情報保護學會論文誌
第18卷 第3號, 2008. 6

MANEMO 환경에서 임시 인증서를 이용한 이동 라우터 간 상호인증 기법*

노 효 선†, 정 수 환‡
숭실대학교 정보통신전자공학부

Mutual Authentication Scheme of Mobile Routers Using Temporary Certificate in MANEMO*

Hyosun Roh†, Souhwan Jung‡
School of Electronic Engineering, Soongsil University

요 약

본 논문은 MANEMO 환경에서 액세스 라우터의 임시 인증서를 이용한 이동 라우터 간의 상호인증 기법을 제안한다. 기존 NEMO에서는 AAA 서버를 사용하여 이동 라우터를 인증하기 때문에 중첩된 이동 네트워크 레벨이 증가할수록 인증 시간과 인증 메시지의 오버헤드가 증가하는 문제가 있다. 본 논문에서 제안된 방법은 액세스 라우터가 자신의 개인키로 서명한 임시 인증서를 이동 라우터에게 발급하여 중첩된 이동 네트워크에 속한 이동 라우터 간에 AAA 서버를 사용하지 않고 상호인증 하는 방법으로 AAA 서버를 사용하는 방법보다 인증시간이 적게 들고 인증 메시지의 오버헤드를 줄일 수 있다.

ABSTRACT

This paper proposes a mutual authentication scheme for mobile router in MANEMO. The NEMO used AAA server in order to authenticate mobile router in nested mobile network. So, this scheme has some problem that increases authentication message overhead and authentication time. The proposed scheme uses temporary certificate that signed by an access router's private key. The temporary certificate authenticates a mobile router when the mobile router entered a MANET domain. The proposed scheme reduces authentication message overhead and authentication time than the scheme to use AAA server when authenticating the mobile router.

Keywords : *Mutual Authentication, Temporary Certificate, MANEMO, NEMO, MANET*

접수일 : 2007년 9월 4일; 수정일 : 1차-2007년 12월 2일, 2차-2008년 1월 17일; 채택일 : 2008년 3월 6일
* 본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업 및 숭실대 교내 연구 지원에 의해 수행되었음.
† 주저자, peterhyo@cns.ssu.ac.kr
‡ 교신저자, souhwanj@ssu.ac.kr

Ⅰ. 서 론

인터넷에 대한 무선접속 기술의 급속한 발전으로 인터넷 프로토콜의 이동성 지원이 중요한 문제로 부각되었으며, 이 문제를 해결하기 위한 연구가 활발히 진행되고 있다. 특히 IETF (Internet Engineering Task Force)의 NEMO (Network Mobility) 워킹 그룹에서는 네트워크

이동성 지원을 위한 NEMO 프로토콜을 제안하여 표준화를 진행하고 있다. 최근에는 NEMO BS (Network Mobility Basic Support) 프로토콜[1]을 표준화 하였으며 NEMO를 이용하여 기존의 Mobile IP[2,3]를 확장하기 위한 논의를 계속해서 진행하고 있다. NEMO는 이동 네트워크가 외부 네트워크로 이동할 경우 MR (Mobile Router)의 서브넷에 존재하는 MNN (Mobile Network Node)가 수행해야하는 핸드오버를 이동 라우터가 대신 수행하여 인터넷에 대한 연결을 계속해서 유지해 주며 네트워크의 자원을 효율적으로 사용할 수 있게 관리한다. 그러나 NEMO의 중첩된 이동 네트워크의 레벨이 증가할 경우 패킷 전달을 위한 루트가 복잡해지고 오버헤드가 증가하는 문제가 있다. 이러한 문제를 해결하여 루트 최적화를 제공해주기 위해 최근 MANET (Mobile Ad hoc Network)과 NEMO를 결합한 MANEMO[4]환경이 제안되었다. MANEMO (MANET-NEMO)는 MANET 라우팅 프로토콜을 사용하여 중첩된 이동 네트워크에 속한 이동 라우터들 간 최적화된 루트를 결정할 수 있게 하였다. 그러나 제안된 MANEMO의 경우 메시지 무결성, 사용자 인증, 메시지 비밀성 등의 보안을 제공하지 않기 때문에 악의 적인 공격자가 쉽게 정상적인 사용자로 가장하여 공격하기 쉽다. 따라서 MANEMO의 MANET 도메인에 속한 이동 라우터들을 인증하기 위한 인증구조와 이동 라우터 간의 안전한 메시지 전달 기법이 필요하다.

기존 NEMO의 경우 AAA (Authentication, Authorization, and Accounting) 서버를 이용하여 이동 라우터들과 이동 라우터의 서브넷에 존재하는 단말들을 인증하고, 인증을 위해 전달되는 제어 메시지와 패킷의 암호화를 제공하였다[6]. 그러나 이 방법은 중첩된 이동 네트워크 레벨이 증가할 경우 통신을 원하는 이동 라우터 내에 속한 이동 단말들의 전체 인증시간, 인증 메시지의 수 그리고 패킷 오버헤드가 증가하는 단점이 있다. 이러한 AAA 서버 기반의 인증 기법[7]을 MANEMO 환경에 적용할 경우에도 NEMO에서와 동일한 문제가 발생한다. 또한 MANEMO의 MANET 도메인 내에서 이동 라우터들이 구성하는 네트워크 토폴로지는 매우 빈번하게 변할 수 있다. 이러한 상황에서 이동 라우터들 간에 상호인증을 제공할 수 있어야 한다. 때문에 AAA 서버 기반의 인증 기법과 비교하여 인증 과정에서 필요한 인증 메시지의 수와 오버헤드를 줄일 수 있는 효과적인 인증 구조가 필요하다.

