼 LR_A에게 전송한다. LR_A는 그림 2의 메시지 (1)을 수신한 후 ID_{OBU}, K_{OBU}를 등록하고 OBU와 LR_A간의 세션 키 생성을 위해 K_{OBU}와 RN_A를 XOR 연산하여 새로운 세션 키(K_{OBU_A})를 생성한다. LR_A는 새롭게 생성된 세션 키(K_{OBU_A})와 RN_A 해쉬 값을 그림 2의 메시지 (2)를 통해 OBU에게 전송함으로써 OBU와 LR_A 사이에는 사용자 등록과 일대일 세션 키(K_{OBU_A}) 생성이 완료된다.

OBU의 이동으로 LR_A에서 LR_B의 영역으로 이동할 경우 OBU는 다음과 같은 과정을 통하여 LR_B와 새로운 세션 키를 교환하게 된다. OBU는 주기적으로 전송되는 RSU의 비콘 신호에 포함된 ID_{LR}을 통하여 새로운 LR_B의 영역으로 이동한 것을 알게 된다. LR_B의 영역으로 이동 한 것을 인지한 OBU는 LR_B와의 새로운 세션 키 생성을 위해 K_{OBU_A}, ID_{OBU}, RN_B를 해쉬한 값, RN_B를 암호화한 값 그리고 ID_{OBU}를 포함한 그림 2의 메시지 (4)를 LR_B에게 전송한다. LR_B는 사전에 LR_A에게 받은 그림 2의 메시지 (3)의 K_{OBU_A}의 해쉬 값과 메시지 (4)의 RN_B 두 값의 XOR 연산을 통하여 새로운 세션 키 (K_{OBU_B})를 생성한다. OBU는 새롭게 이동한 LR_B의 영역에서 새롭게 생성된 세션 키(K_{OBU_B})를 사용하여 안전한 통신을 할 수 있어 기존의 IEEE 802.11i 및 PKI 방식에 비하여 신속한 V2I 간의 세션 키 교환이 가능하다. 뿐만 아니라 제안 기법은 세션 키 생성 주체가 LR이므로 Proactive, 이동성 예측 방식과 달리 AAA 서버와 추가적인 통신 없이 세션 키를 생성할 수 있다.

3.3 동일한 LR에서의 OBU와 RSU 간의 세션 키 전달 기법

OBU와 동일한 LR의 영역에 포함된 RSU 간의 세션 키 교환을 위해서는 그림 3과 같은 과정을 수행한다. LR은 자신의 영역에 포함된 RSU_{ID} 정보를 OBU와 LR_A 간 세션 키(K_{OBU_A})로 암호화 하여 OBU에게 전달하게 된다. OBU는 전달 받은 RSU_{ID} 정보와 세션 키 (K_{OBU_A})를 식 (1)을 이용하여 OBU와 RSU 간의 새로운 세션 키를 생성한다.

$$H(K_{OBU\_A}||RSU_{ID}) \quad (1)$$

LR 또한 식 (1)을 사용하여 OBU와 동일한 방식으로 OBU와 RSU 간의 세션 키를 생성하고 자신의 영역에 속해 있는 RSU에게 안전한 채널을 이용하여 OBU_{ID} 정보와 세션 키($H(K_{OBU\_A}||RSU_{ID})$)를 전달하게 된다. OBU_{ID} 정보와 세션 키를 전달 받은 RSU는 추후에 이동 해 오는 OBU_{ID} 정보를 이용하여 OBU를 구분하며, 안전한 통신을 위해서 사전에 LR로부터 전달받은 OBU와 RSU 간의 세션 키를 이용하여 신속하고 안전한 통신을 할 수 있다.

OBU는 RSU의 비콘 신호에 포함된 RSU_{ID} 정보를 이용하여 자신이 이동한 RSU를 인지하게 되며 이동한 새로운 RSU 영역에서 사전에 생성된 새로운 세션 키 ($H(K_{OBU\_B}||RSU_{ID})$)를 이용하여 OBU와 RSU 간의 안전한 통신을 수행한다.

4. 안전성 및 성능 분석

4.1 기존 방식과 제안기법 비교

위의 표 1은 OBU와 LR 간의 세션 키 생성과 관련된 기존 보안 기법인 IEEE 802.11i[9], PKI[10] 방식, WLAN 환경에서의 핸드오버 지원 기법[14,15]들과 본 논문에서 제안하는 방식을 비교하여 나타낸 것이다.

