

논문 2008-45TC-5-4

빠른 이동성을 지원하는 VANET 환경의 핸드오버 인증 프로토콜

(Handover Authentication Protocol in VANET Supporting the Fast Mobility)

최재덕*, 정수환**

(Jaeduck Choi and Souhwan Jung)

요약

본 논문은 VANET (Vehicular Ad hoc NETwork) 환경에서 안전하고 이동 단말에 적합한 Fast MIPv6 핸드오버 인증 프로토콜을 제안한다. 기존의 핸드오버 인증 프로토콜은 간단한 해쉬 함수나 XOR 연산을 사용하기 때문에 자원이 한정적인 이동 단말에 적합하지만, PBS와 같은 기본 보안 기능을 제공하지 못하는 문제점이 있다. 반대로 보안 문제를 해결하기 위하여 CGA (Cryptographically Generated Addresses) 기반의 RSA 공개키를 사용하는 기법이 제안되었지만, 액세스 라우터와 이동 단말에서 많은 지수 연산을 요구하기 때문에 액세스 라우터를 대상으로 DoS 공격이 가능하고 이동 단말에 적합하지 않다. 제안 프로토콜은 light-weight Diffie-Hellman 알고리즘을 사용하여 기존의 핸드오버 인증 프로토콜보다 PBS와 같은 기본적인 보안 특징을 제공하며, DoS 공격으로부터 안전하고, 기존의 방법보다 이동 단말에서 수행하는 지수 연산량이 적어 이동 단말에 적합하다.

Abstract

This paper proposes a secure and efficient handover authentication protocol in VANET supporting fast mobility. Although the existing schemes commonly use the hash function or XOR operation to be suitable for a light-weight mobile, it does not support the security feature such as PBS. To solve this security problem, another protocol utilizing the CGA technology is proposed but it is vulnerable to the DoS attack due to a number of exponent operations. The proposed protocol using a light-weight Diffie-Hellman provides security features and performs a reduced number of exponential operation at the MN than the existing scheme.

Keywords : VANET, 핸드오버 인증, Fast MIPv6, Diffie-Hellman

I. 서 론

VANET (Vehicular Ad hoc NETwork)은 차량과 차량 사이 또는 차량과 RSU (Road Side Unit) 사이에서

교통안전 정보를 제공해주는 V2V (Vehicular-to-Vehicular) 환경과, 차량내의 단말 또는 사용자 휴대용 단말 등을 사용하여 인터넷 서비스를 이용할 수 있는 V2I (Vehicular-to-Infrastructure) 통신 구조로 구분된다. V2V 환경은 이동 애드 흑 (Mobile Ad hoc) 네트워크 구조이고, V2I는 RSU를 거쳐 기존 인프라 구조에 액세스 할 수 있는 구조이다. VANET에서는 운전자의 생명을 보호하기 위한 안전 통신 기술이 중요하기 때문에 V2V 환경에서 교통사고 발생, 갑작스런 기상 변화, 노면 결빙 상태 등을 뒤따르는 차량들에게 안전하고 신뢰성 있게 전달해주는 기술이 중요시 여겨지고 있다. 그러나 최근 사용자의 멀티미디어 서비스에 대한 수요

* 정회원, ** 평생회원-교신저자,
숭실대학교 정보통신전자공학부
(School of Electronic Engineering, Soongsil University)

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

접수일자: 2008년2월5일, 수정완료일: 2008년5월18일

가 증가하면서 이동 중에도 차량 내에 장착된 단말 또는 사용자의 노트북, PDA와 같은 단말들을 사용하여 멀티미디어 서비스를 받고자 하는 경향 또한 증가하고 있다.

VANET V2I 환경에서 차량 이동 중에도 멀티미디어 서비스를 받기 위해서는 MIPv6 (Mobile IPv6)^[1] 기술이 필요하다. 멀티미디어 서비스 특성상 끊김 없는 서비스를 요구하는 환경에서 MIPv6 기술은 네트워크 계층 간 핸드오버시에 IP 패킷 손실을 최소화하고 끊김 없는 전달을 지원할 수 있다. 그러나 MIPv6는 기본 동작 모델에서 이동성 감지, CoA (Care-of-Address) 설정, 위치 정보 업데이트 문제 때문에 실질적으로 빠른 핸드오버 지원이 어렵다. 이에 IETF MIPSHOP WG에서는 MIPv6의 근본적인 문제를 해결하고 보다 빠른 네트워크 계층의 핸드오버를 제공하기 위하여 FMIPv6 (Fast MIPv6)^[2] 기술을 표준화하였다. FMIPv6에서는 MN (Mobile Node)이 NAR (Next Access Router)로 핸드오버 하기 전에 NAR에 대한 정보를 PAR (Previous Access Router)로부터 미리 획득하고 NCoA (NAR CoA)를 미리 설정한 후에 NAR로 핸드오버 하기 때문에 MIPv6 보다 빠른 핸드오버를 지원한다.

FMIPv6 환경에서는 MN이 AR을 이동함에 따라 새로운 주소를 생성하고, 새로운 주소를 이전 주소와 바꿔주는 FBU (Fast Binding Update) 과정을 안전하게 수행해야 한다. 그렇지 않을 경우 공격자가 FBU 과정을 악의적으로 사용하여 DoS 공격 또는 패킷 경로 재설정 공격 등을 수행할 수 있다^{[1][2]}. 이러한 문제를 해결하기 위하여, FMIPv6 핸드오버 인증키 교환 프로토콜들이 많이 연구되고 있다. FMIPv6 핸드오버 인증 기술들은 AAA 기반의 FMIPv6 핸드오버 인증 기술과, non-AAA 기반의 인증 기술들로 분류될 수 있다. 일반적으로 AAA 기반의 인증 방식은 높은 보안성을 제공해주지만, 핸드오버 인증이 수행될 때마다 AAA 서버와 통신해야 하기 때문에 MN과 AAA 서버 간에 인증 요청 메시지의 RTT (Round Trip Time) 지연과 AAA 네트워크에서 인증 트래픽 폭주로 인한 패킷 지연 및 손실이 발생할 수 있다. Non-AAA 기반의 방식은 핸드오버 인증이 AAA 서버 대신 AR과 MN 간에 이루어지기 때문에 핸드오버 인증 패킷의 지연 및 손실이 적은 장점이 있다. 그러나 non-AAA 방식은 신뢰 관계가 없는 MN과 AR 사이에서 높은 보안성을 제공하기 위하여 공개키 암호 방식과 같이 연산량이 많은 암호 알고리즘을 사용하기 때문에 자원이 한정적인 이동 단말

에 적합하지 않다. 이와 같이, 핸드오버 인증 프로토콜 설계시에 단말의 성능과 보안 사이에서 트레이드 오프 (Trade off) 문제가 발생한다.