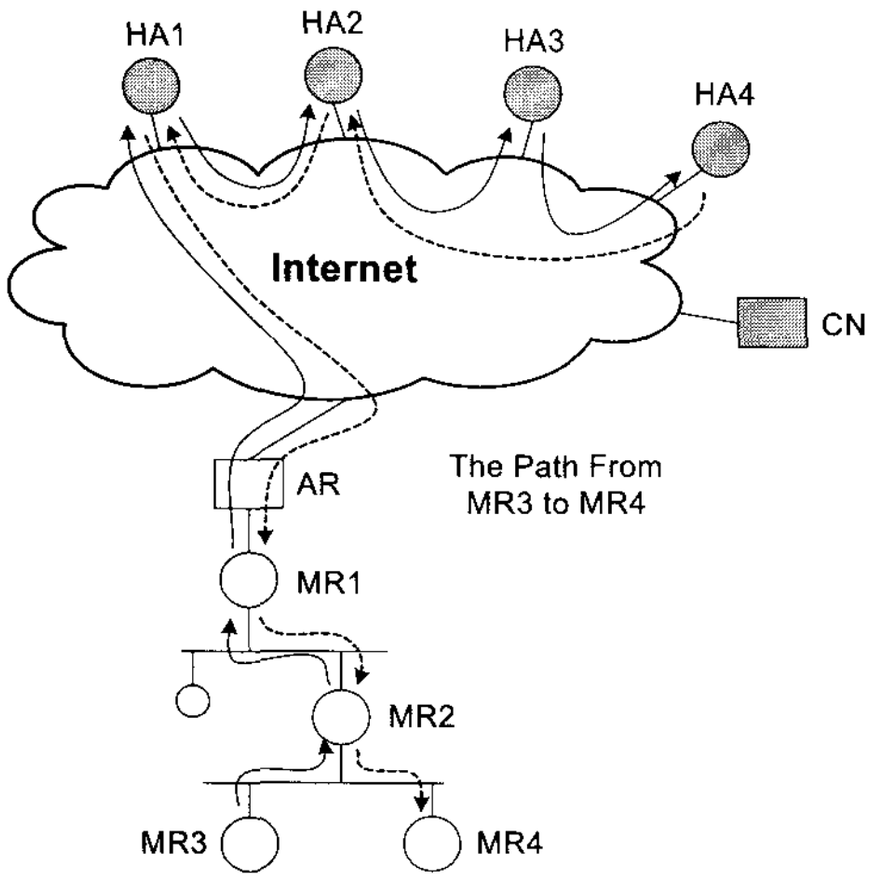
이동 라우터를 인증하는 방법으로 기존 PKI 기반의 인증 기법[8]이 존재한다. 공인 인증기관으로부터 발급받은 공인 인증서를 사용하여 효율적이고 안전하게 이동 라우터를 인증할 수 있다. 그러나 PKI 기반의 인증 기술의 경우 MANEMO 환경에 존재할 수 있는 다양한 이동 라우터 또는 액세스 라우터들이 서로 다른 공인 인증기관으로부터 발급받은 공인 인증서를 사용할 경우 이동 라우터의 인증 과정에서 인증서 체인[9]을 형성해야 한다. 이때 생성된 인증서 체인은 이동 라우터가 상호인증을 수행하는 과정에서 인증서의 길이가 길어져 인증서를 처리하는 시간이 증가되며 인증서가 길어짐에 따른 오버헤드가 발생한다. 또한 서로 다른 인증기관의 공인 인증서를 사용하는 이동 라우터 또는 액세스 라우터의 공개키를 디렉토리 서버에서 받아 와야 하기 때문에 인증 메시지의 수가 증가한다. 위와 같은 문제를 해결하기 위해 본 논문에서는 MANET 도메인에 속한 이동 라우터들 간의 상호인증에 액세스 라우터에서 발행하는 임시 인증서를 사용하여 AAA 서버를 사용할 때보다 상호인증시간과 오버헤드를 줄일 수 있는 기법을 제안한다. 또한 기존 PKI 방법에서 문제가 되는 인증서 체인의 길이를 줄여 이동 라우터 간 상호인증하는 과정에서 인증서 체인에 의해 발생할 수 있는 있는 오버헤드와 인증서 처리 시간을 최소화 할 수 있는 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 MANEMO와 관련된 네트워크 기술과 기존 인증기술의 문제점을 살펴보고, 3장에서 본 논문에서 제안하는 인증 기법에 대해 설명한다. 4장에서는 기존 인증 기법과 제안하는 기법을 비교 분석해 보고, 마지막 5장에서 본 논문의 결론을 맺는다.

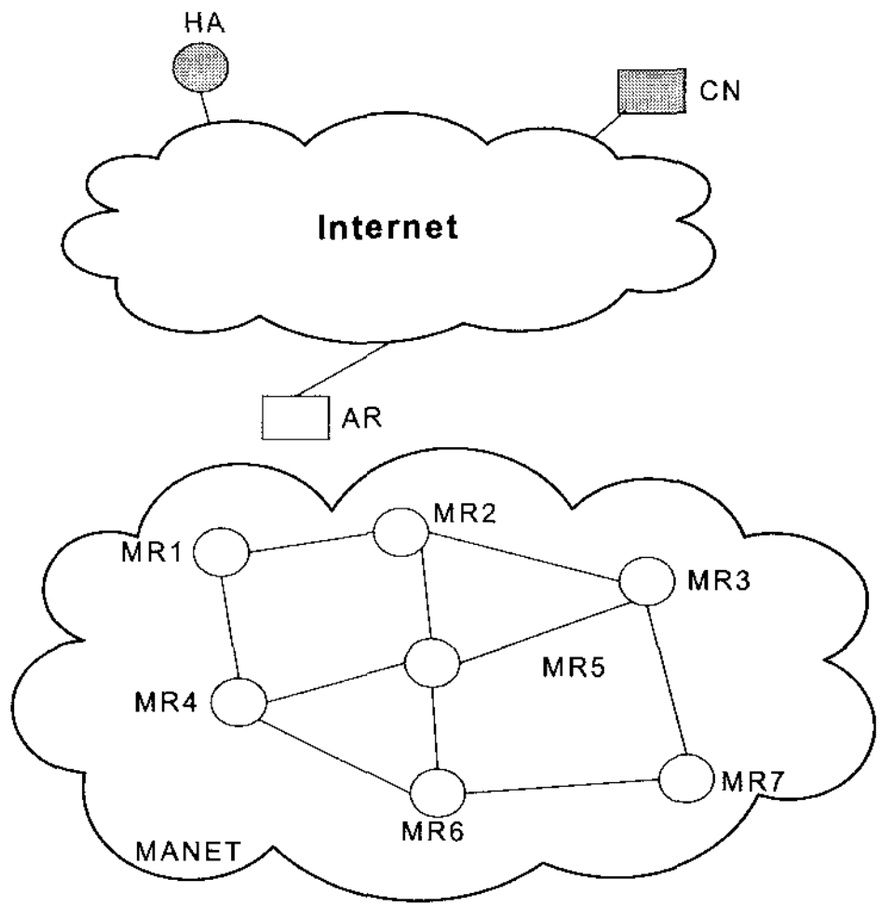
Ⅱ. MANEMO 관련 연구 및 인증기술 문제점

2.1 MANEMO (MANET-NEMO) 관련 네트워크 기술

NEMO는 이동 네트워크가 이동할 때 이동 라우터를 통해 이동성을 지원하며 이동 라우터 내부의 서브넷에 존재하는 다양한 이동 단말과 고정된 단말에 지속적인 인터넷 연결을 제공한다. 또한 다른 이동 네트워크에 투명한 연결성을 지원하는데 목적이 있다. 이러한 목적을 가진 NEMO는 열차, 비행기 또는 자동차 등의 운송수단에 적용될 수 있으며 그 내부에 PAN (Personal Area Network)[10,11] 또는 NEMO 등의 다른 네트워크가



〔그림 1〕 중첩된 네트워크에서 경로 설정



〔그림 2〕 MANEMO 구조

중첩될 수 있다. 이동 네트워크가 중첩되었을 때 중첩된 네트워크에 포함된 이동 네트워크들의 이동성 관리를 지원하기 위해 IETF NEMO 워킹 그룹에서는 NEMO BS 프로토콜을 새롭게 제안하였다. 제안된 NEMO BS에서는 네트워크의 이동성을 관리하기 위해 Explicit Mode와 Implicit Mode 두 가지 모드를 지원한다[1]. 그러나 NEMO BS의 경우 중첩된 이동 네트워크의 레벨이 증가할 경우 데이터를 전달하기 위한 과정에서 [그림 1]과 같은 핀볼 라우팅 문제[12]가 발생하고 이로 인해 패킷 터널링 과정에서 패킷 오버헤드가 증가하는 문제가 발생한다.

위에서 설명한 NEMO의 중첩된 네트워크에서의 루트 최적화 문제를 해결하여 데이터 전달과정에서 발생하는 오버헤드와 전달 지연시간을 줄이기 위해 MANEMO[4]가 제안되었다. [그림 2]는 MANEMO의 구조를 보여준다. [그림 2]와 같이 MANEMO는 NEMO의 중첩된 네트워크에 속한 이동 라우터들 간에 통신을 원할 경우 MANET 라우팅 프로토콜을 이용하여 이동 라우터들 간에 직접적인 통신을 할 수 있게 하였다. 때문에 NEMO에서 통신을 위해 생성했던 홈 에이전트와의 터널이 필요 없으며, 터널로 인해 증가했던 패킷 오버헤드를 줄였다. 또한 중첩된 네트워크의 상위 이동 라우터의 홈 에이전트를 거치지 않고, MANET 라우팅 프로토콜을 이용하여 소스와 목적지 노드가 직접 통신을 진행하기 때문에 패킷 전달지연시간을 줄일 수 있다. 그러나 이러한 MANEMO의 경우도 MANET 도메인에 속하지 않은 이동 라우터 또는 다른 MANET 도메인에 속한 이동 라우터와의 통신을 위해서는 NEMO BS 프로토콜을 그대로 적용하기 때문에 패킷 오버헤드와 패킷 전달 과정에서 지연 시간이 생길 수 있다.

