논문 2009-46TC-1-15

VANET의 V2I 환경에서 IBC를 이용한 세션키 분배 기법

(Session Key Distribution Scheme in V2I of VANET using Identity-Based Cryptography)

노 효 선*, 정 수 환**

(Hyosun Roh and Souhwan Jung)

요 약

본 논문은 VANET (Vehicular Ad-hoc Network)의 V2I 환경을 위해 ID 기반의 비대화형 키 분배 기법을 적용한 세션키 분배 기법을 제안한다. 기존 VANET에서는 V2I 환경의 무선 구간에 IEEE 802.11i를 적용하여 안전한 데이터 통신을 지원하고 있다. 그러나 IEEE 802.11i의 경우 차량이 여러 RSU/AP를 핸드오버 할 때마다 새로운 세션키 공유를 위해 4-way handshake 과정을 반복함으로 커뮤니케이션 오버헤드와 지연시간이 증가하는 문제점이 있다. 제안 기법은 ID 기반의 비대화형 키 분배 알고리즘을 적용하여 차량이 여러 RSU/AP를 핸드오버 할 경우 세션키 생성을 위한 메시지 교환 없이 상대 노드의 ID 정보를 통해 세션키를 생성하고 공유할 수 있게 하였으며, 기존 IEEE802.11i에 비해 세션키 교환시 발생하는 커뮤니케이션 오버헤드와 지연시간을 줄였다.

Abstract

This paper proposes a session key distribution scheme on non-interactive key distribution algorithm of Identity-based cryptography in V2I of VANET. In the current VANET, IEEE 802.11i is used to provide secure data communication between the vehicle and infrastructure. However, since the 4-way handshake procedure reply when the vehicle handover to another RSU/AP, IEEE 802.11i increases the communication overhead and latency. The proposed scheme using non-interactive key distribution algorithm of Identity-based cryptography provided session key generation and exchange without message exchange and reduced communication overhead and latency than the IEEE 802.11i.

Keywords: VANET, ID 기반, 세션키 교환, Ad hoc

I. 서 론

VANET (Vehicular Ad hoc NETwork)은 최근 활발하게 연구가 진행되고 있는 지능형 교통 안전시스템 (ITS: Intelligent Transportation System)에서 무선 네트워크 기술을 이용하여 차량통신을 제공하기 위한 네트워크 기술이다[1~2]. VANET에서 제안되고 있는 차량통신은 교통정보 제공 서비스, 인터넷 접속 서비스, 엔터테인먼트 서비스 등을 주목적으로 하는 V2I (Vehicular-to-Infrastructure) 통신과 차량안전 관련 정보 교환, 교차로 진입 제어, 차량 주변의 상황을 고려한 실시간 서비스 등을 주목적으로 하는 V2V (Vehicular-to-Vehicular) 통신으로 나누어진다.

VANET에서는 효과적인 V2I 및 V2V 통신을 지원하기 위해서 MANET (Mobile Ad-hoc Network)[3], NEMO (Network Mobility)[4], MIPv6 (Mobile IPv6)[5~6], WLAN (Wireless LAN) 등 다양한 무선 네트워크 기술이 V2V와 V2I 환경에 적용되고 있다. VANET의 V2I 환경에서는 이동 간에도 원활하게 인터넷 서비스를 받을 수 있도록 지원하기 위해 MIPv6, WLAN, NEMO 기술들을 적용하여 끊김 없는 서비스를 제공하기 위한 연구가 꾸준히 진행되고 있다. 또한 VANET

* 정회원, ** 평생회원-교신저자, 숭실대학교 정보통신전자공학부
(School of electronic Engineering, Soongsil University)
※ 이 논문은 숭실대학교 교내 연구비 지원에 의해 수행되었음
접수일자: 2008년8월20일, 수정완료일: 2009년1월19일

V2V 환경의 경우 MANET 기술을 적용하여 고속으로 이동하는 차량과 차량 간 통신을 지원하기 위한 연구가 활발하게 진행되고 있다. 이렇듯 VANET은 무선 네트워크 환경을 기반으로 개발되고 있기 때문에 무선 네트워크 환경에서 존재하는 보안 취약성을 그대로 가지고 있으며, 또한 차량의 고속 이동에 따른 빠른 네트워크 토폴로지 변화로 인한 보안 취약성이 존재한다[7]. 이와 같은 VANET 환경에서의 보안 취약성을 해결하여 다양한 응용서비스를 차량 통신에서 활용하기 위한 보안 구조 연구가 국내뿐만 아니라 미국, 유럽을 비롯한 여러 국가들에서 활발하게 진행되고 있다. 특히 유럽의 경우 국가지원 과제인 i2010 Flagship의 Intelligent Car Initiative를 통해 지능형 차량과 보안을 위한 전략수립과 세부과제를 수행하고 있으며, 미국은 IEEE 802.11p/P1609 (WAVE)에서 VSCC (Vehicle Safety Communication Consortium)의 지원을 받아 차량 통신 보안 및 무선 인프라 표준화 규격을 만들기 위한 연구를 진행하고 있다. 최근에는 V2I 환경에서 IEEE 802.11i 표준[8]을 차량 보안 구조에 적용하기 위한 기술들이 제안되고 있다. IEEE 802.11i는 IEEE 802.11 작업그룹의 TG (Task Group) i에서 제안되었으며, 무선 제품들이 동작하는데 있어 어떻게 보안을 유지할 것인가에 대한 기술들이 정의되어 있다. 특히 IEEE 802.11i는 무선랜 프라이버시 강화를 위한 방안으로 RSN (Robust Security Network) 보안 구조를 채택하여 협상을 통한 보안세션관리, 4-way handshake 과정을 통한 키 공유기법을 정의하고 있다. 또한 단기적인 프라이버시 기법인 TKIP (Temporal Key Integrity Protocol)와 장기적인 프라이버시 기법인 CCMP (Counter Mode-CBC MAC Protocol)를 제안하고 있다. 그러나 IEEE 802.11i의 경우 현재 접속된 AP와의 세션이 끊기고, 새로운 AP로 이동할 경우 EAP-TLS 전체 인증을 통해 사용자가 재인증을 받아야 하고, 4-way handshake 과정을 통해 세션키를 새롭게 공유하게 되므로 커뮤니케이션 오버헤드 및 지연시간이 증가하는 문제점이 있다. 따라서 이러한 문제를 해결할 수 있는 세션키 분배 기법이 필요하다.