본 논문에서는 FMIPv6와 같이 빠른 이동성 기술을 제공하는 VANET 환경에서 light-weight DH (Diffie-Hellman)을 사용하여 non-AAA 기반의 안전하고 효율적인 핸드오버 인증키 교환 프로토콜을 제안한다. 제안 프로토콜은 MN과 PAR 간에 이미 형성되어 있는 SA (Security Association)를 기반으로 MN과 NAR 사이에서 DH 알고리즘을 사용하여 핸드오버 인증키를 교환한다. 제안 기법은 기존 non-AAA 방식보다 PBS (Perfect Backward Secrecy)와 같은 기본적인 보안 기능을 제공하고, DoS 공격으로부터 안전하다. 또한 제안 프로토콜은 단말에서 DH 지수 연산에 따른 오버헤드를 줄이기 위하여 단말의 DH 공개키 지수 연산을 AR에게 위임하는 light-weight DH 방식을 사용하였다. 따라서 MN은 1회의 지수 연산만을 수행한다.

본 논문의 구성은 다음과 같다. II장에서 FMIPv6 고속 이동성을 제공하는 VANET 구조와 기존의 FMIPv6 핸드오버 인증 기술에 대해서 살펴보고, III장에서 안전하고 효율적인 FMIPv6 핸드오버 인증키 교환 프로토콜을 제안한다. IV장에서 제안 기술의 안전성 분석 및 기존 기술과 비교 분석한다. 마지막으로 V장에서 결론을 맺는다.

II. 관련 기술

1. FMIPv6 고속 이동성을 제공하는 VANET 환경

VANET 환경에서 빠른 이동성 제공은 필수적이다. IETF MIPSHOP WG에서는 네트워크 계층에서 이동성을 제공하기 위하여 표준화되었던 MIPv6의 이동성 감지, CoA 설정, 위치 정보 업데이트 문제 등을 해결하여 네트워크 계층에서 빠른 이동성을 제공해주는 FMIPv6 기술을 표준화하였다^[2]. Mussabbir 등은 차량 네트워크에서 IEEE 802.21 MIH (Media Independent Handover) 기술을 사용하여 FMIPv6를 최적화하는 기술을 제안하였다^[4]. Mussabbir 등이 제안한 기술에서 링크 계층의 액세스 기술에 상관없이 차량들은 네트워크 계층에서 FMIPv6 기술을 사용하여 최적화된 이동성 기술을 제공 받을 수 있다. 그림 1은 Mussabbir 등이 제안한 차량 네트워크 구조를 링크 계층에서 IEEE 802.11p 기술을 사용하는 구조로 재구성한 VANET 환경이다. 그림에서 차량들은 링크 계층에서 IEEE 802.11p 기술을 사

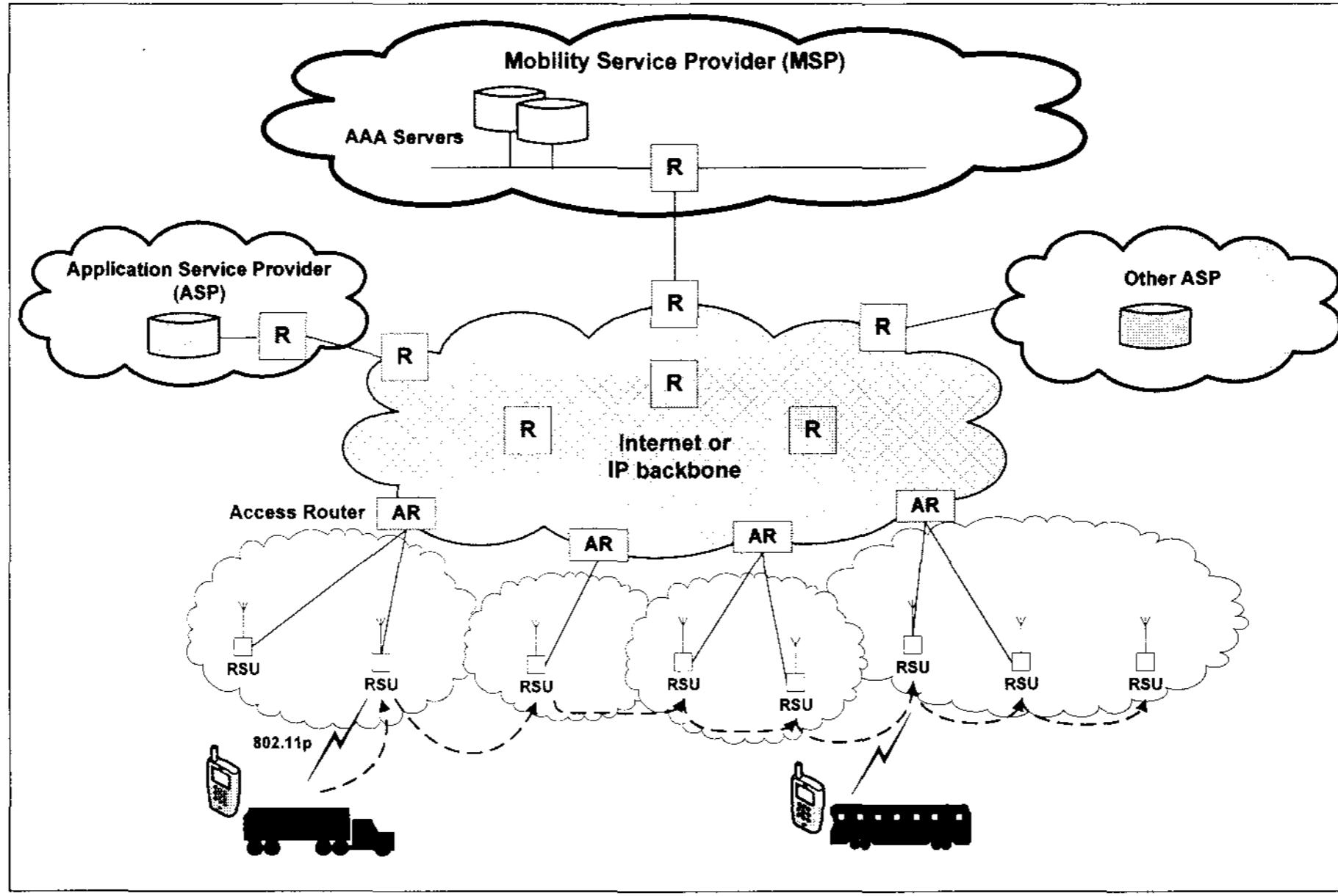


그림 1. FMIPv6 이동성을 제공하는 VANET 환경
Fig. 1. VANET Environment Supporting the FMIPv6.

용하여 RSU에 액세스하고, 인터넷 및 IP 백본망 접속은 네트워크 계층의 AR를 통해 통신한다. MSP (Mobility Service Provider)에 가입된 차량들은 이동성 서비스를 제공받기 전에 AAA 인증 서버와 초기 인증을 받고, 이동 중에는 FMIPv6 기술을 통해 핸드오버 및 인증을 수행한다. 또한 다양한 ASP (Application Service Provider)에 가입된 사용자 및 차량은 빠른 이동 중에도 네트워크 계층에서 FMIPv6 핸드오버 기술을 사용하여 실시간으로 끊김 없는 응용 서비스를 제공 받는다.