2.2 제안된 기존 인증기술들의 문제점

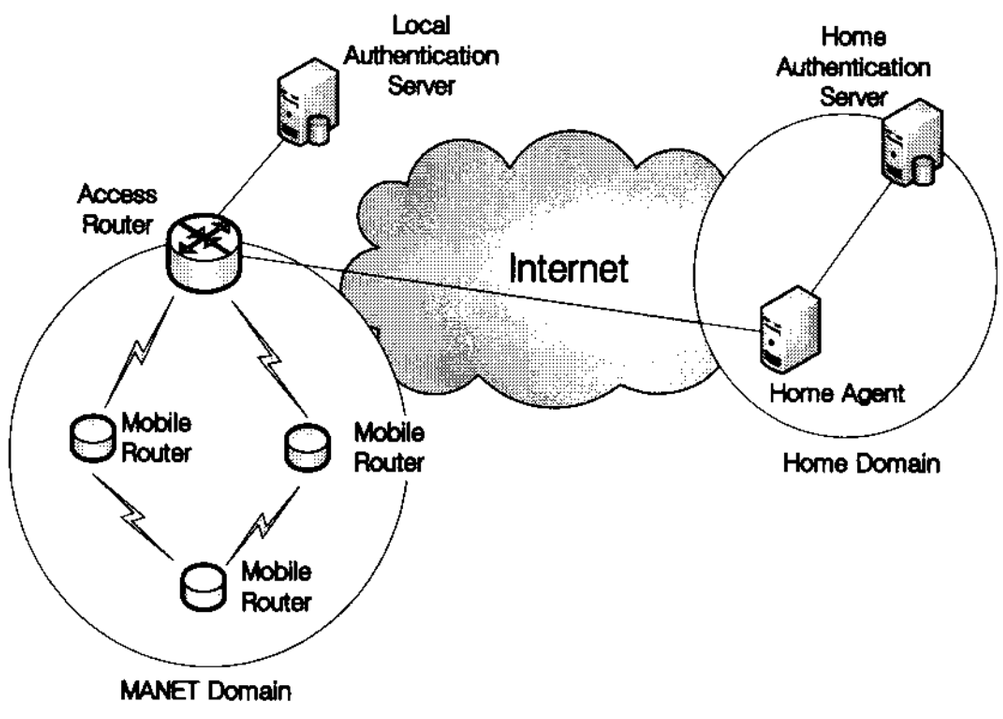
기존 NEMO에서는 이동 라우터 또는 이동 단말 간에 제어 메시지의 안전한 전달을 위해 AAA 인증서버를 이용한 인증기술[6]이 제안되었다. 이동 라우터는 새로운 네트워크 도메인으로 진입하면 액세스 라우터에게 네트워크 접속을 위한 인증 요청 메시지를 전송한다. 이때 이동 라우터는 자신의 홈 에이전트와 사전에 공유하고 있는 비밀키를 이용하여 인증 요청 메시지를 암호화하여 액세스 라우터에게 전달하고, 액세스 라우터는 이동 라우터의 홈 에이전트에게 인증 요청 메시지를 전달한다. 이후 이동 라우터의 AAAH 서버와 액세스 라우터의 AAAL 서버를 통해 이동 라우터를 인증 한다. AAA 서버를 통해 인증된 이동 라우터의 인증 정보는 액세스 라우터가 이동 라우터를 인증할 수 있도록 하기위해 다시 액세스 라우터에게 전달되고, 액세스 라우터는 이동 라우터에 대한 인증을 확인한 후 이동 라우터의 네트워크 접근을 허가한다. 위에서 설명한 것처럼 NEMO에서 제안된 AAA 인증서버를 이용한 인증 기법의 경우 중첩된 네트워크 레벨이 증가할 경우 이동 라우터 간 상호인증하는 과정에서 다량의 패킷 오버헤드, 인증 메시지 수의 증가, 그리고 지연시간이 발생한다.

앞서 AAA 서버를 이용하는 방법 이외에 또 다른 방

법으로 PKI 기반의 상호인증 기법을 사용한다. PKI 기반의 인증기술은 공인 인증서를 사용하여 이동 라우터들 간에 상호인증을 제공한다. PKI 기반 인증기술에서 공인된 인증기관을 통해 발급받은 인증서를 사용할 경우 인증기관에 접속하게 되는 모든 사용자는 공개키를 습득할 수 있으며 인증서를 발급한 인증기관 이외의 누구도 임의로 인증서의 내용을 수정할 수 없는 이점이 있다. 그러나 공개키를 얻기 위해 필요한 인증서 체인 [9] 사용에 따른 오버헤드, 저장 메모리 크기 그리고 연산 부담이 증가하는 문제점이 있으며, 사전에 공개키를 습득하지 못했을 경우 디렉토리 서버를 통해 필요한 공개키를 알아오기 때문에 인증서 습득을 위한 추가적인 메시지가 필요하다.

Ⅲ. MANEMO 환경에서 이동라우터 간의 상호인증 기법

이번 장에서는 앞서 설명한 AAA 서버를 이용한 인증 기법과 PKI 기반의 인증 기법에서 이동 라우터를 인증할 때 발생하는 오버헤드와 지연시간을 줄이며, MANEMO 환경의 MANET 도메인에 최적화된 이동 라우터 간 상호인증을 위해 본 논문에서 제안하는 임시 인증서를 이용한 상호인증 기법에 대해서 자세하게 설명한다. [그림 3]은 본 논문에서 제안하는 이동 라우터의 임시 인증서 발급을 위한 네트워크 구성요소와 MANEMO의 MANET 도메인을 보여준다. 본 논문에서 제안하는 기법은 크게 세 가지 단계로 설명한다. 이동 라우터가 초기부팅 되었을 때 EAP-TLS 초기인증을 통해 홈 인증서버 (HAS : Home Authentication Server)



〔그림 3〕 Mobile Router의 임시 인증서 발급을 위한 네트워크 구조

에게 초기 인증을 받는 과정, 초기 인증이 끝난 이동 라우터가 MANET 도메인으로 이동하여 액세스 라우터 (AR : Access Router)로부터 임시 인증서를 발급 받는 과정, 그리고 마지막으로 MANET 도메인에 속한 다른 이동 라우터와 임시 인증서를 이용한 상호인증 과정으로 나누어 설명한다. 제안하는 기법을 설명하기 전에 본 논문에서는 기본적으로 다음과 같은 사항을 가정한다. 제안하는 기법은 MANEMO 환경에서 액세스 라우터와 인증서버 간에는 TLS 또는 IPSec 보안 프로토콜을 사용하여 안전한 채널이 형성되어 있음과, 이동 라우터 초기 인증은 EAP-TLS를 사용한다고 가정한다. 또한 MANEMO의 MANET 도메인에 속한 이동 라우터 간에는 OLSR (Optimized Link State Routing) 라우팅 프로토콜을 사용하며, 액세스 라우터는 임시 인증서 발급 과정에서 사용하는 자신의 개인키와 공개키를 RSA를 이용하여 생성한다. 그리고 이동 라우터 간에 상호인증 과정이 끝난 후 안전한 통신을 위해 사용되는 세션키 교환은 Diffie-Hellman을 이용한다고 가정한다.