본 논문에서는 앞서 언급한 문제를 해결하기 위해 VANET의 V2I 환경에서 차량의 ID를 이용한 키 생성을 통해 V2I 환경에서의 빠른 세션키 교환 및 데이터의 안전한 통신을 위한 ID 기반의 세션키 교환 기법을 제안한다. 제안하는 기법은 차량의 ID로 사용할 수 있는 IP 주소 등을 이용하여 각 차량을 위한 마스터 세션키를 생성하고, 생성된 마스터 세션키를 VANET 환경에 가입하는 차량에게 분배함으로서 이후 마스터 세션키를 가진 노드들 간에 키 교환 없이 세션키를 공유하고, 생성한 세션키로 데이터를 암호화하여 안전한 통신을 할 수 있도록 제안하였다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 기존 VANET의 V2I 환경에서 세션키 교환 기법에 대해서 살펴보고, Ⅲ장에서 안전한 세션키 교환 기법을 제안한다. Ⅳ장에서 제안 기법의 안전성 분석 및 기존 기술과의 비교 분석을 하고, 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 기술

VANET의 V2V 환경에서 제공되는 지능형 차량 서비스들을 위해 차량과 차량 간에 주고받는 메시지들에는 차량의 안전을 위한 중요한 정보들이 포함되어 있다. 따라서 이러한 메시지들이 악의적인 목적으로 변경, 사용되지 않도록 하기 위한 보안 기법들이 필요하고, 이를 위해 VANET의 특성을 고려한 키 분배 기법이 필요하다.

1. 키 분배방법

- 비대화형 키 분배방법

Maurer와 Yacobi가 Eurocrypt' 91에서 제안한 키 분배방법으로 신뢰할 수 있는 키 분배 서버의 비밀정보와 사용자의 ID를 이용한 이산대수를 통해 ID 소유자의 비밀키를 생성하는 방법이다[9]. 이 방법의 핵심은 적절하게 선택된 어떤 큰 합성수 m을 소인수분해하는 것은 계산상 불가능하다는 것과, 충분히 큰 소수 p에 대한 이산대수를 계산하는 것이 가능하다는 것을 기반으로 하고 있다. Maurer-Yacobi가 제안한 이 방법은 시스템 초기화 과정과 사용자 등록 및 키 분배 과정으로 나누어진다. 먼저 시스템 초기화 과정이 시작되면 신뢰할 수 있는 키 분배 서버는 네 개의 소수 p_j를 선택한다. 다음은 사용자 등록 및 키 분배과정으로 사용자 U_i가 자신의 ID_i를 신뢰할 수 있는 키 분배 서버에 등록하기 원할 경우 자신의 식별 정보를 오프라인 또는 온라인으로 안전한 방법을 통해 신뢰할 수 있는 키 분배 서버에게 전달한다. 이후 신뢰할 수 있는 키 분배 서버는 다음의 식 1과 같이 등록을 원하는 사용자 U_i의 ID와 자신

의 비밀 값을 이용하여 비밀 키 S_i를 생성한다.

$$S_i = \log_g(ID_i^2) \bmod \phi(m) \quad (1)$$

위의 식에서처럼 등록을 원하는 사용자 U_i를 위한 비밀키 S_i를 생성한 다음 신뢰할 수 있는 키 분배 서버는 안전한 방법을 통해 사용자 U_i에게 비밀키를 전달한다. 이후 비밀키를 전달받은 사용자 U_i는 신뢰할 수 있는 키 분배 서버에 등록하고 비밀키를 분배받은 또 다른 사용자들과 상대방의 ID를 이용하여 세션키를 공유하게 된다. 사용자 U_i가 사용자 U_j와 세션키를 공유하기 원할 경우 사용자 U_i는 신뢰할 수 있는 키 분배 서버로부터 전달받은 비밀키와 사용자 U_j의 ID_j를 다음의 식 2와 같이 한 번의 모듈라 멱승 계산을 통해 세션키를 계산하여 공유하게 된다.

$$K_{ij} \equiv (ID_j)^{2S_i} \equiv (ID_i)^{2S_j} \quad (2)$$

사용자 U_j도 위의 식 2에서와 같이 사용자 U_i의 ID_i와 자신의 비밀키를 이용하여 동일한 세션키를 생성한다. 위에서처럼 Maurer-Yacobi가 제안한 이 방법은 신뢰할 수 있는 키 분배 서버에 등록된 두 사용자 간에 세션키 공유를 위한 메시지 교환 없이도 세션키를 공유할 수 있게 한다.