제안 기법은 초기에 OBU와 LR 간의 세션 키 교환을 위하여 IEEE 802.11i와 동일한 수행 절차에 따라 OBU와 RSU 간에 세션 키 생성한 후 RSU는 세션 키를

표 1 V2I 간 세션 키 교환 기법 비교 분석

		IEEE 802.11i [9]	PKI [10]	Proactive 방식 [14]	FHR 방식 [15]	제안 기법
세션 키 생성 경우		OBU의 RSU 이동 시	OBU의 RSU 이동 시	OBU의 RSU 이동 시	OBU의 RSU 이동 시	OBU의 LR 이동 시
빠른 핸드오버 지원		빠른 핸드오버 지원 불가능	빠른 핸드오버 지원 불가능	빠른 핸드오버 지원 가능	빠른 핸드오버 지원 가능	빠른 핸드오버 지원 가능
세션 키 생성 주체		AAA 서버	OBU, CA 서버	AAA 서버	AAA 서버	OBU, LR
세션 키 교환 대상		OBU와 RSU 사이	OBU와 RSU 사이	OBU와 RSU 사이	OBU와 RSU 사이	OBU와 LR 사이
OBU의 세션 키 생성 개수		1	1	N	1	1
세션 키 생성을 위해 교환하는 메시지 개수	RSU 간 핸드오버	4	2	M + N	L + 1	0
	LR 간 핸드오버	0	0	0	0	2
PBS (Perfect Backward Secrecy)		PBS 지원	PBS 지원	PBS 지원	PBS 지원	PBS 지원 못함 - OBU와 LR 간의 주기적인 TEK 교환으로 PBS 지원

M: RSU의 neighbor RSU 수, N: Notify-Request 메시지에 응답한 RSU 개수, L: FHR에 의해 선택된 RSU 개수 ($0 \le N \le M$, $0 \le L \le N$)

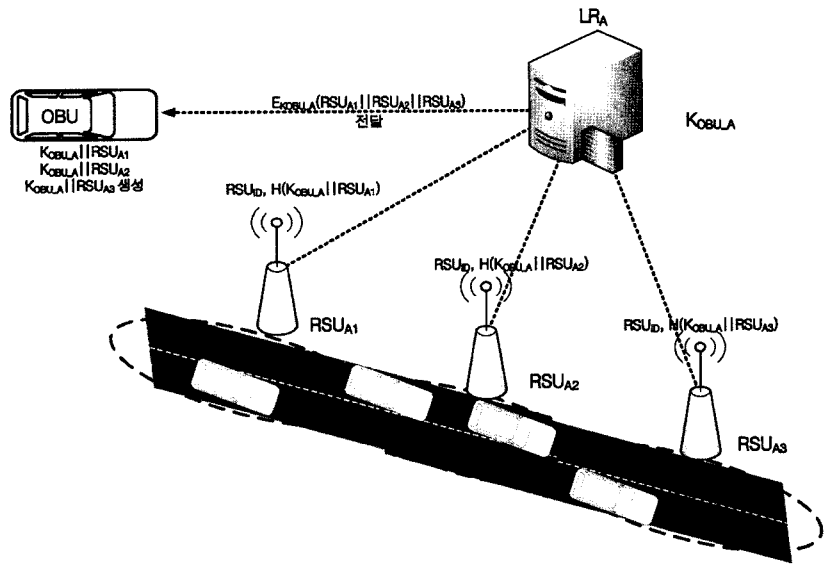

그림 3 동일한 LR에서의 OBU와 RSU 간의 세션 키 전달 구조

LR과의 안전한 채널을 이용해 전달함으로써 OBU와 LR 간 세션 키를 공유하게 된다. OBU는 LR과의 세션 키를 기반으로 OBU와 RSU 간의 세션 키를 RSU_{ID} 정보만을 이용하여 RSU가 LR로부터 수신한 세션 키와 동일한 세션 키를 생성하게 됨으로써 RSU의 이동 시 추가적인 메시지 교환 없이 OBU와 RSU는 세션 키를 공유할 수 있다. 그러므로 OBU가 이동한 RSU 개수만큼 세션 키를 생성하는 기존의 방식과는 달리 제안한 기법은 이동한 LR 개수만큼만 세션 키를 생성함으로써 세션 키 생성 횟수를 줄였다. 또한 차량의 빠른 이동성을 고려하여 V2I 간 세션 키를 OBU가 다른 영역의 LR로 이동 전 LR 간의 안전한 채널을 통하여 전에 전달할 수 있어 IEEE 802.11i와 PKI보다 신속한 핸드오버 세션 키를 전달할 수 있다.