2. 기존의 FMIPv6 핸드오버 인증 기술

VANET V2I 통신 환경에서 네트워크 계층의 빠른 핸드오버 기술을 제공해주는 FMIPv6의 보안 기술들은 두 가지로 분류할 수 있다. 즉, AAA 기반과 non-AAA 기반의 핸드오버 인증기술로 분류된다. 먼저, AAA 기반의 핸드오버 인증 기술로는 공유키 기반의 핸드오버 키 분배 기법과^[5] 이동 노드 주도의 핸드오버 인증 기법이^[6] 있다. 공유키 기반의 핸드오버 키 분배 방식은^[5] MN과 AAA 서버 사이에 공유된 HMK (Handover Master Key)를 기반으로 MN과 PAR 간에 핸드오버 키 HK (Handover Key)를 생성한다. MN은 HMK로부터 직접 HK를 생성하고, PAR은 AAA 서버로부터 HK를 안전하게 전달 받는다. 이동 노드 주도의 핸드오버 인증 기법은^[6] FMIPv6 환경에서 네트워크 계층과 링크 계층의 핸드오버 인증 과정을 통합하였다. 이동 노드

주도의 핸드오버 인증 기술은 MN이 임의의 랜덤 값을 사용하여 직접 핸드오버 인증키 HMK를 생성하고, AAA 서버와 공유하고 있는 HKEK (Handover Key Encryption Key)를 사용하여 핸드오버 인증키 HMK를 암호화하여 AAA 서버에게 전달한다. AAA 서버는 HRAK (Handover Request Authentication Key)를 사용하여 MN을 인증한 후, HMK를 복호화하여 NAR에게 안전한 채널을 통해 전달한다. 이동 노드 주도의 핸드오버 인증 기술에서는 AAA 서버의 기능을 단순화시켜 AAA 서버의 오버헤드를 줄였고, 네트워크 계층과 링크 계층의 핸드오버 과정을 통합하여 핸드오버 인증 지연 시간을 줄일 수 있는 구조를 제시하였다.

Non-AAA 기반 방식은 AAA 서버를 통하지 않고 MN과 AR 사이에서 핸드오버 인증키를 교환하는 방식이다. 가장 간단한 방법으로 Wang 등의 기법에서는 SN (Serving Network)이 MN과 TN (Target Network) 간 세션키 교환을 위하여, SN이 SN과 MN 사이에서 사용하였던 세션키 K_s 를 랜덤값과 XOR 연산하여 생성된 K_M 을 TN에게 안전한 채널을 통해 전달한다^[7]. Wang 등의 기법은 간단한 방법으로 핸드오버 인증을 수행할 수 있지만, SN이 TN의 세션키를 알지 못해야 하는 PBS (Perfect Backward Secrecy)가 제공되지 않는다. Kempf 등의 방식에서는 CGA (Cryptographically Generated Addresses)^[9] 기반의 SEND (SEcure Neighbor Discovery)^[10] 프로토콜을 사용하여 FMIPv6에서 핸드오버 인증키 교환 방법을 제

안하였다^[8]. Kempf 등의 기술에서는 MN이 핸드오버 인증 요청시 자신의 CGA 개인키로 핸드오버 인증 요청 메시지를 서명하여 AR에게 보내고, AR은 MN의 CGA 공개키로 인증 요청 메시지 서명을 검증한다. 또한, 핸드오버 인증키를 MN에게 전달하기 위하여 MN의 CGA 공개키로 핸드오버 인증키를 암호화하여 MN에게 전송한다. Kempf 등의 방식은 Wang 등의 방법보다 안전한 핸드오버 인증키 교환 방법을 제공하지만, RSA 암호 알고리즘 사용으로 자원이 한정적인 MN에게 부담이 된다. 또한, Kempf 등의 기법은 자체 생성된 인증서를 사용하기 때문에 Sybil^[11] 공격이 가능하며 이를 악용한 DoS 공격도 가능하다.

따라서 FMIPv6 이동성 기술을 제공하는 VANET 환경에서 이동 단말의 자원을 효율적으로 사용하고, 무선 환경에서 보다 안전한 핸드오버를 수행할 수 있는 핸드오버 인증 프로토콜 기술이 필요하다.

III. FMIPv6 핸드오버 인증키 교환 프로토콜

1. 프로토콜 표기법

본 논문에서 사용되는 표기법은 표 1과 같다. 또한 본 논문에서는 차량 및 차량내의 사용자 이동 단말들을 FMIPv6 환경에서 MN으로 통일하여 표기한다.

표 1. 프로토콜 표기법

Table 1. Definition.

표 기	정 의
HK_i	i 번째 AR과 MN 간 핸드오버 인증키
$H()$	안전한 일방향 해쉬함수
ID_x	x 노드의 식별자
\parallel	두 개 비트열의 연접
p	큰 소수
Z_p^*	모듈러 p 로의 곱셈군
r, x, y	Z_p^* 속하는 랜덤 값
g	Z_p^* 의 생성자

2. 안전하고 효율적인 FMIPv6 핸드오버 인증키 교환 프로토콜

가. 설계 원리 및 프로토콜 개요

본 논문에서 제안하는 non-AAA 기반의 핸드오버 인증 프로토콜은 두 가지 기본 원리가 있다. 첫 번째는 PFS (Perfect Forward Secrecy) 및 PBS와 같은 보안

기능 제공과 MN의 자원을 효율적으로 사용하기 위하여 light-weight DH 알고리즘을 적용하는 것이다. 즉, MN의 자원을 효율적으로 사용하기 위하여 본 논문에서는 MN의 DH 공개키 지수 계산을 AR에게 위임하였다. 두 번째는 MN과 PAR 사이에서 이미 형성되어 있는 SA를 이용하여 MN과 NAR 사이에서 핸드오버 인증키를 생성하는 것이다. MN과 AR 사이에서 DH 알고리즘 수행시 상호 신뢰 관계가 형성되어 있지 않기 때문에 MITM (Man-in-the-middle)과 같은 공격이 발생할 수 있다. 이 문제를 해결하기 위하여, 본 논문에서는 MN이 NAR에게 핸드오버 인증을 요청할 때 PAR이 MN을 인증하도록 하였다.

