MIH 환경에서 카멜레온 해쉬 기반의 인증값을 이용한 선행 인증 기법

준회원 채 강 석*, 정회원 최 재 덕**, 종신회원 정 수 환*°

A Proactive Authentication Using Credentials based on Chameleon Hashing in MIH Environments

Kangsuk Chae* *Associate Member*, Jaeduck Choi** *Regular Member*,
Souhwan Jung*° *Lifelong Member*

요 약

본 논문에서는 카멜레온 해쉬 기반의 인증값을 이용한 MIH 선행 인증 기법을 제안한다. IEEE 802.21 보안 그룹은 MIH 환경에서 링크 액세스를 위한 인증 기술로 핸드오버 이전에 인증을 수행하는 선행 인증 구조를 정의하고 있다. 선행 인증 구조에 적용 가능한 기법으로 EAP 및 PKI 기반의 인증 기법들이 제안되고 있지만, 복잡한 인증 절차로 인한 네트워크 통신 및 PKI 환경 구축에 따른 부담이 발생한다. 제안 기법은 인증 서버 및 PKI 환경 구축 없이 카멜레온 해쉬 기반의 인증값을 이용하여 단말과 MIH 키 홀더 간에 선행 인증을 수행한다. 제안 기법은 MIH 선행 인증 과정에서 인증 서버의 개입이 필요하지 않기 때문에 인증 메시지 발생에 따른 네트워크 혼잡도를 감소키고, 카멜레온 해쉬 기반의 인증된 디피-헬만 공개키 교환을 수행하기 때문에 핸드오버 인증키에 대한 PFS 및 PBS와 같은 향상된 보안 서비스를 제공한다.

Key Words : Chameleon Hashing, Pre-Authentication, MIH, Vertical Handover, Diffie-Hellman

ABSTRACT

This paper proposes a proactive authentication scheme using credentials based on chameleon hashing in MIH environments. There is a proactive authentication structure defined by IEEE 802.21 Security Study Group for the link access in MIH environment. Both schemes based on EAP and on PKI can be applied to such structure, but the former has caused network traffic due to the complicated authentication procedure and the latter has complex structure for managing certificates. The proposed scheme performs the proactive authentication procedure only between a mobile node and a MIH Key Holder by using credentials based on chameleon hashing. Our scheme reduces the network traffic since authentication with the server is unnecessary in MIH environment and PKI structure is not required as well. In addition, the proposed scheme provides secure PFS and PBS features owing to the authenticated Diffie-Hellman key exchange of the chameleon-based credential.

※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. 2010-0000100)
* 숭실대학교 정보통신전자공학부 (chaekhan@cns.ssu.ac.kr, souhwanj@ssu.ac.kr), (° : 교신저자)
** ETRI 부설연구소 (cjduck@ensec.re.kr)
논문번호 : KICS2010-03-132, 접수일자 : 2010년 3월 31일, 최종논문접수일자 : 2010년 5월 10일

Ⅰ. 서 론

최근 이동통신의 급격한 발달로 이동성이 지원되는 고속의 데이터 서비스에 대한 요구가 증가하고 있다. 이러한 요구에 대한 일환으로 이기종 무선망 간 핸드오버시 끊김 없는 서비스 지원을 위한 연구가 다양하게 진행되고 있다. 특히 IEEE에서는 2004년 3월 802.21 WG (Working Group)을 구성하여 이기종 무선망간 상이한 미디어에 독립적인 핸드오버를 지원하는 기술의 표준화를 시작하였다. IEEE 802.21 MIH (Media Independent Handover) 기술[1]은 둘 이상의 링크 접속 인터페이스를 가진 이동 단말의 미디어 독립적인 핸드오버 수행을 지원한다. 이 기술에서 MIHF (Media Independent Handover Function)는 MIH 서비스 실행을 위한 구성요소이며, MIHF는 MIES (Media Independent Event Service), MICS (Media Independent Command Service), MIIS (Media Independent Information Service)의 3가지 주요 서비스를 제공하여 이기종 네트워크 간 미디어 독립적인 핸드오버를 지원한다.