3.1 이동 라우터 초기 인증 과정

MANEMO 환경에서 이동 라우터가 초기 부팅을 시작하면 자신의 홈 인증서버와 EAP-TLS를 통해 초기 인증 과정을 시작한다. 이동 라우터는 미리 홈 인증서버에 등록한 인증 키 값을 이용하여 홈 인증서버에게 자신이 등록된 이동 라우터임을 증명하며, 이때 사용하는 이동 라우터의 인증 키 (Authentication Key)는 패스워드와 같은 비밀 값을 사용한다. 이동 라우터는 홈 인증서버와 EAP-TLS를 통한 초기 인증 과정을 끝낸 후 상호 간에 MSK (Master Session Key)를 공유한다. 이 키는 MANET 도메인에서 이동 라우터가 액세스 라우터에게 임시 인증서 발급을 요청하는 과정에서 이동 라우터의 식별 정보를 안전하게 보호하기 위해 사용하는 세션키 $SK_{MR\text{-}HAS}$와 액세스 라우터에서 발급하는 임시 인증서를 안전하게 보호하기 위해 사용하는 세션키 $SK_{MR\text{-}AR}$를 생성하는데 사용된다.

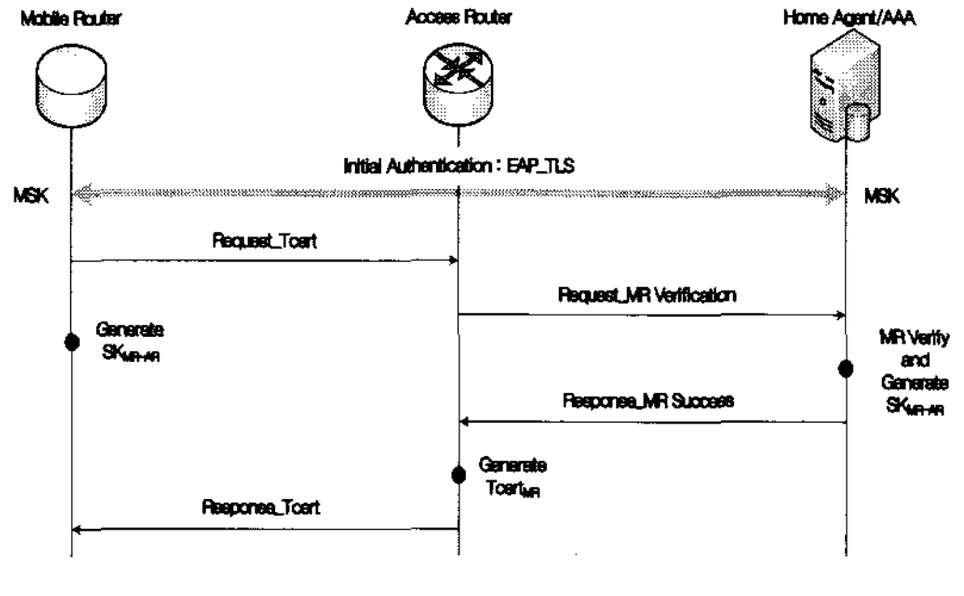
3.2 임시 인증서 발급 과정

이동 라우터는 초기 인증을 끝낸 후 MANET 도메인에 존재하는 이동 라우터 간의 상호인증을 위해 사용하는 임시 인증서 발급 요청을 액세스 라우터에게 한다.

다음은 임시 인증서 발급 과정에서 사용되는 주요 용어를 정의한다.

- Request_Tcert (Request Temporary Certificate) : 이동 라우터가 액세스 라우터에게 임시 인증서 발급을 요청할 때 사용하는 메시지
- Response_Tcert (Response Temporary Certificate) : Request_Tcert 메시지에 대한 응답으로 액세스 라우터가 이동 라우터에게 임시 인증서를 발급할 때 사용하는 메시지
- Request_MR Verification (Request Mobile Router Verification) : 액세스 라우터가 임시 인증서 발급 요청을 한 이동 라우터의 홈 인증서버에게 이동 라우터의 인증을 요청할 때 사용하는 메시지
- Response_MR Success (Response Mobile Router Success) : 홈 인증서버에서 액세스 라우터가 전송한 Request_MR Verification 메시지의 응답으로 이동 라우터의 인증 성공을 알릴 때 사용하는 메시지
- Tcert (Temporary Certificate) : 액세스 라우터에서 이동 라우터에게 발급하는 임시 인증서
- MSK (Master Session Key) : EAP-TLS 초기인증 과정을 통해 이동 라우터와 홈 인증서버 간에 공유하는 키
- K_{AR-}, K_{AR+} (Private Key and Public Key of AR) : 액세스 라우터의 개인키 K_{AR-}와 공개키 K_{AR+}
- SK_{X1-X2} (Session Key) : X1과 X2 간의 세션키
- X_{MR}, Y_{MR} : 이동 라우터의 Diffie-Hellman 비밀값 X와 공개 값 Y
- [ ]E_K : 키 K를 이용한 암호화
- ID_X : 이동 라우터 X의 식별자
- t_{AR} : 액세스 라우터에서 생성하는 타임스탬프
- $nonce_X$: 이동 라우터 X에서 생성한 임의의 랜덤 값
- h[ ] : HMAC-SHA1
- MAC_X : 세션키 X를 이용하여 생성한 값

앞서 설명한 이동 라우터의 초기 인증 과정과 임시 인증서 발급 과정을 [그림 4]에서 설명하고 있다. 위의 그림에서처럼 MANET 도메인의 이동 라우터가 임시 인증서를 액세스 라우터로부터 안전하게 발급 받기 위해서는 액세스 라우터를 검증 할 수 있어야 하고, 액세스 라우터는 이동 라우터를 검증 할 수 있어야 한다. 이동 라우터와 액세스 라우터 간에는 사전에 SA (Secure Association)가 설립되어 있지 않기 때문에 홈 인증서버를 통해 서로를 검증한다. 이동 라우터는 액세스 라우터에게 임시 인증서 발급 요청을 위해 전송하는 Request_Tcert 메시지에 임시 인증서 발행에 필요한 자신의 식별정보를 포함하여 전송한다. 이때 전송되는 이동 라우터의 식별정보는 이동 라우터와 홈 인증서버 간에 초기 인증 과정을 통해 공유하고 있는 MSK를 이용하여 식 1과 같이 생성한 세션키 SK_{MR-HAS}로 암호화하여 전송한다. 이렇게 함으로서 검증되지 않은 액세스 라우터 또는 악의 적인 공격자로부터 이동 라우터의 식별정보가 변경되지 않도록 보호하고, 이후 검증된 액세스 라우터가 이동 라우터의 식별정보를 안전하게 전달받을 수 있게 한다. 이동 라우터가 전송하는 Request_Tcert 메시지는 식 2와 같다. 액세스 라우터가 Request_Tcert 메시지를 수신하면 이동 라우터를 검증하기 위해 이동 라우터의 홈 인증서버에게 식 3과 같은 Request_MR Verification 메시지를 전송한다. 이 메시지는 액세스 라우터의 인증서버를 통해 이동 라우터의 홈 인증서버로 전달되며, 이때 전달되는 메시지는 TLS 또는 IPSec 프로토콜에 의해 안전하게 보호된다.