그림 2는 FMIPv6 이동성 환경에서 MN이 초기 인증부터 AR를 이동하면서 핸드오버 인증을 수행하는 전체 개요를 보여준다. 각 AR 간에는 IPSec (IP Security)이나 TLS (Transport Layer Security)와 같은 보안 프로토콜로 안전한 채널이 형성되어 있음을 가정한다. 단계 ①에서 MN은 AAA 서버와 EAP 기반의 초기 인증을 (예, EAP-TLS) 수행한다. 또한 MN은 EAP 인증 과정을 통해 생성된 마스터키로부터 HK_1 을 생성하고, AR_1 은 AAA 서버로부터 HK_1 을 받는다. MN이 AR_2 로 핸드오버하기 위해 AR_1 과 FBU 과정을 수행할 때, MN은 단계 ②와 같이 FBU 메시지를 HK_1 을 사용하여 보호한다. MN이 AR_2 로 핸드오버를 한 후 (③), MN은 AR_2 에서 AR_3 로 이동할 때 FBU 메시지를 보호하기 위한 핸드오버 인증키 HK_2 를 생성해야 한다. 단계 ④에서 MN은 인증 요청 메시지에 HK_1 로 생성한 인증값과 AR_2 와 DH 교환을 위한 DH 값을 포함하여 AR_1 에게 전송한다. AR_1 에서는 HK_1 을 사용하여 MN과 DH 공개키 생성을 위한 값을 검증하고, AR_2 와 MN이 DH 키

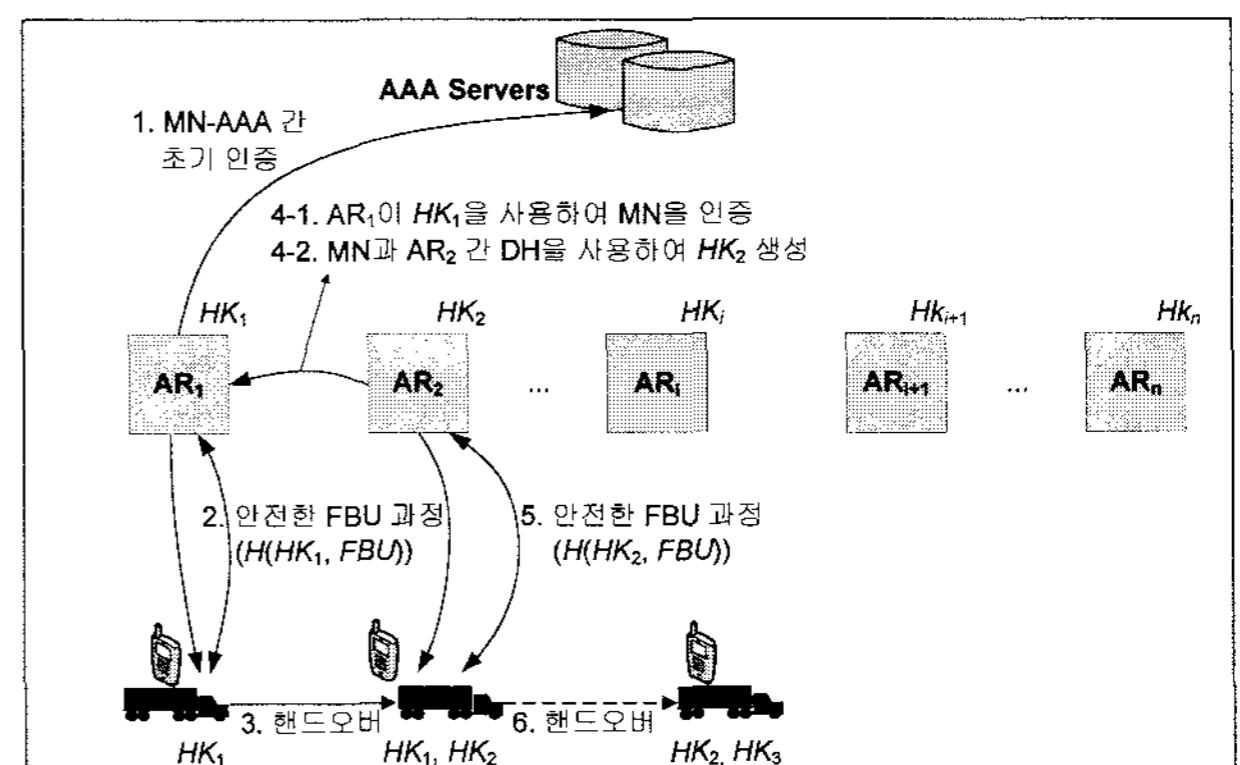


그림 2. 제안하는 핸드오버 인증 프로토콜의 개요

Fig. 2. Overview of the Proposed Handover Authentication.

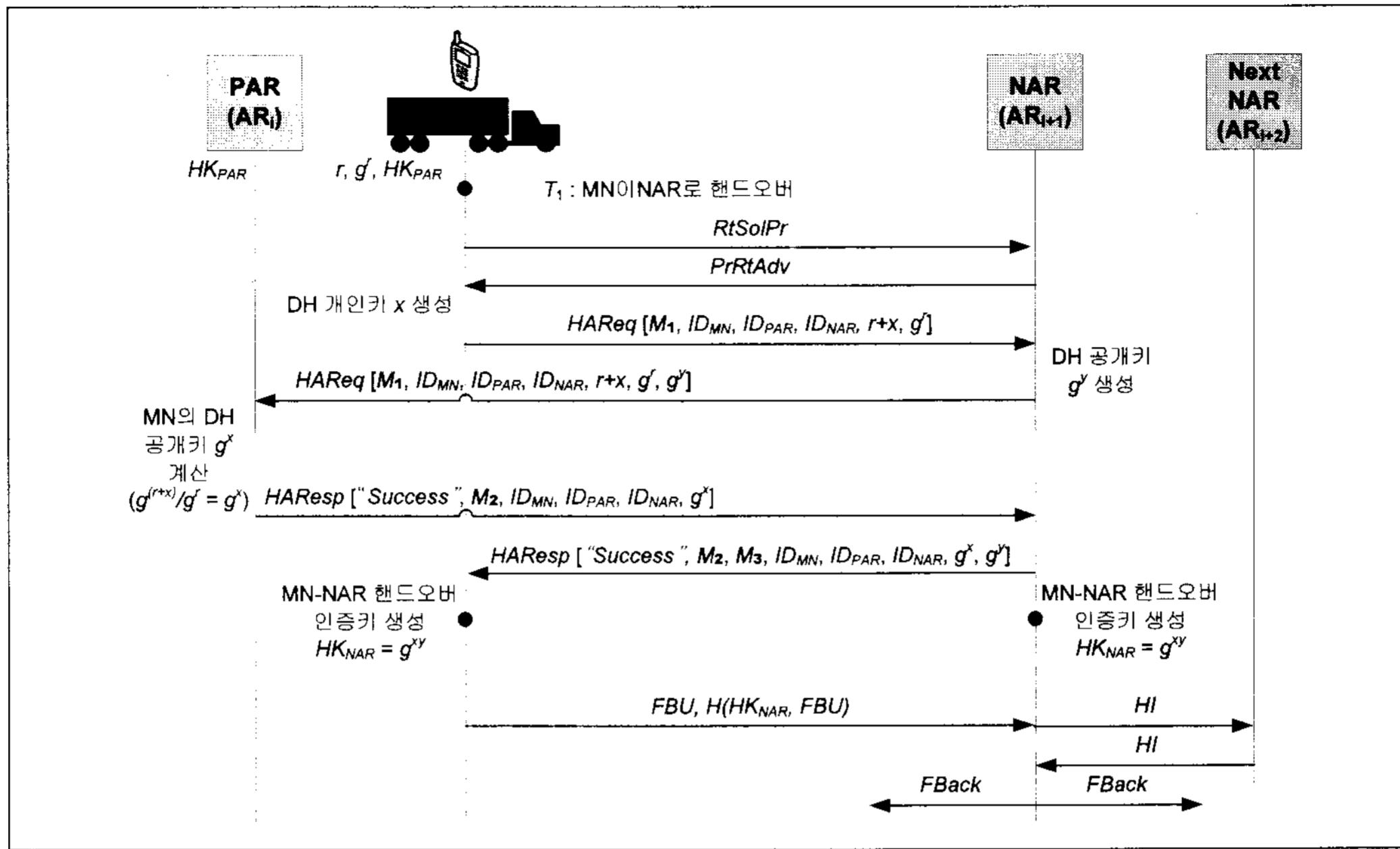


그림 3. 제안하는 핸드오버 인증 프로토콜의 메시지 흐름

Fig. 3. The Message Flow of the Proposed Handover Authentication.