- IEEE 802.11i

IEEE 802.11i는 기존 무선랜 환경에서 WEP (Wired Equivalent Privacy)을 이용하여 제공하던 보안 서비스에 문제점이 드러남에 따라 이를 보완하고, 이동 단말이 여러 AP (Access Point)를 핸드오버 하는 경우에도 안전한 보안 서비스를 제공받을 수 있도록 표준화 하고 있다. 특히 IEEE 802.11i 표준에서는 무선구간에서의 데이터 보호기능을 강화하기 위해 RSN (Robust Security Network) 보안 구조를 적용하였다. RSN은 IEEE 802.1X 기반 인증 구조로서 포트기반접근제어 (Port-Based Access Control)를 통해 사용자 인증, 키 관리, 무선구간 암호화 및 핸드오버 보안 프레임워크를 제공한다. 또한 RSN에서는 단기적인 프라이버시 제공을 위해 AES (Advanced Encryption Standard)와 TKIP (Temporal Key Integrity Protocol)를 사용한다. TKIP는 기존 WEP RC4의 보안 취약성을 소프트웨어적으로 패치하여 이동 단말과 AP 간의 보안 취약성을 해결하고, 보안을 강화할 수 있게 한다. IEEE 802.11i의 개선된 인증방식은 크게 인증서버 기반의 인증방식과 사전 공유

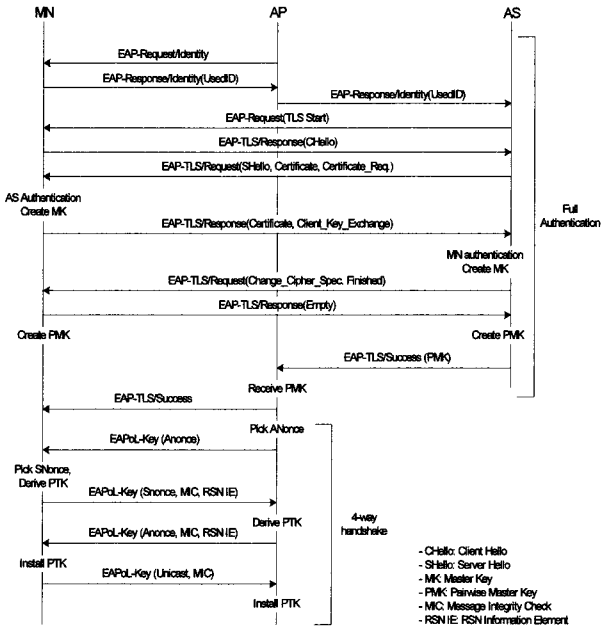

그림 1. IEEE 802.11i 전체 인증과정
Fig. 1. IEEE 802.11i Authentication Procedure.

키 기반의 인증 방식으로 나눌 수 있다. 인증서버 기반의 인증방식의 경우 인증서버와 이동 단말간 상호인증을 위해 EAP-TLS, EAP-MD5 또는 EAP-TTLS 등을 이용하여 인증과정을 수행한다. 인증과정이 성공적으로 마무리되면 무선구간의 암호화에 필요한 임시키를 IEEE 802.1X 표준에 정의된 키 분배절차에 따라 키를 설정한다. 사전 공유키 기반의 인증 방식의 경우 인증서버 없이 이동 단말과 AP간에 사전에 공유하고 있는 공유키를 사용하여 사용자가 AP에 접속할 경우 인증을 수행한다. 인증이 성공적으로 마무리되면 인증서버 기반의 인증방식에서와 같이 무선구간의 암호화를 위해 필요한 키를 설정한다. 그림 1은 IEEE 802.11i의 전체 인증과 4-way handshake 과정을 보여준다.

앞에서 살펴본 바와 같이 IEEE 802.11i의 경우 전체 인증과정이 끝난 후 AP와 이동 단말 간에 4-way handshake 과정을 통해 무선구간 암호화에 사용되는 키를 분배한다. 이러한 과정은 이동 단말이 새로운 AP로 핸드오버할 경우 매번 반복해야하는 과정으로 차량이 고속으로 이동하며 핸드오버 하는 VANET 환경에 적용할 경우 키 교환 과정으로 인한 핸드오버 지연과 커뮤니케이션 오버헤드가 발생하게 된다. 따라서 이러한 핸드오버 지연시간과 커뮤니케이션 오버헤드를 줄일 수 있는 키 교환 기법이 필요하다.

Ⅲ. 제안기법

다음 그림 2는 본 논문에서 제안하는 INK (Identity-based Non-interactive session Key exchange scheme) 세션키 분배 기법이 적용되는 VANET의 V2V 및 V2I 네트워크 환경을 보여준다. 또한 본 논문에서 제안하는 기법에서 사용되는 용어들의 표기법을 표 1에서 정리하였다.

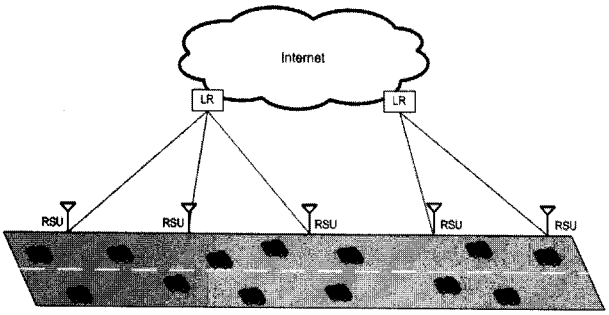

그림 2. VANET의 V2I 및 V2V 환경
Fig 2. V2I and V2V Environment of VANET.