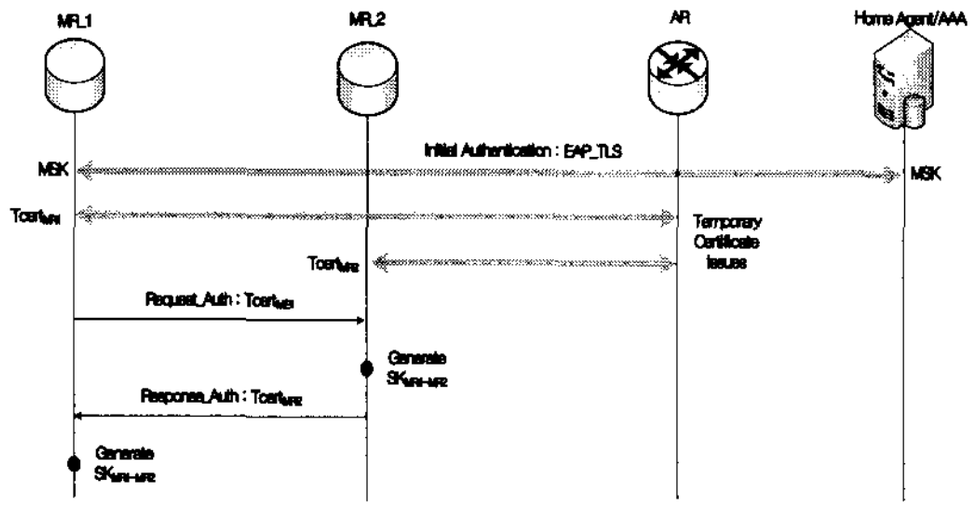
〔그림 4〕 Mobile Router를 위한 임시 인증서 발급 과정

$$SK_{MR-HAS} : h[MSK, Authentication\ Key] \quad (1)$$

$$Request\_Tcert : [ID_{MR}, nonce_{MR}, Y_{MR}]E_{SK_{MR-HAS}} \quad (2)$$

$$Request\_MR\ Verification : [ID_{MR}, nonce_{MR}, Y_{MR}]E_{SK_{MR-HAS}} \quad (3)$$

홈 인증서버가 Request_MR Verification 메시지를 수신하면 이동 라우터에서 식별정보 암호화를 위해 사용한 세션키 SK_{MR-HAS}를 식 1과 같이 동일한 방법으로 생성하여 암호화된 메시지를 복호화 함으로서 이동 라우터를 검증한다. 이동 라우터의 검증이 성공하면 홈 인



〔그림 5〕 Mobile Router 간의 상호인증 과정

증서버는 이동 라우터와 액세스 라우터 간에 안전한 임시 인증서 전달 및 정상적인 액세스 라우터임을 이동 라우터가 검증하는데 사용하는 세션키 $SK_{MR\text{-}AR}$를 MSK와 $SK_{MR\text{-}HAS}$를 해쉬하여 수식 4와 같이 생성한다. 이렇게 생성된 세션키 $SK_{MR\text{-}AR}$는 홈 인증서버와 이동 라우터만 알고 있는 키들을 사용하여 생성하기 때문에 임의의 노드들이 생성할 수 없다. 따라서 액세스 라우터가 이 세션키로 임시 인증서를 암호화하여 이동 라우터에게 전달하게 함으로서 액세스 라우터를 이동 라우터가 검증할 수 있으며, 임시 인증서를 안전하게 전달할 수 있다. 세션키 $SK_{MR\text{-}AR}$를 생성한 후 홈 인증서버는 식 5와 같이 이동 라우터의 식별정보와 Request_MR Verification 메시지, 그리고 인증서버가 생성한 세션키 $SK_{MR\text{-}AR}$를 해쉬하여 $MAC_{SKMR\text{-}AR}$을 생성한다. 생성된 $MAC_{SKMR\text{-}AR}$ 값은 이후 이동 라우터가 식 8과 같은 메시지를 수신했을 때 세션키 $SK_{MR\text{-}AR}$를 검증하는데 사용되고, 액세스 라우터가 식 6과 같은 메시지를 인증서버로부터 수신 했을 때 자신이 수신한 정보들이 올바른 정보임을 검증하는데 사용된다. 이렇게 생성된 $MAC_{SKMR\text{-}AR}$과 세션키 $SK_{MR\text{-}AR}$, 그리고 이동 라우터의 식별정보는 식 6과 같이 Response_MR Success 메시지에 포함되어 안전한 채널을 통해 액세스 라우터에게 전송된다.

$$SK_{MR-AR} : h[MSK, SK_{MR-HAS}, nonce_{MR}] \quad (4)$$

$$MAC_{SK_{MR-AR}} : h[ID_{MR}, nonce_{MR}, Y_{MR}, Request\_MR\,Verification, SK_{MR-AR}] \quad (5)$$

$$Response\_MR\,Success : ID_{MR}, nonce_{MR}, Y_{MR}, SK_{MR-AR}, MAC_{SK_{MR-AR}} \quad (6)$$

액세스 라우터가 안전한 채널을 통해 Response_MR Success 메시지를 수신한 후 메시지에 포함된 이동 라우터의 식별정보를 자신의 개인키 $K_{AR\text{-}}$로 서명하여 임시 인증서를 식 7과 같이 생성한다. 이때 사용하는 개인키 $K_{AR\text{-}}$는 RSA 알고리즘을 이용하여 액세스 라우터가 생성한 개인키이며, t_{AR}은 임시 인증서가 생성된 시간을 의미한다. 액세스 라우터는 임시 인증서를 생성한 다음 홈 인증서버가 생성하여 전달해준 세션키 $SK_{MR\text{-}AR}$로 임시 인증서와 액세스 라우터의 공개키 K_{AR+}를 암호화 하여 이동 라우터에게 전송한다. 이렇게 공개키를 세션키 $SK_{MR\text{-}AR}$로 암호화하여 전달하면 PKI에서처럼 공인 인증서를 사용하지 않고도 이동 라우터에게 액세스 라우터의 공개키에 대한 신뢰성을 제공할 수 있다. 이때 암호화 되어 전달되는 액세스 라우터의 공개키 K_{AR+}는 액세스 라우터의 개인키 $K_{AR\text{-}}$로 서명되어 발급된 다른 이동 라우터의 임시 인증서를 이동 라우터들이 검증하는데 사용한다. 액세스 라우터는 임시 인증서를 생성한 후 식 8과 같이 Response_Tcert 메시지에 생성한 임시 인증서, 액세스 라우터의 공개키, 그리고 홈 인증서버가 생성한 $MAC_{SKMR\text{-}AR}$을 포함하여 이동 라우터로 전송한다.

$$Tcert_{MR} : [ID_{MR}, nonce_{MR}, Y_{MR}, t_{AR}]E_{K_{AR-}} \quad (7)$$

$$Response\_Tcert : [Tcert_{MR}, K_{AR+}]E_{SK_{MR-AR}}, MAC_{SK_{MR-AR}} \quad (8)$$

이동 라우터가 Response_Tcert 메시지를 수신하면 식 4에서와 같이 $SK_{MR\text{-}AR}$ 세션키를 동일한 방법으로 생성한다. 생성된 세션키 $SK_{MR\text{-}AR}$를 이용하여 홈 인증서버가 생성한 $MAC_{SKMR\text{-}AR}$을 검증하고, 암호화된 메시지를 복호화 함으로서 정상적인 액세스 라우터로부터 임시 인증서를 발급 받았음을 검증한다. 만약 $MAC_{SKMR\text{-}AR}$ 검증이 실패 할 경우 암호화된 메시지를 복호화하지 않고 바로 폐기하여 악의적인 공격자가 생성하여 전송하는 임의의 메시지로 인한 공격을 막는다. 이후 이동 라우터는 발급 받은 임시 인증서를 사용하여 MANET 도메인에 속한 다른 이동 라우터들과 상호인증을 위해 사용한다.

3.3 이동 라우터 간 상호인증 과정

MANET 도메인에 속한 이동 라우터 간의 상호인증 과정을 위의 [그림 5]에서 보여준다. 위의 그림에서처럼

상호인증을 수행한 이동 라우터들은 상호인증 과정에서 Diffie-Hellman을 이용하여 세션키를 공유하고 이 키를 이용하여 안전한 통신을 할 수 있도록 지원한다.