교환을 통해 새로운 핸드오버 인증키 HK_2 를 생성하도록 알린다. MN은 AR_2 와 DH 키 교환을 통해 HK_2 를 생성한다. MN이 AR_2 에서 AR_3 로 이동하려고 할 때 (⑥), MN은 단계 ⑤와 같이 FBU 메시지를 HK_2 로 보호하여 안전하게 핸드오버를 수행한다. MN은 이와 같은 과정을 AR_i 로 이동할 때마다 수행한다.

나. 제안 프로토콜

그림 3은 제안하는 FMIPv6의 핸드오버 인증 프로토콜의 메시지 흐름을 보여준다. MN은 초기 인증 수행 후, 랜덤 값 r 과 $g^r \text{mod } p$ 값을 생성하고 저장한 상태이다. 두 값 r 과 $g^r \text{mod } p$ 은 MN이 핸드오버 할 때마다 재사용 된다. 또한 MN은 T₁ 시점에서 이미 NAR로 핸드오버하여 현재 NAR 도메인 영역에 있는 상태이다. MN은 다음 NAR (AR_{i+2})로 핸드오버 할 때 NAR과 안전하게 FBU 과정을 수행하기 위하여 핸드오버 인증키 HK_{NAR} 를 생성해야 한다. MN은 다음과 같은 핸드오버 인증 요청 과정을 NAR과 FMIPv6의 RtsolPr/PrRtAdv 메시지 교환 과정을 마친 후에 시작한다.

MN은 DH 개인키 x 를 생성하고 HK_{PAR} 을 사용하여 식 (1)과 같이 M_1 을 생성한다. 또한 MN은 HARreq 메시지를 생성하여 NAR에게 전송한다.

$$M_1 = H(HK_{PAR}, ID_{MN} || ID_{PAR} || ID_{NAR} || r+x || g^r \text{mod } p) \quad (1)$$

NAR은 DH 개인키 y 와 공개키 $g^y \text{mod } p$ 를 생성하고, MN으로부터 수신한 HARreq 메시지에 $g^y \text{mod } p$ 값을 포함하여 PAR에게 전송한다.

PAR은 ID_{MN} 을 확인하고, HK_{PAR} 를 사용하여 M_1 값을 확인한다. M_1 검증이 성공적으로 이루어지면, PAR은 식 (2)와 같이 MN의 DH 공개키 $g^x \text{mod } p$ 를 대신 계산한다. 마지막으로 PAR은 MN과 NAR의 DH 공개키들을 $(g^x \text{mod } p, g^y \text{mod } p)$ HK_{PAR} 을 사용하여 식 (3)과 같이 M_2 값을 생성하고, 성공 "Success" 메시지와 함께 HARresp를 NAR에게 전달한다.

$$g^x \text{mod } p = \frac{g^{(r+x)} \text{mod } p}{g^r \text{mod } p} \quad (2)$$

$$M_2 = H(HK_{PAR}, ID_{MN} || ID_{PAR} || ID_{NAR} || g^{r+x} \text{mod } p || g^x \text{mod } p || g^y \text{mod } p) \quad (3)$$

NAR이 PAR로부터 HARresp 메시지를 수신하면, NAR은 MN의 DH 공개키 $g^x \text{mod } p$ 값과 NAR의 DH 개인키 y 를 사용하여 핸드오버 인증키 HK_{NAR} ($g^{xy} \text{mod } p$)를 생성한다. NAR은 HK_{NAR} 을 사용하여 식 (4)와 같이 M_3 값을 생성하고, M_3 와 $g^y \text{mod } p$ 를 포함한 HARresp 메시지를 MN에게 전송한다.

$$M_3 = H(HK_{NAR}, M_2 || ID_{MN} || ID_{PAR} || ID_{NAR}) \quad (4)$$

MN은 $g^r \text{mod } p$ 과 $g^x \text{mod } p$ 를 사용하여 $g^{r+x} \text{mod } p$ 를 생성하고, HK_{PAR} 을 이용하여 M_2 를 검증한다. M_2 값이

성공적으로 검증이 되면, MN은 자신의 DH 개인키 x 를 사용하여 $HK_{NAR}(g^{xy} \bmod p)$ 를 생성하고, M_3 값을 검증 한다. M_3 값도 검증이 성공적으로 이루어지면, MN은 NAR과 핸드오버 인증키 HK_{NAR} 을 공유하게 된다. 이 HK_{NAR} 은 추후에 MN이 다음 NAR (AR_{i+2})로 핸드오버 할 때 MN과 NAR 사이에서 FBU 메시지를 보호하는데 사용된다.

MN은 Next NAR로 핸드오버하기 전에 HK_{NAR} 을 사용하여 FBU 과정을 안전하게 수행한다.

IV. 분석 및 비교

1. 제안 프로토콜의 안전성 분석

- DoS 공격

DoS 공격에는 네트워크 트래픽을 이용한다거나 노드에게 과다한 연산량을 수행하도록 하여 CPU 성능을 떨어뜨리는 형태가 있다. 네트워크 트래픽을 이용한 DoS 공격은 무차별적으로 대량의 메시지를 보내기 때문에 근본적으로 차단하는 것이 어렵다. 그러나 서버가 인증 요청 메시지를 수신하고 수행해야 하는 연산량을 증가시키는 DoS 공격은 서버의 연산량을 줄임으로써 DoS 공격에 대응할 수 있다. 제안 프로토콜에서 AR의 연산량을 고려해보면, PAR에서는 한 번의 지수 연산과 $(g^{r+x} \bmod p)$ 해쉬 연산을 수행하고, NAR에서는 두 번의 지수 계산을 $(g^y \bmod p, g^{xy} \bmod p)$ 수행한다. PAR의 경우 MN의 인증 요청 메시지를 MN과 공유하고 있는 HK_{PAR} 를 사용하여 해쉬 연산을 통해 쉽게 M_1 을 검증 할 수 있기 때문에, 공격자가 임의로 생성한 인증 요청 메시지에 대해서 지수 연산을 수행할 필요 없이 인증 요청을 거절할 수 있다. NAR에서는 두 번의 지수 연산을 수행하지만, NAR이 PAR로부터 MN의 인증 요청 메시지 검증 실패를 받으면 NAR은 이미 생성했던 DH 공개키 $g^y \bmod p$ 를 재사용한다. 따라서 NAR은 악의적인 메시지를 대량으로 수신할 경우, 추가적인 NAR의 DH 공개키 지수 연산을 수행하지 않기 때문에 NAR의 지수 연산에 따른 부담을 줄일 수 있다.