제안 기법은 OBU와 LR가 세션 키 생성 시 보안 파라미터(security context) 전달 방식으로 AAA 서버와 CA 서버를 이용하지 않고 V2I 간의 세션 키를 생성함으로써 세션 키 생성 시 발생되는 메시지 전송 지연 시간 및 서버의 오버헤드를 줄였다. 또한 새로운 세션 키 교환을 위해 OBU와 LR 간 2번의 메시지 교환만을 수행함으로써 기존의 세션 키 교환 방식인 IEEE 802.11i, Proactive, FHR 방식 보다 메시지 전송 횟수가 적은 장점이 있다.

그러나 제안 기법은 악의적인 공격자에게 세션 키가 노출 될 경우 추가적으로 생성 되는 세션 키의 유추가 가능한 문제점이 있어 PFS 문제점을 보완하기 위해 주기적으로 IEEE 802.11i 과정을 통한 OBU와 LR 간의 세션 키 교환 과정이 필요하다. 또한 차량 무선 네트워크 환경 구축 시 기존의 시설에 LR을 추가적으로 설치해야 한다.

4.2 안전성 분석

핸드오버 세션 키 교환 기법은 멀티미디어 데이타와 같이 패킷 지연 시간에 민감한 데이타를 안전하게 전송하기 위한 세션 키 전달 과정을 최소화할 뿐만 아니라, 핸드오버 과정에서 안전하게 세션 키를 분배하고 정당한 이동 노드만이 안전하게 네트워크 액세스 서비스를 이용할 수 있어야 한다.

본 논문에서 제안하는 핸드오버 세션 키 전달 기법은 LR과 RSU 간, LR과 LR 간 안전한 채널을 가정하였기 때문에 초기 부팅 과정 후 생성된 TEK를 RSU에서 LR에 전달하는 과정과 LR 사이에서 송·수신하는 ID_{OBU}, $H(K_{OBU_LR})$를 전달하는데 있어서 안전하다. 또한 OBU가 LR과 RSU 간, LR과 LR 간의 핸드오버 시 LR과 RSU는 이동한 OBU에 대해 사전에 등록된 OBU 인지 확인할 수 있다. 따라서 악의적인 공격자가 정상적인 OBU의 정보를 사용하여 새로운 RSU를 통해 불법적으로 네트워크에 접속을 시도할 경우 RSU는 OBU에 대해 사전에 등록된 OBU 인지를 확인을 위한 액세스 인증을 수행하고 인증된 OBU에 대해서만 네트워크 접근을 허가하여 악의적인 공격자의 접근을 차단할 수 있다. 또한 LR은 메시지에 포함된 RN을 비교, 검사하여 재생 공격을 예방할 수 있다.

제안 기법은 security context 전달 방식으로 AAA 서버를 사용하지 않고 현재 LR에서 다음 LR에게 세션 키

를 해쉬하여 안전한 채널을 통하여 전달하기 때문에 PFS (Perfect Forward Secrecy) 보안 서비스가 제공된다. 또한 OBU와 RSU 간 연속적인 세션 키 공유가 가능하여 무선 구간에서 악의적인 공격자에 의한 트래픽 위변조 공격, 위장 공격, 위조 공격 등으로부터 안전한 통신을 지원할 수 있다. 그러나 제안 기법은 기존의 LR에서 사용된 세션 키가 악의적인 공격자에게 노출될 경우 PBS의 취약점이 있다. 이를 보완하기 위하여 RN과 RSU_{ID}의 값을 포함한 계산 과정을 추가하였으나 근본적인 PBS 문제 해결을 위해서는 IEEE 802.11i 과정을 통해 주기적인 OBU와 LR 간의 세션 키 교환이 필요하다.