이동 라우터가 MANET 도메인에 속한 또 다른 이동 라우터들과 안전한 통신을 원할 경우 이동 라우터들은 액세스 라우터로부터 발급 받은 임시 인증서를 이용하여 상호인증 과정을 수행 한다. 위의 [그림 5]에서처럼 MR_1과 MR_2가 상호인증을 수행할 때 MR_1은 MR_2에게 자신의 인증서가 포함된 식 9와 같은 Request_Auth 메시지를 전송한다. 이 메시지에는 MR_1의 식별정보, Diffie-Hellman 공개 값, 그리고 임시 인증서 등이 포함되어 있다. 상호인증 수행을 위한 Request_Auth 메시지를 수신한 MR_2는 MR_1의 임시 인증서를 액세스 라우터의 공개키 K_{AR+}로 확인하여 MR_1을 인증한다. 이후 메시지에 포함된 MR_1의 Diffie-Hellman 공개 값 Y_{MR1}을 이용하여 세션키 $SK_{MR1\text{-}MR2}$를 생성한다. 세션키를 생성한 MR_2는 자신의 임시 인증서와 MR_1의 임시 인증서를 생성한 세션키 $SK_{MR1\text{-}MR2}$와 함께 해쉬하여 식 10과 같은 $MAC_{SKMR1\text{-}MR2}$을 생성한다. 생성된 $MAC_{SKMR1\text{-}MR2}$ 값은 상호인증 과정에서 생성된 세션키가 정상적인 이동 라우터, 즉 MR_2에서 생성되었음을 검증하고, 전송되는 과정에서 메시지의 무결성을 보장해준다. 또한 $MAC_{SKMR1\text{-}MR2}$를 생성할 때 사용한 세션키 $SK_{MR1\text{-}MR2}$는 임시 인증서에 포함된 Diffie-Hellman 공개 값을 사용하여 생성하는 값이므로 상호인증 과정가운데 존재하는 악의적인 공격자가 이동 라우터들의 임시 인증서를 습득하여 취할 수 있는 중간자 공격을 막을 수 있다. 앞서 설명한 것처럼 MR_2는 세션키와 $MAC_{SKMR1\text{-}MR2}$을 생성한 후 자신의 인증서와 함께 Response_Auth 메시지를 식 11처럼 생성하여 MR_1에게 전송한다. 이 메시지를 수신한 MR_1은 액세스 라우터의 공개키 K_{AR+}로 MR_2의 임시 인증서를 확인하고, 임시 인증서에 포함된 Diffie-Hellman 공개 값 Y_{MR2}를 이용하여 세션키 SKMR1-MR2를 생성한다. 생성된 세션키 $SK_{MR1\text{-}MR2}$로 동일한 $MAC_{SKMR1\text{-}MR2}$을 생성 후 비교함으로서 상호인증 과정을 끝낸다.

$$Request\_Auth \ : \ Tcert_{MR1}, ID_{MR1}, Y_{MR1} \tag{9}$$

$$MAC_{SK_{MR1-MR2}} \ : \ h[Tcert_{MR1}, Tcert_{MR2}, SK_{MR1-MR2}] \tag{10}$$

$$Response\_Auth \ : \ Tcert_{MR2}, MAC_{SK_{MR1-MR2}} \tag{11}$$

앞서 설명한 것처럼 상호인증 과정에서 액세스 라우터가 발행한 임시 인증서를 사용하여 상호인증을 수행한다. 때문에 MANET 도메인에 속한 이동 라우터 간에는 AAA 서버를 이용한 인증기술 또는 공인 인증서 기반의 PKI 인증기술에 비해 간단하게 상호인증을 수행하고, 인증서 교환 과정에서 상호간 세션키를 공유하여 사용하기 때문에 안전한 통신이 보장된다.

Ⅳ. 기존 인증 기법과 제안 기법 비교 분석

이번 장에서는 MANEMO 환경에서 이동 라우터 간 상호인증을 위해 본 논문에서 제안하는 임시 인증서 기반 인증 기법과 앞서 설명했던 AAA 서버 기반의 상호인증 기법 그리고 기존 PKI 인증서 기반의 상호인증 기법과의 비교 분석을 통해 제안하는 상호인증 기법의 효율성을 검증 한다.

4.1 이동 라우터 인증 기법 비교 분석

기존에 제안된 여러 인증 기법은 AAA 서버를 이용한 상호인증 기법과 PKI 인증서 기반을 이용한 상호인증 기법으로 크게 두 가지로 분류할 수 있다. 본 논문에서 비교분석하는 AAA 서버 모델과 기존 PKI 모델의 경우 NEMO에서 제안된 모델을 기준으로 한다. [표 1] AAA 서버 모델과 기존 PKI 모델, 본 논문에서 제안하는 인증 기법에 대해 비교 분석한 표이다. [표 1]은 중첩된 네트워크에 존재하는 이동 라우터 간에 통신을 원할 경우, 두 이동 라우터 간 상호인증 과정에서 발생하는 인증 메시지의 수와 인증 메시지에 추가되는 오버헤드를 비교한 결과이다. 표에서 보는 것처럼 제안기법은 기존 인증방식에 비해 상호인증 과정에서 필요한 인증 메시지의 수와 인증 메시지에 추가되는 오버헤드를 최소화하였다.

AAA 서버를 이용한 인증 모델의 경우 표 1에서처럼 커뮤니케이션 오버헤드 즉, 메시지 수가 9로서 가장 높다. 이는 이동 라우터 간 상호인증 시 AAA 서버에서 이동 라우터 인증을 수행하기 때문에 상호인증을 위한 전체 인증 메시지의 수가 증가한다. 인증 메시지 수의 증가는 전체 레이턴시를 증가시켜 이동 라우터의 상호인증시 다른 인증 모델에 비해 전체 인증시간이 상대적으로 많이 걸리는 단점이 있다.

기존 PKI 인증서 기반 모델의 경우 인터넷 접속을 제

〔표 1〕 기존 인증 기법과 제안 기법의 효율성 비교분석

		기존 인증 모델		제안 기법
		AAA 서버 모델[6]	PKI 인증서 기반 모델[9]	제안 프로토콜
이동 라우터 인증 방식		AAA 서버를 통해 인증	공인 인증서 사용	AR에서 발행하는 임시 인증서 사용
이동 라우터 간 직접적인 상호인증		미지원 (AAA 서버에 의존적)	지원 (공인 인증서 사용)	지원 (임시 인증서 사용)
서로 다른 망사업자에 속한 이동 라우터 간 상호인증 시	커뮤니케이션 오버헤드	9개	8개	2개
	Latency	$4T_{MR1-MR2}+2T_{MR2-AR}+2T_{AR-HAS2}+2T_{HAS1-HAS2}+2T_{HAS1-HA1}$	$4T_{MR1-D} + 4T_{MR2-D}$	$2T_{MR1-MR2}$
AR의 역할		인터넷 연결 제공	인터넷 연결 제공	인터넷 연결 제공, 임시 인증서 발행

TA-B는 노드 A, B 간의 레이턴시 시간을 나타낸다. D는 PKI에서 인증서를 위한 디렉토리 서버를 의미한다.
효율성 비교를 위한 가정 : PKI 인증서 기반 모델에서 이동 라우터들은 서로 다른 공인인증 기관으로부터 인증서를 발급받아 사용한다고 가정하였다.