- 재전송 공격

제안 프로토콜은 매 핸드오버 인증 세션마다 DH 개인키 및 공개키가 바뀌기 때문에 핸드오버 인증 요청 메시지 재전송 공격으로부터 안전하다. 예를 들어, 공격자가 이전에 사용된 핸드오버 인증 요청 메시지를 재전송한다고 가정하자. 공격자가 새롭게 보낸 핸드오버 인증 요청 메시지 HAR_{req}는 정상적으로 NAR을 거쳐

PAR로 전송되고, 정상적인 핸드오버 인증 응답 메시지가 NAR을 통해 공격자에게 수신될 것이다. 그러나 이 과정에서 NAR은 새로운 DH 개인키와 공개키를 생성하여 사용했기 때문에 공격자가 정상적으로 처리된 HAR_{esp} 메시지를 수신한다 해도 HK_{NAR} 을 생성하지 못한다. 즉, 공격자는 정상적인 MN의 DH 개인키 x 를 모르기 때문에 NAR의 DH 공개키 $g^y \bmod p$ 를 수신해도 HK_{NAR} 을 생성하지 못한다. 따라서 제안 프로토콜에서는 재전송 공격이 의미가 없다.

- 메시지 위조 및 MN 위장 공격

제안 프로토콜에서 공격자는 핸드오버 인증 요청 및 응답 메시지들을 조작하여 핸드오버 인증키를 교환할 수 없다. 만약 공격자가 HAR_{req} 메시지를 임의로 조작하여 정상적인 MN인 것처럼 위장하여 인증을 요청하면, PAR이 조작된 HAR_{req} 메시지에서 M_1 을 검증할 때 실패하므로 공격자의 핸드오버 인증 요청은 거절된다. 또한, 공격자가 HAR_{esp} 메시지를 임의로 조작하여 NAR인 것처럼 위장한다고 하더라도, HAR_{esp} 메시지의 각 파라미터들은 M_2 와 M_3 에 의해서 무결성이 보장되므로 MN에서 HAR_{esp} 메시지 위조 사실을 알 수 있다.

- MITM 공격

본 논문에서는 IPSec 또는 TLS와 같은 보안 프로토콜을 사용하여 AR 간에 안전한 채널이 형성되어 있음을 가정하였다. 따라서 AR 간에 주고받는 메시지에 대해서 공격자가 MITM 공격을 수행할 수 없다. MN과 AR 사이에서는 보안 채널이 형성되어 있지 않지만, MN과 PAR 사이에 이미 형성되어 있는 SA를 사용하여 MN과 PAR이 상호 인증하고 MN과 NAR이 새로운 인증키를 교환하기 때문에 MN과 PAR 사이에 공유하고 있는 HK_{PAR} 를 모르는 공격자가 MITM 공격을 수행할 수 없다.

- PFS와 PBS

제안 프로토콜에서 PFS와 PBS는 임의의 핸드오버 키 HK_i 가 노출되었을 때, 그 키를 사용하여 이전의 핸드오버 키들 ($HK_1 \sim HK_{i-1}$) 또는 노출된 시점 이후의 핸드오버 키들을 ($HK_{i+1} \sim HK_n$) 알아낼 수 없음을 보장하는 보안 특성이다. 제안 프로토콜은 PFS와 PBS를 제공하기 위하여 DH 알고리즘을 사용하였다. 제안 프로토콜에서 HK 는 MN과 AR이 매 핸드오버 인증 세션 때마다 새로운 DH 개인키들로부터 생성한 값이기 때문에 공격자가 HK_i 를 알았다고 해도 이전 및 이후의 핸드오버 인증키를 알아낼 수 없다. 매번 새롭게 생성되

는 DH 개인키들은 DLP (Discrete Logarithm Problem) 때문에 안전하다.

- 핸드오버 인증키 HK 노출

제안 프로토콜은 MN과 AR_{i+1} 사이에서 HK_{i+1} 을 생성하기 전에, MN과 AR_i 사이에서 HK_i 를 기반으로 인증이 이루어져야 한다. 따라서 만약 HK_i 가 어떤 이유에서 노출 된다면, 공격자는 $i+1$ 핸드오버 과정부터 정상적인 MN의 모든 핸드오버 인증 권한을 획득할 수 있다. 그러나 HK_i 의 노출은 AAA 기반의 핸드오버 인증 방법 및 기존의 non-AAA 기반의 인증 방법에서 핸드오버 인증 마스터키가 노출되는 것과 같은 수준의 공격이기 때문에 제안 프로토콜만의 취약성이라고 보기 어렵다. 또한, 이러한 공격은 MN이 주기적으로 초기 인증 과정을 재 수행함으로써 공격자의 핸드오버 인증 권한 사용을 제한 할 수 있다.

- Ping-Pong 문제

MN이 PAR과 NAR 사이를 자주 빠르게 이동하는 것을 ping-pong 현상이라고 한다. Ping-pong 상황에서 MN과 AR은 이동할 때마다 핸드오버 인증키를 재생성해야 하는 문제로 핸드오버 과정을 지연시킬 수 있다. 이러한 문제는 MN과 AR에서 핸드오버 인증키를 일정 시간 동안 캐쉬하는 방식을 통하여 쉽게 해결할 수 있다. 제안 프로토콜은 ping-pong 현상이 나타날 때 핸드오버 인증키 캐쉬 방법을 통하여 핸드오버 지연 없이 기존의 핸드오버 인증키로 안전하고 신속하게 FBU 과정을 수행할 수 있다.

- 이동 단말의 DH 지수 연산량을 줄이기 위해 수정된 DH 기법 (light-weight DH)

본 논문에서는 MN의 DH 공개키인 $g^x \text{mod } p$ 지수 연산을 PAR에게 위임하기 위하여, MN이 $r+x$, $g^r \text{mod } p$ 값들을 PAR에게 전송하는 방식을 사용하였다. PAR에서는 식 (2)를 통해 MN 대신 $g^x \text{mod } p$ 값을 생성하고, 생성된 $g^x \text{mod } p$ 값의 무결성을 보장하기 위하여 M_2 메시지에 HK_{PAR} 과 함께 MAC 값을 생성하고 MN에게 전송한다. 제안 프로토콜에서 공격자는 공개된 값 $r+x$, $g^{r+x} \text{mod } p$, $g^r \text{mod } p$, $g^x \text{mod } p$, $g^y \text{mod } p$ 값을 이용하여 r , x 또는 y 의 값을 계산할 수 없다. 즉, 공격자는 $\{r+x_i, g^r \text{mod } p, g^{x_i} \text{mod } p, g^{y_i} \text{mod } p\}$ 로 이루어진 여러 세트의 값을 수집하였다하더라도, r 또는 x_i 값을 얻지 못한다. 예를 들어, 공격자가 수집한 값을 사용하여 r 또는 x_i 값을 구한다고 할 때 수집한 $\{r+x_0, r+x_1, r+x_1, \dots, r+x_i\}$ 값을 사용하여 구해야

한다. 그러나 공격자는 $i+1$ 개의 식과 $i+2$ 개의 변수를 갖는 부정 방정식을 풀 수 없기 때문에 r 또는 x_i 값을 구할 수 없다. 또한, 수집된 $\{g^r \text{mod } p, g^{x_i} \text{mod } p, g^{y_i} \text{mod } p\}$ 값을 부터는 DLP를 풀 수 없기 때문에 r 또는 x_i 에 대해 안전성이 보장된다.