한편, MIH 서비스 구조에서 핸드오버 인증을 위한 선행 인증 기법과, TLS를 이용하여 MIH 노드 간에 교환되는 메시지를 보호하는 기술에 대한 표준화를 IEEE 802.21 보안 그룹에서 진행하고 있다[2]. 선행 인증 기법은 이동 단말이 이동 대상 네트워크로 핸드오버 하기 전에 이동 대상 네트워크와 미리 핸드오버 인증을 수행한다. 보안 그룹에서는 MIH 프로토콜 선행 인증 기법으로 EAP 기반의 인증 프로토콜들을 정의하고 있으며, EAP 기반의 인증 기술로는 EAP-TLS [3],[4], EAP-Kerberos Ⅱ [5], ERP (EAP Re-authentication Protocol) [6],[7] 등이 있다. IEEE 802.21 보안 그룹에서 선행 인증 기법으로 EAP 기반의 인증 기술만 언급하고 있으나, PKI 기반의 선행 인증 기술도 [8] MIH 환경에 적용시킬 수 있다. 그러나 EAP 및 PKI 기반의 인증 프로토콜들은 인증서버를 통한 인증 절차 또는 PKI 환경 구축에 따른 부담을 가지고 있어 MIH 환경에서 핸드오버 인증시 네트워크 혼잡도 및 통신비용이 증가하여 비효율적이다.

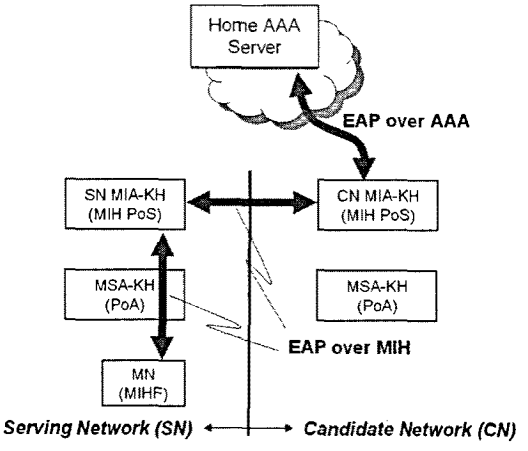
본 논문은 카멜레온 해쉬 기반의 인증값을 이용하여 MIH 환경에서 선행 인증을 수행하는 기법을 제안한다. 제안 기법은 매번 새롭게 생성하는 디피-헬만 (Diffie-Hellman) 공개키에 대한 인증을 위해서 카멜레온 해쉬 기반의 인증값을 이용한다. 또한 인증값을 이용하여 단말과 MIH 키 홀더 간에만 선행 인증 절차를 수행한다. 제안 기법은 카멜레온 해쉬 기반의 인증값으로 인증된 디피-헬만 키 교환을 수행하기 때문에 인증 서버와의 인증절차로 인한 네트워크 혼잡도 및 통신비용을 줄이고, PFS (Perfect Forward Secrecy) 및 PBS (Perfect Backward Secrecy) 기능과 같은 향상된 보안 서비스를 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 기법과 관련된 기술들을 설명하고, 3장에서 제안 기법을 설명하고, 4장에서 제안 기법에 대한 안전성 및 효율성 분석을 하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 MIH 환경의 선행 인증

IEEE 802.21 보안 그룹에서는 MIH 환경에서 핸드오버 인증을 위한 방법으로 EAP 선행 인증 기법을 수행하는 모델을 제안하고 있다 [2]. 선행 인증 모델로는 Direct 및 Indirect의 두 가지 모델이 소개되고 있다. Direct는 핸드오버 대상 PoS (Point of Service)와 상위 계층 통신을 이용하여 직접적으로 메시지를 전달하는 방식이고, Indirect는 Serving PoS를 통한 MIH 메시지 포워딩 방식이다. 그중 Indirect 선행 인증 모델은 그림 1과 같다. 선행 인증을 위한 네트워크 구성요소는 MSA-KH (Media Specific Authenticator and Key Holder)와 MIA-KH (Media Independent Authenticator and Key



MN: Mobile Node, PoA: Point of Attachment, PoS: Point of Service
MIA-KH: Media Independent Authenticator and Key Holder
MSA-KH: Media Specific Authenticator and Key Holder

그림 1. Indirect Proactive Authentication 모델[2]

표 1. 선행 인증을 위한 MIH 메시지[2]

메세지	기능
MIH_Pro_auth Request	EAP 메시지 전달
MIH_Pro_auth Response	
MIH_Pro_auth Indication	인증 절차 시작 지시
MIH_Pro_auth_Termination Request	인증 세션 종료 및 동기화
MIH_Pro_auth_Termination Response	