표 1. 용어 정리
Table 1. Definition.

표 기	정 의
TEK	LR과 차량의 OBU와의 세션키
MK_M	OBU의 마스터 세션키
ID_x	OBU_X의 식별자
d_{LR}	LR의 비밀 값
n	LR의 공개 값
p_i	큰 소수
R_i	임의의 수
E_{TK}	TEK로 암호화
E_{SK}	세션키 SK_{ij}로 암호화
$h[\ ]$	일방향 해쉬함수
$Beacon$	비콘 메시지
t_{pi}	타임 스템프 값

1. 세션키 분배 기법

가. 설계 원리 및 제안 기법 개요

본 논문에서 제안하는 INK 세션키 교환 기법을 VANET 환경에 적용하기 위해서 다음과 같은 몇 가지 가정을 하였다. 첫째, 차량의 OBU (On Board Units)는 EAP-TLS로 초기 인증과정을 수행하고, 이후 LR (Local Router)과 TEK를 공유한다. 둘째, 지역적으로 RSU (Road Side Unit)를 관리하기 위한 LR이 적용된 계층적 구조를 가정하고, LR과 RSU 간은 IPSec 또는 TLS가 적용된 안전한 채널을 가정한다. 마지막으로 제안기법에서 사용하는 차량 OBU의 ID는 IP 주소를 사용하고, ID를 이용하여 마스터 세션키 MK를 생성하기 위해 Maurer-Yacobi의 키 생성 알고리즘을 사용한다.

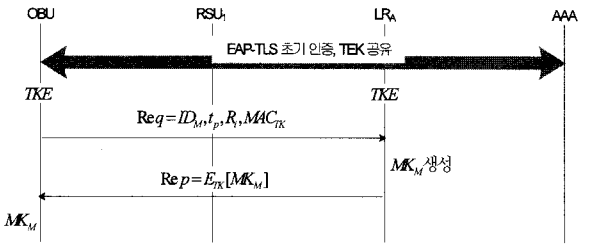

그림 3. 초기 인증 및 마스터 세션키 생성과정
Fig. 3. Initial Authentication and Master Session Key Generation Procedure.

그림 3은 차량의 초기 인증과정과 초기 인증 후 V2I와 V2V 환경에서 세션키 공유를 위해 필요한 마스터 세션키 MK를 분배받는 과정을 보여준다. 차량의 OBU가 처음 부팅을 시작하면 EAP-TLS를 통해 인증서버로부터 초기 인증을 받는다. 초기 인증 과정을 통해 LR과 차량의 OBU 간에는 안전한 방법으로 세션키 TEK를 공유하고, 초기 인증과정이 성공하면 차량의 OBU는 LR에게 마스터 세션키 MK_M을 요청한다. 마스터 세션키 MK_M 요청을 받은 LR은 요청한 차량의 ID를 이용하여 식 3과 같이 마스터 세션키 MK_M을 생성한다.

$$MK_M = d_{LR}(\log_g(ID_M)^2) \bmod \phi(n) \quad (3)$$

식 3과 같이 생성되는 마스터 세션키 MK_M은 각 차량의 ID를 이용하여 생성되므로 각 차량 마다 각기 다른 마스터 세션키 MK를 분배 받는다. 생성된 마스터 세션키 MK는 LR과 차량의 OBU 간에 공유하고 있는 TEK로 암호화하여 차량의 OBU에게 안전하게 전달된다.

나. 제안 기법

- 차량간 세션키 교환 과정

다음 그림 4는 동일한 LR 영역에 속한 차량들 간에 마스터 세션키 MK를 이용하여 세션키 SK를 공유하는 과정을 보여준다.

LR로부터 마스터 세션키 MK_{M1}을 분배받은 OBU_1은 이웃 차량이 주기적으로 브로드 캐스트하는 비콘 메시지를 통해 이웃 차량들의 ID 정보를 알게 된다. OBU_1

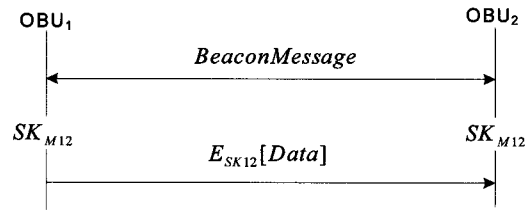

그림 4. 차량 간 세션키 교환 과정
Fig. 4. Session Key Exchange between the Vehiculars.

이 OBU_2와 안전한 통신을 원할 경우 OBU_1은 OBU_2의 ID를 이용하여 식 4와 같이 세션키 SK_{12}를 생성한다.

$$SK_{12} = (ID_{M2}^2)^{Ri * MK_{M1}} \bmod N \quad (4)$$

OBU_1은 세션키 SK_{12}를 생성한 다음 세션키로 전달하고자 하는 데이터를 암호화한 후 세션키를 생성할 때 사용한 임의의 수 R_i를 함께 OBU_2로 전송한다. 암호화된 메시지를 받은 OBU_2는 식 5과 같이 OBU_1의 ID와 R_i를 이용하여 동일한 세션키 SK_{12}를 생성한다.

$$SK_{12} = (ID_{M1}^2)^{Ri * MK_{M2}} \bmod N \quad (5)$$

이렇게 함으로써 세션키 교환을 위한 추가 메시지 필요 없이 LR이 분배한 마스터 세션키 MK_M을 통해 애드혹 모드로 통신하는 차량들 간에 세션키를 공유할 수 있으며 안전한 데이터 전송을 할 수 있다.