공하는 망 사업자가 단일 사업자이며 액세스 라우터와 모든 이동 라우터들이 동일한 공인 인증기관으로부터 발급받은 인증서를 사용할 경우 간단하게 인증서 교환을 통해 상호인증을 수행할 수 있다. 그러나 실제 MANEMO 환경의 경우 다양한 망 사업자들이 공존하며 각 망 사업자들은 서로 다른 공인 인증기관을 통해 발급받은 인증서를 사용한다. 때문에 서로 다른 인증기관으로부터 인증서를 발급받은 이동 라우터 간에 상호인증을 수행할 경우 각 이동 라우터들은 상대방의 인증서를 검증하기 위한 공개키를 얻기 위해 인증서 체인을 형성하게 되고, 디렉토리 서버에서 필요한 공개키를 받아와야 한다. 디렉토리 서버에서 필요한 공개키를 받아오기 위한 메시지가 상호인증 과정에서 추가되기 때문에 커뮤니케이션 오버헤드가 8이 된다. 전체 레이턴시는 AAA 서버 모델 보다 상대적으로 낮다. 그러나 본 논문에서 제안하는 기법의 경우 이동 라우터 간 상호인증을 위해 공인 인증서를 사용하지 않고 액세스 라우터가 발급하는 임시 인증서를 사용하여 인증을 수행하기 때문에 인증서 체인을 형성할 필요가 없으며, MANET 도메인에서 임시 인증서를 발급 받은 이동 라우터 간에 상호인증시 2번의 메시지 교환만을 필요로 한다. 따라서 AAA 서버 모델이나 PKI 인증서 기반 모델에 비해서 전체 레이턴시와 커뮤니케이션 오버헤드가 상대적으로 더 낮다.

위에서 언급한 것처럼 중첩된 네트워크 환경에 존재하는 이동 라우터 간 상호인증시 기존 방법에 비해 커뮤니케이션 오버헤드 및 상호인증시간이 단축되는 것을 알 수 있다. 그러나 제안하는 방법의 경우 초기 인증 과정에서 사용하는 EAP-TLS와 MANEMO의 MANET 도메인에서 사용하는 임시 인증서를 액세스 라우터로부터 최초 발행 받게 될 때 커뮤니케이션 오버헤드가 발생할 수 있다. 초기 부팅 과정을 끝낸 이동 라우터가 임시 인증서를 발급 받지 않은 상태에서 MANEMO의 MANET 도메인으로 이동 하였을 경우 액세스 라우터로부터 임시 인증서를 발급받는 과정이 필요하기 때문에 커뮤니케이션 오버헤드가 발생할 수 있다.

4.2 안전성 분석

다음은 본 논문에서 제안하고 있는 임시 인증서를 이용한 이동 라우터 간 상호인증 기법에 대한 보안 안전성을 분석하였다.

4.2.1 중간자 공격 및 위조/수정 공격

MANET 도메인에는 악의적인 공격자가 쉽게 접근할 수 있으며 MANET 환경의 다양한 보안 취약성을 이용한 공격이 가능하다. 그중에서 멀티 홉으로 통신하는 MANET 환경에서 악의적인 공격자에 의한 중간자 공격은 정상적인 통신을 하고자 하는 이동 라우터들에게 심각한 피해를 줄 수 있다. 본 논문의 제안기법에서 임시 인증서를 발행할 때 악의적인 공격자가 중간자 공격에 성공하려면 임시 인증서 발행 요청을 위해 전송하는 Request_Tcert 메시지에 암호화된 이동 라우터의 식

별정보를 변경할 수 있어야 하고, 식별정보를 암호화 하는데 사용한 세션키 $SK_{MR\text{-}HAS}$를 생성할 수 있어야 한다. 하지만 제안하는 기법에서 악의적인 공격자가 Request_Tcert 메시지에 포함된 이동 라우터의 식별정보를 변경하는 것은 매우 어렵다. 임시 인증서를 요청하는 이동 라우터는 자신의 식별 정보를 세션키 $SK_{MR\text{-}HAS}$로 암호화하여 액세스 라우터에게 전송한다. 이 세션키는 초기 인증 과정을 통해 홈 인증서버와 공유하는 MSK를 이용하여 생성되기 때문에 악의적인 공격자는 세션키 $SK_{MR\text{-}HAS}$를 임의로 생성할 수 없으며, 식별정보를 변경할 수 없다. 따라서 전송되는 Request_Tcert 메시지의 비밀성이 보장되므로 중간자 공격에 안전하다. 또한 이동 라우터에게 발급되는 임시 인증서는 홈 인증서버가 생성하여 액세스 라우터에게 전송해준 세션키 $SK_{MR\text{-}AR}$로 암호화 되어 전달되므로 중간자 공격에 안전하다. 임시 인증서 발행이 완료된 후 상호인증 과정에서 악의적인 공격자가 중간자 공격을 시도할 수 있다. 그러나 상호인증 과정에서 사용되는 임시 인증서는 액세스 라우터의 개인키로 서명되어 있기 때문에 악의적인 공격자는 임시 인증서의 내용을 수정할 수 없다. 또한 MR_1과 MR_2 간의 상호인증 과정에서 생성된 세션키 $SK_{MR1\text{-}MR2}$를 이용하여 해쉬한 $MAC_{SKMR1\text{-}MR2}$을 통해 메시지의 무결성 및 세션키를 생성한 이동 라우터를 검증할 수 있기 때문에 중간자 공격 또는 위조/수정 공격에 안전하다.

4.2.2 위장 공격

본 논문에서 액세스 라우터는 MANET 도메인에 속한 이동 라우터들 간의 상호인증과정에서 사용되는 임시 인증서를 발급한다. 따라서 액세스 라우터가 정상적인 액세스 라우터 인지 이동 라우터 들이 검증할 수 있어야 한다. 만약 악의적인 목적의 액세스 라우터를 이동 라우터에서 검증하지 못할 경우 악의적인 액세스 라우터가 발급하는 임시 인증서를 이동 라우터들이 사용하게 되고, 이동 라우터들의 식별 정보를 이용한 다양한 공격에 노출 될 수 있다. 본 논문에서 제안하는 기법에서 이러한 공격을 막기 위해 임시 인증서를 발행할 때 액세스 라우터는 이동 라우터의 홈 인증서버가 생성한 세션키 $SK_{MR\text{-}AR}$로 임시 인증서를 암호화하여 이동 라우터에게 전달한다. 이 세션키는 홈 인증서버와 이동 라우터만 알고 있는 MSK와 세션키 $SK_{MR\text{-}HAS}$를 해쉬하여 생성하기 때문에 임의의 액세스 라우터가 생성할 수 없다. 따라서 이동 라우터는 이 세션키를 이용하여 임시 인증서를 발행하는 액세스 라우터를 검증 할 수 있다. 만약 위장된 액세스 라우터가 임의의 비밀키로 암호화된 임시 인증서를 생성하여 이동 라우터에게 전송해 주더라도 이동 라우터는 위장된 액세스 라우터가 생성한 세션키 $SK_{MR\text{-}AR}$'와 자신이 생성한 세션키 $SK_{MR\text{-}AR}$가 다르기 때문에 수신한 메시지를 처리할 수 없으며, 액세스 라우터의 검증도 실패하게 된다.

4.2.3 DoS 공격

제안하는 기법은 DoS 공격에 안전하다. 공격자는 이동 라우터가 액세스 라우터에게 임시 인증서를 발급 받기 위해 전송하는 Request_Tcert 메시지를 이용하여 DoS 공격을 시도 할 수 있다. 그러나 Request_Tcert 메시지는 이동 라우터와 홈 인증서버가 초기 인증 이후에 공유하는 MSK를 이용하여 생성하는 세션키 $SK_{MR\text{-}HAS}$로 암호화 되어 전달되기 때문에 악의적인 공격자가 메시지 내용을 수정하거나 임의로 생성하여 전송할 수 없다. 또한 악의적인 공격자는 이동 라우터가 전송한 이전 Request_Tcert 메시지를 재전송하여 정상적인 이동 라우터가 임시 인증서를 발급 받는 것을 방해 할 수 있다. 이런 공격의 경우 액세스 라우터에서 일정시간 수신한 Request_Tcert 메시지를 해쉬하여 그 값을 보관하고, 이후 동일한 해쉬값을 가지는 중복된 Request_Tcert 메시지는 자동 파기함으로서 재전송 공격을 막을 수 있다. 그리고 액세스 라우터와 인증서버 간 안전한 채널을 가정하였기 때문에 액세스 라우터와 인증서버 간 전달되는 메시지를 이용한 공격자의 공격으로부터 안전하다.