Holder)를 두고 있다. 이동단말은 핸드오버 이전에 CN (Candidate Network) MIA-KH와 MIH 프로토콜을 통해 EAP 선행 인증을 수행한다. 이동 단말과 CN MIA-KH가 상호인증 및 공유키 생성이 완료되면, CN MIA-KH는 CN MSA-KH로 계층적 키를 생성하여 분배한다. 이후 이동 단말이 새로운 네트워크로 핸드오버하게 되면 CN MSA-KH와 공유된 계층적 키의 확인 및 무선구간 보호를 위한 키 생성을 위해서 보안 협상 프로토콜 절차를 수행한다.

IEEE 802.21 보안 그룹에서는 이와 같이 MIH 프로토콜을 통한 EAP 선행 인증 동작을 수행하기 위해서 표 1과 같은 새로운 MIH 메시지를 제안하고 있다. 여기에서 정의된 MIH 메시지에 EAP 메시지를 포함하여 선행 인증을 수행한다. IEEE 802.21 보안 그룹에서 MIH 환경에 적용한 선행 인증 기법으로는 EAP를 이용한 인증 기법만 언급하고 있지만, 인증서버와의 절차 없이 이동단말과 MIA-KH 간의 PKI 기반의 선행 인증 기법도 정의된 MIH 메시지에 포함하여 인증 절차를 수행할 수 있다. 본 절에서는 MIH 환경에 적용 가능한 EAP 기반의 선행 인증 기법과 PKI 기반의 선행인증 기법에 대해서 설명한다.

• EAP 기반의 인증 기법

EAP-TLS는 IEEE 802.11i 기술에서 사용되는 인증 기법으로서 PKI 기반의 인증서를 이용하여 이동단말과 인증서버 사이의 상호 인증을 수행하는 기법이다 [3],[4]. 이동단말과 인증서버는 EAP 프로토콜에 TLS 메시지를 포함하여 인증서 기반의 TLS 절차를 수행하여 상호 인증을 수행하고, 무선구간 데이터 보호를 위한 키 생성에 필요한 마스터키를 공유한다. 인증서버는 이동단말의 인증에 성공하면 생성된 마스터키를 EAP 인증 성공 메시지와 함께 AP (Access Point)로 전달한다. 이후 이동단말과 AP는 공유된 마스터키로부터 4-way 핸드쉐이크 절차를 수행하여 무선구간 데이터 보호를 위한 키를 생성한다. 그러나 EAP-TLS는 인증서버와의 TLS 절차를 수행함으로 인증 절차가 복잡하고 인증지연 시간이 발생한다. 또한 PKI 기반의 인증서를 사용하기 때문에 인증서의 안전한 배포 및 인증서의 관리와 같은 부담을 가지고 있다.

Eun 등은 EAP-TLS의 인증절차의 복잡성으로 인한 시간 지연의 문제점을 해결하기 위한 방법으로 EAP-Kerberos Ⅱ 기법을 제안하였다 [5]. 이 기법은 이동단말과 인증서버 간에 공유된 비밀키와 AP와 인증서버 간에 공유된 비밀키를 이용해서 인증서버가 티켓을 생성하여 이동단말에게 전달하고, 이를 이용해서 이동단말과 네트워크 간의 상호인증을 빠르게 수행한다. 그러나 이 기법도 인증을 수행할 때마다 인증서버와의 인증 절차를 수행함으로 네트워크 혼잡도가 여전히 존재한다.

ERP는 잦은 인증서버와의 인증 절차를 줄이고 빠른 인증을 수행하기 위하여 계층적 키 구조를 이용한 재인증을 수행하는 기법이다 [6],[7]. ERP는 최초 홈 도메인에 존재하는 인증서버와의 초기 인증을 수행한 후 계층적 키를 지역 도메인을 관리하는 지역 재인증 서버로 전달한다. 이후 이동단말은 지역 재인증 서버의 도메인 내에서 핸드오버를 수행할 때 홈 도메인에 존재하는 인증서버와의 인증절차 없이 지역 재인증 서버와 빠르게 인증을 수행한다. 그러나 재인증 서버의 도메인이 바뀌는 핸드오버를 수행할 때는 홈 도메인의 인증서버와 인증을 수행해야만 한다.