5. 결 론

본 논문에서는 VANET 환경에 적합한 V2I 간의 세션 키 교환 기법을 제안한다. 기존의 VANET 환경에서는 V2I 간의 안전한 통신 지원을 위하여 IEEE 802.11i와 PKI에서 무선 구간의 데이타 보호를 위한 방법들이 연구 되고 있으나 차량의 고속 이동에 따른 잦은 네트워크 환경 변화 시 신속하고 연속적인 V2I 간의 세션 키 교환이 어렵다. 본 논문에서는 이러한 문제점을 고려하여 VANET 환경에 적절한 V2I 간의 신속한 세션 키 교환 기법을 제안하였다. 제안기법은 OBU와 각각의 RSU간의 세션 키를 교환하지 않고 OBU와 LR간의 세션 키를 교환함으로써 세션 키 생성 횟수를 줄였으며, 초기 사용자 인증 후 추가적인 사용자 인증 없이 세션 키를 교환함으로써 신속한 V2I 간의 세션 키 교환이 가능하다.

참 고 문 헌

[1] R. Mietzner, "COMeSafety," In Proc. of SEVECOM Workshop, BMW Group, February 2006.

[2] SEVECOM, "Secure Vehicular Communication," http://www.sevecom.org, June 2007.

[3] S. Corson and J. Macker, "Mobile ad-hoc networking (MANET)," IETF RFC 2051, January 1999.

[4] V. Devarapalli, et al., "Network mobility basic support protocol," IETF, RFC 3963, January 2005.

[5] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," IETF RFC 3775, June 2004.

[6] P. McCann, "Mobile IPv6 fast handovers for 802.11 Networks," IETF RFC 4260, November 2005.

[7] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, "Hierachical mobile IPv6 mobility management (HMIPv6)," RFC 4140, IETF, August 2005.

[8] M. Raya, P. Papadimitrators, and J. Hubaux, "Securing vehicular communications," In Magazine of IEEE Wireless Communications-IVC Specials, EPFL, pp.8-15, October 2006.

[9] IEEE, "IEEE standard for information technology-telecommunications and information exchange between systems-Local and metropolitan area networks-specific requirements Part 11: Wireless LAN medium access control and physical layer specifications Amendment 6: Medium access control security enhancements," IEEE Std 802.11i, July 2004.

[10] S. Boeyen, T. Howes, and P. Richard, "Internet X.509 public key infrastructure operational protocols-LDAPv2," RFC 2559, IETF PKIX Working Group, April 1999.

[11] IEEE, "IEEE trial-use standard for wireless access in vehicular environments security services for applications and management messages," IEEE Std 1609.2, July 2006.

[12] CALM, "Continuous air interface for long and medium range," http://www.tc204wg16.de/, October 2007.

[13] IEEE standard, "Part 16: Air interface for fixed and mobile broadband wireless access systems amendment 2: physical and medium access control layers for combined fixed and mobile operation in licensed bands," IEEE 802.16e, 2005.

[14] A. Mishra, S. Min Ho, L. Nick, J. Petroni, T. Charles Clancy, and A. William, "Proactive key distribution using neighbor graphs," IEEE Wireless Communications, Volume 11, pp.26-36, February 2004.

[15] S. Pack and Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems," IEE Proceedings-Communications, Volume 151, pp.489-495, October 2004.

[16] A. Mukherjee, T. Joshi, and P. Agrawal, "Minimizing re-authentication overheads in infrastructure IEEE 802.11 WLAN networks," IEEE WCNC 2005, Volume 4, pp.13-17, March 2005.

유 승 호

2005년 2월 안동대학교 정보 통신공학과 (학사). 2008년 2월 숭실대학교 정보 통신전자공학과(석사). 2008년~현재 한국정보인증 서비스 개발팀 연구원. 관심분야는 이동 네트워크 보안, 네트워크 보안

정 수 환

1985년 2월 서울대학교 전자 공학과(학사). 1987년 2월 서울대학교 전자 공학과 (석사). 1998년~1991년 한국통신 전임연구원. 1996년 6월 University of Washington(박사). 1996년~1997년 Stellar One SW Engineer. 1997년~현재 숭실대학교 정보통신전자공학부 부교수. 관심분야는 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안