위에서 설명한 공격들 이외에 MANET 도메인에서는 정상적으로 임시 인증서를 발급 받은 이동 라우터가 악의적인 공격자처럼 행동 할 수도 있다. 또한 다른 이동 라우터가 멀티홉 통신을 위해 자신의 컴퓨팅 파워, 메모리 리소스 등을 사용하여 다른 이동 라우터들과 통신하는 것을 허용하지 않는 이기적인 노드가 존재할 수 있으나 본 논문에서는 정상적인 노드의 이기적인 행동 또는 악의적인 행동은 고려하지 않았다.

V. 결 론

네트워크의 이동성을 지원하기 위해 제안된 NEMO

BS의 경우 중첩된 이동 네트워크의 레벨이 깊어질수록 핀볼 문제와 같은 경로 최적화 문제가 발생한다. 이러한 문제를 해결하기 위해 NEMO와 MANET을 결합한 MANEMO가 제안되었다. MANEMO는 중첩된 이동 네트워크 도메인에 있는 이동 라우터 간에 최적화된 경로를 제공해 주기위해 MANET 라우팅 프로토콜을 사용하여 이동 라우터 간 직접 경로 설정이 가능하도록 하였다. 제안된 MANEMO의 경우 기존 MANET 환경에 존재하던 보안 취약성이 그대로 존재한다. 이러한 보안 위협을 예방하기 위해 기존에 NEMO와 MANET 환경에서 적용된 AAA 서버 모델 또는 PKI 모델을 적용하여 보안 위협을 막을 수 있다. 그러나 기존 보안 모델을 MANEMO 환경에 적용할 경우 상호인증 과정에서 필요한 인증 메시지의 수와 패킷 오버헤드가 증가하는 문제가 있다. 이러한 문제를 해결하기 위해 본 논문에서는 보안 위협을 사전에 예방하고, 기존 보안 모델에 비해 패킷 오버헤드나 인증 메시지의 수를 줄일 수 있는 MANEMO 환경의 MANET 도메인에서의 상호인증 모델을 제안하였다. 본 논문에서 제안된 기법은 PKI를 사용하지 않고 액세스 라우터가 자신에게 인증서를 요청하는 이동 라우터에게 자신의 개인키로 서명한 임시 인증서를 배포하여 MANET 도메인 내에 있는 이웃 이동 라우터들 간에 상호인증을 쉽고 간단하게 할 수 있도록 제안하였다. 이렇게 함으로서 AAA 서버 모델에서처럼 이동 라우터가 인증을 받기 위해 AAA 서버를 이용하지 않기 때문에 전체적인 상호인증시간이 감소하고, 홈 에이전트와 이동 라우터 간에 터널링이 불필요함으로서 터널링에 의한 패킷 오버헤드를 감소 시켰다. 또한 기존 PKI 기반에서 문제가 되었던 인증서 체인으로 인한 이동 라우터에서 메모리 부담, 오버헤드, 인증서 계산량을 감소 시켰으며, 액세스 라우터에서 발급하는 임시 인증서를 이동 라우터들이 사용하게 함으로서 인증서 체인 없이 간단하게 상호인증을 할 수 있게 하였다.

참고문헌

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", *IETF*, RFC 3963, January 2005.

[2] C. Perkins and Ed., "IP Mobility Support for IPv4", *IETF*, RFC 3344, August 2002.

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

[4] B. Mccarthy, C. Edwards, and M. Dunmore, "Advances in MANEMO : Definition of the Problem Domain and the Design of a NEMO-Centric Approach", SAINT Workshops 2007, January 2007.

[5] D. Djenouri, L. Khelladi, Badache, and A.N., "A survey of security issues in mobile ad hoc and sensor networks", *Communications Surveys & Tutorials*, IEEE Volume 7, Issue 4, Fourth Quarter 2005.

[6] B. David, M. Antony, and G. Brahim, "A Proactive Authentication Integration for the Network Mobility", *Proc. ICWMC 2007*, March 2007.

[7] T. Kwon, S. Baek, S. Pack, and Y. Choi, "AAA for NEMO", *IETF Internet Draft*, draft-kwon-aaa-nemo-00, January 2006.

[8] P. Songwu Lu and Z. Lixia, "An overview of PKI trust models", *Networking, IEEE/ACM Transactions*, pp.1049-1063, Volume 12, December 2004.

[9] M. C. Morogan and S. Muftic, "Certificate management in ad hoc networks", *Applications and the Internet Workshops*, pp.337-341, January 2003.

[10] J.A Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15.4 : a developing standard for low-power low-cost wireless personal area networks", *Network IEEE*, Volume 15, September 2001.

[11] L. Jun, A. Bose, and Y.Q. Zhao, "The study of wireless local area networks and wireless personal area networks", *Electrical and Computer Engineering*, pp. 1415-1418, May 2005.

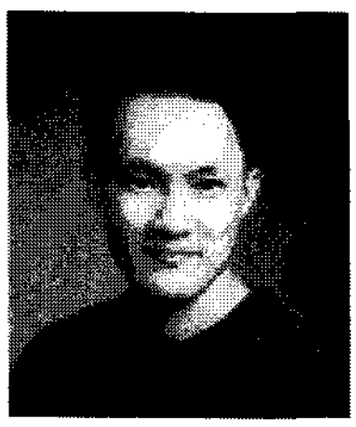
[12] H. Cho, T. Kwon, and Y. Choi, "Route Optimization Using Tree Information Option for Nested Mobile Networks", *Selected Areas in Communications, IEEE Journal*, Volume

24, pp. 1717-1724, September 2006.

[13] H. Fan, H. Liang, and C. Fu, "Secure OLSR", *1st IEEE ICNP Workshop on*, March 2005.

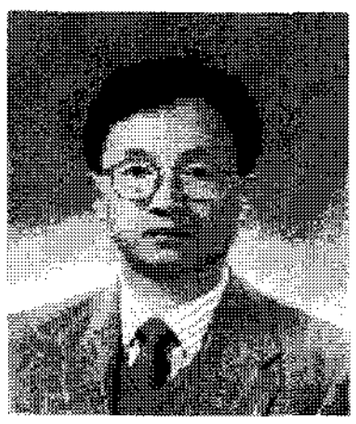
[14] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol", *IETF*, RFC 2716, October 1999.

〈著者紹介〉



노 효 선 (Hyosun Roh) 학생회원

2005년 2월 : 숭실대학교 정보통신전자공학부 졸업
2007년 2월 : 숭실대학교 정보통신전자공학과 석사
2007년 3월~현재 : 숭실대학교 전자공학과 박사과정
<관심분야> 이동 네트워크 보안, MANET 보안, 유비쿼터스 네트워크 보안



정 수 환 (Souhwan Jung) 종신회원

1985년 2월 : 서울대학교 전자공학과 졸업
1987년 2월 : 서울대학교 전자공학과 석사
1988년~1991년 : 한국통신 전임 연구원
1996년 6월 : University of Washington 박사
1996년~1997년 : Stellar One SW Engineer
1997년~현재 : 숭실대학교 정보통신전자공학부 부교수
<관심분야> 이동 네트워크 보안, VoIP 보안, 네트워크 보안, RFID/USN 보안