2. 성능 분석

DH 기반의 핸드오버 인증키 교환 프로토콜들은 지수 연산 때문에 자원 (전원) 활용이 제한적인 이동 단말들에게 적용될 때 지수 연산량을 고려해야 한다. 본 논문에서는 DH 클라이언트 측인 MN에서 기본적으로 수행해야 하는 2번의 DH 지수 계산을 (DH 공개키 $g^x \text{mod } p$ 계산과 DH 세션키 $g^{xy} \text{mod } p$) 1번 수행으로 줄였다. MN은 초기 부팅 인증 후에 r 과 $g^r \text{mod } p$ 값을 일정 시간 동안 저장한다. MN이 핸드오버 인증을 수행할 때, $r+x$, $g^r \text{mod } p$ 값을 NAR을 거쳐 PAR에게 전송한다. 이 두 값을 받은 PAR은 식 (2) 과정을 통해 MN 대신 $g^x \text{mod } p$ 값을 생성한다. 즉, MN의 $g^x \text{mod } p$ 계산을 PAR에게 위임하였기 때문에 MN은 NAR의 DH 공개키 $g^y \text{mod } p$ 를 수신한 후, $g^{xy} \text{mod } p$ 지수 연산 1회만을 수행한다. 비록 MN이 $g^r \text{mod } p$ 값을 생성해야 하는 부담이 있지만, $g^r \text{mod } p$ 값은 이동 단말 내에서 일정 시간동안 안전하게 저장되고 핸드오버 인증이 이루어질 때마다 재사용되는 값이므로 $g^r \text{mod } p$ 지수 연산량은 MN에게 큰 부담이 되지 않는다.

제안하는 핸드오버 인증 프로토콜은 HAReq 메시지와 HAResp 메시지를 추가적으로 정의하였기 때문에 FMIPv6 표준 절차에서 요구하는 통신 이외에 추가적으로 메시지 교환이 MN-NAR-PAR 간에 이루어져야 한다. 이는 빠르게 이동하는 이동 단말 및 차량 사이에서 추가적인 IP 통신으로 빠른 핸드오버 인증 지연에 장애가 될 수 있다. 그러나 제안 프로토콜에서 HAReq 메시지와 HAResp 메시지 교환은 지역적으로 가깝게 위치한 노드들 간에 통신이기 때문에 FMIPv6 핸드오버 지연에 크게 영향을 미치지 않는다. 일반적으로 VANET 환경에서 네트워크 계층인 AR에는 여러 RSU 링크 계층의 노드가 연결되어 있기 때문에 실제 차량이 하나의 AR 영역을 지나가는 동안에 HAReq와 HAResp 메시지를 교환하는 시간은 충분하다.

제안 프로토콜에서 AR은 $g^x \text{mod } p$ 지수 연산을 추가적으로 수행해야 하지만, 일반적으로 AR은 충분한 전력이 공급되는 네트워크 노드이기 때문에 큰 부담이 되

표 2. 제안 프로토콜과 기존의 핸드오버 인증 프로토콜들 비교

Table 2. Comparison on handover authentication protocols.

	Wang의 인증 프로토콜 ^[7]	Kempf의 인증 프로토콜 ^[8]	제안 프로토콜
보안 요구사항	SN과 TN 사이에서 보안 채널	SEND 구조 (Self-signed Certificate 생성 구조)	AR들 사이에서 보안 채널
PFS 및 PBS 제공 여부	PFS 제공 PBS 미제공	PFS 및 PBS 제공	PFS 및 PBS 제공
보안 위협	-	Sybil 및 DoS 공격	-
암호화 연산	XOR 연산 해쉬 함수	RSA 암·복호화 및 서명·검증 해쉬 함수	Diffie-Hellman 해쉬 함수
MN에서 수행하는 지수 연산량	0	2	1
AR에서 수행하는 지수 연산량	0	2	NAR : 2 (MN의 인증 요청 메시지 검증 성공) PAR : 1
핸드오버 인증을 위해 추가적으로 요구되는 메시지 교환	0	0	2 라운드

지 않는다. 또한 제안 프로토콜은 non-AAA 방식이기 때문에 기존의 non-AAA 방식과 같이 다음과 같은 특성을 동일하게 갖는다. 제안 방식은 AAA 서버에서 관리하는 핸드오버 인증키를 AR에서 관리해야 하는 부담이 있다. 하지만 non-AAA 방식에서 AR의 핸드오버 인증키 관리 부담은 AAA 서버 방식에서 고려해야하는 AAA 네트워크에서의 인증 트래픽 및 핸드오버 인증키 관리 집중화 문제를 분산 시킬 수 있다. 또한 AAA 방식은 AAA 인증 서버가 중지되었을 때 이동 중인 MN에 대해서 핸드오버 인증 서비스를 제공할 수 없지만, non-AAA 방식은 지속적으로 핸드오버 인증 서비스를 제공할 수 있다. 예를 들어, AAA 서버가 어떤 이유에서든 중지 되었을 경우, 초기 인증을 시도하려는 MN 및 이동 중인 MN에 대해서 어떠한 인증 서비스도 제공할 수 없지만, non-AAA 방식에서는 이동 중인 MN에 대해서는 지속적으로 핸드오버 인증 서비스를 제공할 수 있다.

3. 기존 프로토콜과 비교 분석

제안하는 FMIPv6 핸드오버 인증키 교환 프로토콜은 기존 방법보다 안전하고 효율적이다. 표 2는 기존의 핸드오버 인증 프로토콜과 제안 프로토콜을 비교 분석한 것이다. 비교 분석 대상에서 AAA 방식의 핸드오버 인증 기법은 제외하고 non-AAA 기반의 인증 프로토콜만을 비교하였다.

Wang 등의 기법은 핸드오버 인증 과정에서 XOR와 해쉬 함수만을 사용하기 때문에 이동 단말에 적합하다. 그러나 PBS를 제공하지 않는 단점이 있다. CGA 기반

의 SEND 방식을 사용하는 Kempf 등의 기법은 공개키 알고리즘을 사용하여 기존의 non-AAA 방식에서 가장 큰 보안 문제가 되었던 PBS를 제공하는 장점이 있다. 그러나 Kempf 등의 방식은 CGA를 사용하기 때문에 Sybil 공격 (아이디 위조 공격)이 가능하다. Sybil 공격은 공격자가 CGA 기반의 임의의 주소를 생성하여 AR로 하여금 여러 개의 MN이 주변에 있다고 생각하도록 하는 공격이다. 공격자는 이 Sybil 공격을 악용하여 AR에게 CPU 성능을 소모하는 DoS 공격이 가능하다. 예를 들어, 공격자가 Sybil 공격을 통해 임의의 MN들을 생성하고 각각의 인증 요청 메시지를 대량으로 AR에게 전송하면, AR에서는 각 인증 요청 메시지에 대해서 CGA 주소 검증을 위하여 RSA 서명 검증 연산과 핸드오버 인증키를 전달하기 위하여 RSA 암호화 과정을 수행해야 한다. 즉, 2 번의 지수 연산을 수행해야 한다. 그러나 제안 프로토콜에서는 공격자의 임의의 인증 요청 메시지에 대해서 PAR이 해쉬 연산을 통해 M_1 메시지를 검증한 후, 실패하면 인증 과정을 중단하기 때문에 Kempf 등의 기법보다 CPU 성능 소모가 적다. 또한 NAR에서는 PAR로부터 인증 요청 메시지 검증에 대해 실패 메시지를 수신하면, NAR의 DH 공개키 $g^y \text{mod} p$ 값을 재사용하기 때문에 NAR에서도 지수 계산에 따른 CPU 성능 저하 문제를 해결할 수 있다.