• LR 핸드오버시 세션키 교환 과정

아래 그림 5는 차량이 LR_A에서 LR_B로 핸드오버 하는 경우 V2I 간 마스터 세션키 교환 과정을 보여준다. 그림 5에서처럼 초기 인증 과정을 끝낸 차량의 OBU가 LR_A로부터 마스터 세션키 MK_M을 분배 받은 후 LR_B의 영역으로 핸드오버 하는 경우 LR_B로부터 새로운 마스터 세션키 MK_M'을 분배받는다. 이때 새롭게 발급되는 마스터 세션키 MK_M'의 분배 과정 가운데 발생할 수 있는 지연시간과 세션키 교환 과정에서 필요로 하는 메시지들로 인한 커뮤니케이션 오버헤드를 줄이기 위해 다음과 같은 과정으로 새로운 마스터 세션키 MK_M'을 분배한다.

VANET의 특성상 LR_A는 차량의 진행방향을 통해 차량이 어떤 LR의 방향으로 이동하는지 예측이 가능하다. 따라서 차량의 이동 방향에 존재하는 LR_B에게 새로운 마스터 세션키 MK_M'을 안전하게 전달하기 위해 사용되는 세션키 TEK'를 식 6과 같이 LR_A가 미리 생성하여 OBU의 ID_M와 함께 전달한다.

$$TEK' = h[TEK, ID_{LB}] \quad (6)$$

LR_A로부터 OBU의 ID_M와 새로운 세션키 TEK'를 전달받은 LR_B는 OBU의 ID_M를 이용하여 새로운 마스터 세션키 MK_M'을 생성한다. 이후 OBU는 LR_B의 영역으로 이동하면 RSU_{BX}가 브로드 캐스트하는 비콘 메시지를 통해 자신이 새로운 LR_B 영역으로 이동한 것을 인식하게 되고, 새로운 LR_B 영역에서 사용할 마스터 세션키를 요청하는 메시지를 식 6에서와 같이 동일한 방법으로 생성한 TEK'로 암호화하여 LR_B에게 전달한다. 전달되는 요청 메시는 식 7과 같이 요청하는 차량의 ID와 타임 스템프 그리고 임의의 수를 함께 암호화하여

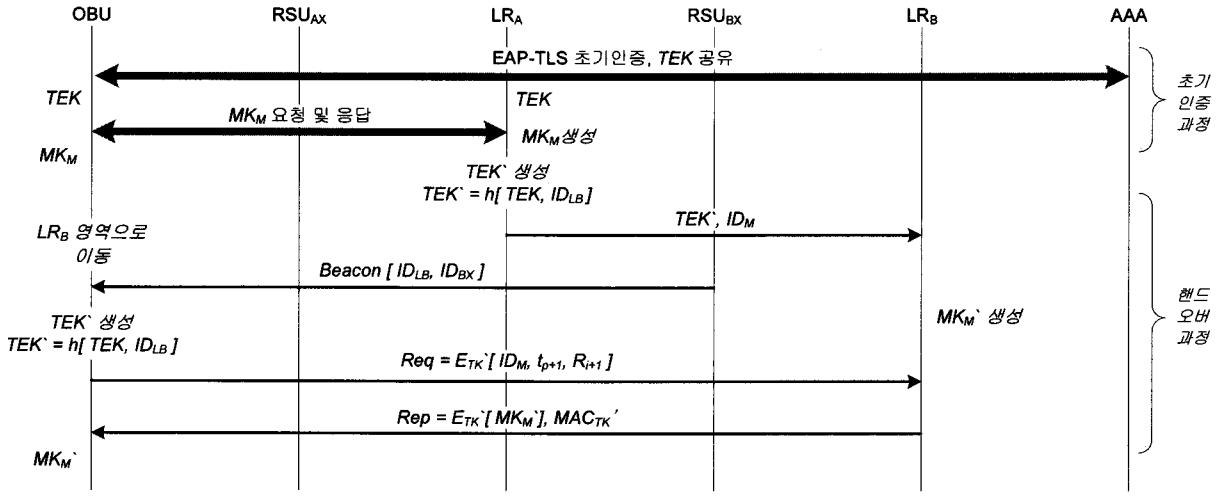

그림 5. 제안하는 세션키 교환 기법 메시지 흐름
Fig. 5. The Message Flow of the Proposed Session Key Exchange.

전송된다.

$$Req = E_{TK}'[ID_M, t_{p+1}, R_{i+1}] \quad (7)$$

OBU가 요청한 메시지를 수신한 LR_B는 요청 메시지를 확인 후 생성해둔 마스터 세션키 MK_M'를 식 8과 같이 생성하여 OBU에게 전달한다.

$$MAC_{TK}' = h[MK_M', TEK', t_{P+2}, R_{i+2}]$$
$$Rep = E_{TK}'[MK_M'], MAC_{TK}' \quad (8)$$

이렇게 함으로써 고속으로 이동하는 차량과 LR 간에 빠르게 세션키를 공유할 수 있게 지원하고, 또한 고속으로 LR의 영역을 이동하는 차량들 간의 안전한 세션키 공유 및 보안 통신을 지원한다.