제안 기법은 기존 기법보다 계산량이 적기 때문에 차량 내에서 자원이 한정적인 이동 단말에 적합하다. Kempf 기법은 단말에서 RSA 서명과 복호화 과정을 수행해야 하지만, 제안 프로토콜은 MN의 DH 공개키 지수 계산을 PAR에게 위임시켰기 때문에 핸드오버 인

증키 생성을 위한 지수 계산 1회만을 수행하면 된다.

Wang의 인증 프로토콜은 FMIPv6 환경에서 제안된 것이 아니지만, 인증 절차를 고려해 볼 때 FMIPv6 표준 동작을 위한 메시지에 임베디드하여 핸드오버 인증을 수행할 수 있다. Kempf의 방법에서는 기본적으로 SEND 기반이기 때문에 ND (Neighbor Discovery) 과정에 핸드오버 인증키 교환 과정이 포함되어 있다. 제안 프로토콜은 기존 두 프로토콜과 달리 FMIPv6 표준 동작에서 요구하는 메시지 교환 이외에 HAReq와 HAResp 메시지를 교환해야 하지만, 앞 절에서 논의했듯이 하나의 AR 영역을 지나가는 동안에 두 메시지 교환을 위한 충분한 시간이 있기 때문에 빠른 핸드오버 절차에 큰 영향을 미치지 않는다.

V. 결 론

본 논문에서는 네트워크 계층의 고속 이동성을 제공하는 VANET 환경에서 안전하고 효율적인 핸드오버 인증 기법을 제안하였다. 사용자들의 멀티미디어 서비스에 대한 사용 욕구가 증가하면서 VANET 환경에서도 이동 중인 차량내의 장치 또는 사용자의 휴대 이동 단말들을 이용해 V2I 네트워크 통신으로 끊김 없는 서비스 제공이 가능해졌다. 그러나 이러한 이동성 환경에서 FMIPv6 핸드오버 기술에 대한 보안이 제공되지 않으면 IP 패킷의 경로 재설정 및 DoS 공격이 발생할 수 있다. 본 논문에서 제안한 프로토콜은 기존 기법보다 향상된 보안 기능을 제공하고 DoS 공격으로부터 안전하다. 또한, 제안 기법은 DH 공개키 지수 계산 위임 방식을 사용하여 기존의 인증 프로토콜보다 이동 단말에 적합하다.

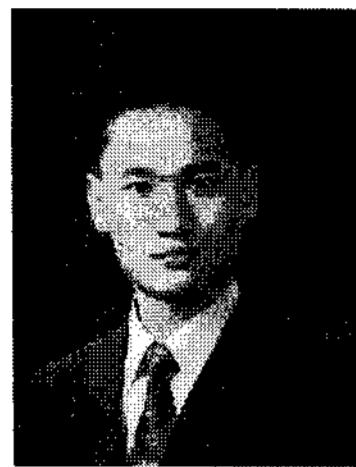
참 고 문 헌

- [1] J. David, P. Charles, and J. Arkko, Mobility Support in IPv6, IETF RFC 3775, June 2004.
- [2] R. Koodli, Mobile IPv6 Fast Handovers, IETF draft-ietf-mipshop-fmipv6-rfc4068bis-07, April 2008.
- [3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, Vol. 22 (6), pp. 644-654, November 1976.
- [4] Q. Mussabir, W. Yao, Z. Niu, and X. Fu, "Optimized FMIPv6 using IEEE 802.21 MIIH Services in Vehicular Networks," *IEEE Trans. Veh. Technol.*, Vol. 56 (6), pp. 3397-3407,

November 2007.

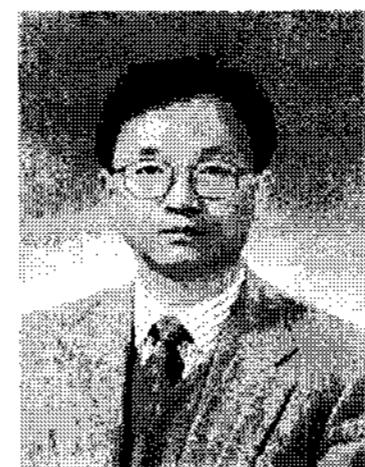
- [5] V. Narayanan, N. Venkitaraman, H. Tschofenig, G. Giaretta, and J. Bournelle, Establishing Handover Keys using Shared Keys, IETF draft-vidya-mipshop-handover-keys-aaa-04, March 2007.
- [6] 최재덕, 정수환, "이기종 FMIPv6 기반의 이동 망에서 이동 노드 주도형 핸드오버 인증 기법", 정보보호학회논문지, 제17권, 제2호, 104-114쪽, 2007년 4월
- [7] H. Wang and A.R. Prasad, "Fast Authentication for Inter-domain Handover," ICT 2004, LNCS 3124, pp. 973-982, August 2004.
- [8] J. Kempf and R. Koodli, Distributing a Symmetric FMIPv6 Handover Key using SEND, IETF draft-ietf-mipshop-handover-key-03, November 2007.
- [9] T. Aura, Cryptographically Generated Addresses (CGA), IETF RFC 3972, March 2005.
- [10] J. Arkko, J. Kempf, B. Zill, and P. Nikander, SECure Neighbor Discovery (SEND), IETF RFC 3971, March 2005.
- [11] J. R. Douceur, "The Sybil Attack," IPTPS 2002, LNCS 2429, pp. 251-260, March 2002.

저 자 소 개



최재덕(정회원)
 2002년 중실대학교
 정보통신전자공학부 학사.
 2004년 중실대학교
 정보통신공학과 석사.
 2005년~현재 중실대학교 전자
 공학과 박사과정 재학중.

<주관심분야 : 차량 네트워크 보안, VoIP 보안,
 이동 인터넷 보안>



정수환(평생회원)-교신저자
 1985년 서울대학교
 전자공학과 학사.
 1987년 서울대학교
 전자공학과 석사.
 1996년 University of
 Washington 박사.

1996년~1997년 Stellar One SW Engineer
 1997년~현재 중실대학교 정보통신전자공학부
 부교수

<주관심분야 : 차량 네트워크 보안, VoIP 보안,
 이동 인터넷 보안, RFID/USN 보안>