IV. 분석 및 비교

1. 제안 프로토콜의 안전성 분석

• DoS 공격

DoS 공격에는 네트워크 트래픽을 과도하게 발생시켜 공격 대상 노드가 정상적인 작업을 수행하지 못하게 한다거나, 불필요한 과다 연산 수행을 통해 CPU 성능을 떨어뜨리는 형태의 공격이 있다. 일반적으로 네트워크 트래픽을 과도하게 발생시켜 공격하는 DoS 공격의 경우는 무차별적으로 대량의 메시지를 생성하여 공격하기 때문에 근본적으로 차단하는 것은 어렵다. 그러나 세션키를 요청하는 메시지를 대량 전송하여 불필요한 연산을 유도하는 DoS 공격에는 대응할 수 있다. 악의적인 공격자가 임의로 생성한 세션키 요청 메시지의 경우 세션키 생성 서버에서 세션키 생성을 위한 연산을 수행할 필요 없이 세션키 생성 요청을 거절할 수 있다. 세션키 요청 메시지에 포함되어 전달되는 *MAC* 값은 상호간에 공유하고 있는 *TEK*와 임의의 수, 타임 스템프 값 등을 해쉬하여 생성된다. 악의적인 공격자가 임의로 타임 스템프 값과 임의의 수를 변경하여 *MAC*을 생성하더라도 *TEK*를 알지 못하기 때문에 정상적인 *MAC*을 생성할 수 없다. 때문에 세션키를 생성하는 서버에서는 세션키 요청 메시지의 *MAC*을 검사하기 위한 한 번의 해쉬 계산이후 검증이 실패하면 추가적인 연산을 수행하지 않기 때문에 불필요한 연산 수행 부담을 줄일 수 있다.

• 재전송 공격

제안하는 기법은 차량의 OBU가 LR에게 마스터 세션키 MK_M을 요청할 때, 매 메시지마다 타임 스템프 값과 임의의 수를 바꾸어 LR과 사전에 공유하는 세션키 *TEK*로 암호화하여 전달하기 때문에 마스터 세션키 인증 요청 메시지 재전송 공격에 안전하다. 또한 차량 간에 공유하는 하는 세션키 SK_{ij}를 상호 검증하기 위해서 처음 데이터를 전송하는 차량의 OBU가 전달하는 메시지의 경우에도 매 메시지마다 포함되는 임의의수가 바뀌기 때문에 메시지 재전송 공격에 안전하다.

• 메시지 위조 및 OBU 위장 공격

제안하는 기법에서 공격자는 새로운 LR로 이동하는 차량이 마스터 세션키를 요청하는 메시지를 위조하거나, 차량 간에 공유하는 세션키를 임의로 위조하는 공격을 할 수 없다. 먼저 LR과 차량의 OBU 간에는 초기 인증 과정을 통해 안전하게 *TEK*를 공유한다. 이후 차량이 새로운 LR의 영역으로 이동할 경우 이전 LR은 새롭게 이동하는 LR의 *ID*와 차량의 OBU 간에 공유하고 있는 *TEK*를 해쉬하여 새로운 *TEK'*을 생성하고, 차량이 이동하는 LR에게 안전한 채널을 통해 전달한다. 이때 차량의 OBU는 새로운 LR 영역으로 이동하면 새로운 LR이 관리하는 RSU가 브로드 캐스트 하는 비콘 메시지에 포함된 LR의 *ID* 정보를 통해 자신이 새로운 LR 영역으로 이동한 것을 알게 되고, 이전 LR과 공유하고 있던 *TEK*와 새로운 LR의 *ID*를 해쉬하여 이전 LR이 생성하여 새로운 LR에게 전달해준 *TEK'*을 동일하게 생성한다. 이후 차량의 OBU는 새로운 마스터 세션키 MK_M'을 요청하는 메시지를 *TEK'*으로 암호화하여 전달한다. 공격자는 *TEK*를 알 수 없기 때문에 마스터 세션키를 요청하는 메시지를 위조할 수 없으며, 메시지와 함께 전달되는 MAC_{TK}'을 생성할 수 없으므로 메시지를 위조할 수 없다. 또한 V2V 통신을 하는 차량 간에 공유하는 세션키는 LR이 차량의 OBU의 *ID*와 LR 자신의 비밀 값 d_{LR}을 통해 생성하기 때문에 LR 이외의 어떤 노드도 마스터 세션키를 생성할 수 없으며, 생성된 마스터 세션키는 암호화되어 전달되기 때문에 제 삼자에게 알려지지 않는다. 따라서 악의적인 공격자가 OBU로 위장하기 위해서는 LR이 생성하는 마스터 세션키를 생성할 수 있어야 하지만, 이것은 불가능하다.

• MITM 공격

본 논문에서는 IPSec 또는 TLS와 같은 보안 프로토콜을 사용하여 LR 간, LR과 RSU 간에 안전한 채널이

형성되어 있음을 가정하였다. 따라서 LR 간에 주고받는 메시지와 LR과 RSU 간에 주고받는 메시지에 대해서 공격자는 MIMT 공격을 수행할 수 없다. 또한 LR과 차량의 OBU, RSU와 차량의 OBU 간에는 사전 SA가 설립되어 있지 않지만 초기 인증 과정을 통해 LR과 차량의 OBU 간 *TEK* 공유를 통해 SA가 형성된다. 이후 차량이 새로운 LR의 영역으로 이동할 경우 이전 LR을 통해 차량의 OBU와 공유하게 되는 새로운 *TEK'*을 전달받아 사용하며, 이 키를 통해 이동하는 OBU를 검증하기 때문에 *TEK*를 모르는 공격자는 MIMT 공격을 수행할 수 없다.

2. 기존 프로토콜과 비교 분석

다음 그림 6은 본 논문에서 제안하는 기법과 IEEE 802.11i의 세션키 공유 기법의 커뮤니케이션 오버헤드와 세션키 공유과정에서 발생하는 지연시간을 비교분석하기 위한 실험 환경을 보여준다.

실험 환경은 앞서 설명하고 있는 VANET 환경을 기반으로 했으며 제안하는 기법과 IEEE 802.11i의 초기 전체인증은 EAP-TLS를 사용하며, 각 장비 간에 발생하는 지연시간을 다음과 같이 정의하였다.

- t_{LA}: 인증 서버 AS와 LR 간 지연시간
- t_{RL}: LR과 RSU/AP 간 지연시간
- t_{OR}: RSU/AP와 차량의 OBU 간 지연시간
- t_{LL}: LR과 LR 간 지연시간
- t_{RR}: RSU/AP와 RSP/AP 간 지연시간

또한 본 논문에서는 이동 단말의 핸드오버를 LR 영역 내의 RSU 간의 핸드오버와 LR와 LR 간의 핸드오버로 구분하여 지연시간을 비교 분석하였다.

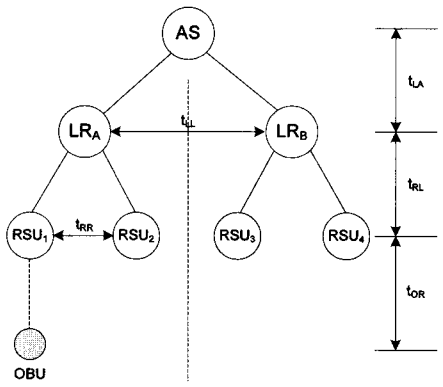

그림 6. 실험 환경
Fig. 6. Test Environment.

• 동일 LR에 속한 RSU/AP 간 핸드오버

IEEE 802.11i 환경에서 차량의 OBU는 EAP-TLS를 이용한 초기 전체인증을 수행한 후 4-way handshake 과정을 통해 RSU/AP와 세션키를 공유한다. 이후 차량의 OBU는 동일한 LR에 속한 RSU/AP들을 이동하며 각각의 RSU/AP들과 4-way handshake 과정을 반복수행하며 새롭게 세션키를 공유하고 이때 발생하는 지연시간은 다음 식 9와 같다.

$$T_D = T_I + (i_{RSU} \times 4t_{OR}) \tag{9}$$

위의 식에서 T_D는 핸드오버 과정에서 발생하는 지연시간, T_I는 초기 전체인증 과정의 지연시간, i_{RSU}는 핸드오버 하는 RSU/AP의 개수를 의미 한다.

다음으로 본 논문에서 제안하는 INK (Identity-based Non-interactive session Key exchange scheme)에서 EAP-TLS를 이용하여 초기 전체인증 과정이 성공하면, 차량의 OBU는 LR로부터 마스터 세션키를 분배받기 위해 자신의 *ID* 정보를 LR에게 전달하고, LR은 차량의 OBU와 자신의 비밀 값을 이용하여 생성한 마스터 세션키를 차량의 OBU에게 전달한다. 이후 동일한 LR에 속한 RSU/AP 간을 차량의 OBU가 핸드오버 하는 경우 차량의 OBU는 각 RSU/AP의 ID 정보와 마스터 세션키를 이용하여 세션키를 생성하고, 생성된 세션키를 확인하기 위한 한 번의 메시지를 교환한다. 이때 발생하는 지연시간은 다음 식 10과 같다.

$$T_D = T_I + 2t_{OR} + ((i_{RSU} - 1) \times t_{OR}) \tag{10}$$

다음 그림 7은 동일한 LR에 속한 10개의 RSU/AP를

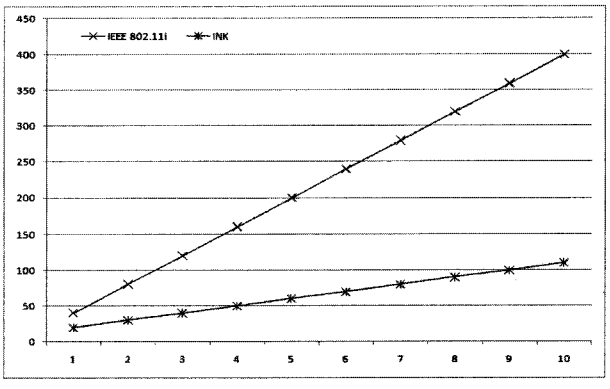

그림 7. RSU간 핸드오버 지연시간
Fig. 7. Handover latency between the RSUs.

핸드오버 하는 경우 발생하는 지연시간을 비교한 것이다. 지연시간을 비교하기 위해 무선 전송 구간의 메시지 전송 속도는 10ms로 가정하였고, 세로축은 지연시간, 가로축은 RSU/AP의 개수를 의미한다.

위의 그래프에서 확인할 수 있는 것처럼 본 논문에서 제안하는 INK의 경우가 기존 IEEE 802.11i에 비해 지연시간이 감소한 것을 확인할 수 있다.

• LR과 LR 간 핸드오버

다음은 차량이 다른 LR에 속한 RSU/AP로 핸드오버 하는 동안 세션키 공유과정에서 발생하는 지연시간을 비교하였다. 먼저 IEEE 802.11i의 경우 LR_A에서 LR_B로 이동할 경우 EAP-TLS 전체인증을 통해 재인증 과정을 수행하고, 이후 4-way handshake 과정을 통해 LR_B에 속한 RSU/AP와 세션키를 공유한다. 이때 발생하는 지연시간은 다음 식 11과 같다.

$$T_D = (j_{LR} \times T_I) + (i_{RSU} \times 4t_{OR}) \quad (11)$$

위의 식에서 j_{LR}은 LR의 개수이고, 새로운 LR로 핸드오버 할 경우 전체인증 과정이 추가된다. 그러나 본 논문에서 제안하는 INK의 경우 LR_A에서 LR_B로 핸드오버시 IEEE 802.11i에서처럼 전체인증을 하지 않고, LR_B의 RSU/AP와 세션키를 공유할 수 있기 때문에 지연시간이 감소하고, 이때 발생하는 지연시간은 식 12와 같다.

$$T_D = T_I + (j_{LR} \times 2t_{OR}) + ((i_{RSU} - j_{LR}) \times t_{OR}) \quad (12)$$

다음 그림 8은 LR 간 핸드오버시 세션키 공유과정 가운데 발생하는 지연시간을 비교하였다. 지연시간을 비교하기 위해 무선 전송 구간의 메시지 전송 속도는 10ms로 가정하였고, 세로축은 지연시간, 가로축은 RSU/AP의 개수를 의미한다.

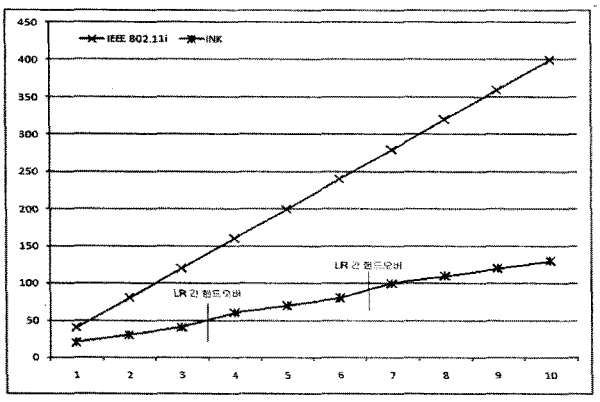

그림 8. LR간 핸드오버 지연시간
Fig. 8. Handover latency between the LRs.

앞의 그래프에서처럼 본 논문에서 제안하는 INK는 기존 IEEE 802.11i에 비해 지연시간이 감소함을 확인할 수 있다. 이는 세션키 교환을 위해 필요한 메시지의 수가 감소했기 때문이다. 기본적으로 IEEE 802.11i의 경우 차량의 OBU와 RSU/AP 간 세션키 교환은 4-way handshake 과정을 통해 이루어진다. 때문에 세션키 교환을 위해 4번의 메시지 교환이 필요하다. 앞에서도 확인한 것처럼 차량이 빈번하게 핸드오버를 수행할 경우 세션키 교환을 위한 4-way handshake 과정을 반복 수행해야 하기 때문에 커뮤니케이션 오버헤드가 증가하게 된다. 그러나 본 논문에서 제안하고 있는 INK의 경우 생성된 세션키를 확인하기 위해 한 번의 메시지 교환만을 필요로 하기 때문에 IEEE 802.11i에 비해 커뮤니케이션 오버헤드를 줄일 수 있다.

Ⅳ. 결 론

본 논문은 VANET (Vehicular Ad-hoc Network)의 V2I 환경에서 ID 기반의 비대화형 키 분배 알고리즘을 적용한 세션키 분배 기법을 제안하였다. 차량이 핸드오버할 때 기존 IEEE 802.11i를 통한 키 분배 기법의 경우 새로운 RSU/AP와 세션키를 교환하기 위해 4-way handshake 과정을 반복 수행해야만 한다. 때문에 핸드오버가 빈번하게 수행될 경우 세션키 분배과정에서 지연시간과 커뮤니케이션 오버헤드가 증가한다. 이러한 문제를 해결하기 위해 본 논문에서는 ID 기반의 비대화형 키분배 알고리즘을 적용한 INK를 제안하였고, 제안한 기법과 IEEE 802.11i의 비교분석을 통해 핸드오버 과정에서 발생하는 지연시간과 커뮤니케이션 오버헤드가 IEEE 802.11i에 비해 감소하는 것을 확인하였다.

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] M. Raya, P. Papadimitrators, and J. Hubaux, "Securing vehicular communications," In Magazine of IEEE Wireless Communications IVC Specials, EPFL, pp.8-15, October 2006.
[8] 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.
[9] M. Maurer and Y. Yacobi, "A remark on a Non-interactive public-key distribution system," EUROCRYPT' 92, 1998.

저 자 소 개

노 효 선(정회원)
2005년 숭실대학교 정보통신전자공학부 학사
2007년 숭실대학교 정보통신전자공학과 석사
2007년~현재 숭실대학교 전자공학과 박사과정
<주관심분야 : 이동 네트워크 보안, 네트워크 보안>

정 수 환(평생회원)-교신저자
1985년 서울대학교 전자공학과 학사
1987년 서울대학교 전자공학과 석사
1996년 University of Washington 박사
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
<주관심분야 : 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안>