• PKI 기반의 선행 인증 기법

Sun 등은 PKI 기반의 인증서를 이용하여 인증서버와의 인증 절차를 없애고, 이동단말과 핸드오버 대상 네트워크 간의 선행 인증 기법을 제안하였다 [8]. 이동단말은 핸드오버를 수행하기 전에 핸드오버 대상 네트워크의 Authenticator와 인증서를 기반으로 하는 인증절차를 수행한다. 이때 인증서는 이동단말과 핸드오버 대상 네트워크의 Authenticator의 인증서이며, 인증서버와의 인증절차는 없다. 또한 인증 절차를 간소화하여 네트워크 혼잡도를 감소시켰다. 그러나 이 기법은 PKI 기반의 인증서를 사용하기 때문에 PKI 환경이 갖는 인증서의 배포 및 관리와 같은 부담이 존재한다.

2.2 카멜레온 해쉬 기법

Krawczyk 등은 특수한 트랩도어 해쉬 함수를 카멜레온 해쉬 함수로 정의하고 있다 [9]. 우선 큰 소

수 g, p를 생성하고 카멜레온 해쉬 비밀키 x를 선택한다 ($x \in Z_p^*$). 이후 카멜레온 해쉬에 사용되는 카멜레온 해쉬 공개키 y를 식 (1)과 같이 계산한다.

$$y = g^x \bmod p \tag{1}$$

임의의 값 $r_{(0)}$와 $m_{(0)}$을 변수로 하고, 카멜레온 해쉬 공개키 y를 이용한 카멜레온 해쉬값을 식 (2)와 같이 계산한다.

$$CH_y(r_{(0)}, m_{(0)}) = g^{r_{(0)}} y^{m_{(0)}} \bmod p \tag{2}$$

이후 새로운 메시지 $m_{(1)}$에 대해서 동일한 카멜레온 해쉬값을 가지는 충돌값 $r_{(1)}$은 식 (3)과 같이 계산하며, 이 값은 카멜레온 해쉬 비밀키 x를 아는 사용자만 계산할 수 있다.

$$r_{(1)} = r_{(0)} + x(m_{(0)} - m_{(1)}) \tag{3}$$

새롭게 생성한 $r_{(1)}$과 $m_{(1)}$에 대한 카멜레온 해쉬값은 최초 임의의 값 $r_{(0)}$, $m_{(0)}$에 대한 카멜레온 해쉬값과 동일한 것을 식 (4)와 같이 확인 할 수 있다.

$$\begin{aligned} & CH_y(r_{(1)}, m_{(1)}) \\ &= g^{r_{(1)}} y^{m_{(1)}} \bmod p \\ &= g^{r_{(0)} + x(m_{(0)} - m_{(1)})} g^{x m_{(1)}} \bmod p \\ &= g^{r_{(0)}} g^{x m_{(0)}} \bmod p \\ &= CH_y(r_{(0)}, m_{(0)}) \end{aligned} \tag{4}$$

Ⅲ. 제안 기법

본 논문은 MIH 환경에서 카멜레온 해쉬 기반 인증값을 이용한 선행 인증 기법을 제안한다. 본 논문에서는 카멜레온 해쉬를 이용한 인증된 디피-헬만 키 교환 및 인증 기법을 [10] 사용하여 MIH 환경에서 선행 인증 기법을 제안한다. 카멜레온 해쉬 기반의 키 교환 및 인증 기법은 카멜레온 해쉬를 이용하여 매번 새롭게 생성한 디피-헬만 공개키에 대한 인증을 제공하기 때문에 PKI 기반이 요구되지 않는다. 또한 인증값을 이용한 디피-헬만 키 교환을 수행함으로써 인증서버와의 인증절차 없이 이동단말과 이동 대상 MIA-KH간 상호 인증 및 키 교환을 수행할 수 있어 핸드오버 인증의 통신비용을 줄일 수 있다.

본 논문에서 제안하는 MIH 프로토콜에서 동작하는 선행 인증 기법은 IEEE 802.21 보안 그룹에서 정의한 MIH 메시지를 이용하여 이루어진다. 제안 기법의 프로토콜 절차는 초기 인증 및 인증값 분배 단계, MIH 선행 인증 단계의 두 단계로 이루어진다. 본 논문에서 사용하는 프로토콜 표기는 표 2와 같고, 제안 기법의 전체 프로토콜 수행 절차는 그림 2와 같다.

- 초기 인증 및 인증값 분배 단계

이동단말이 처음 무선망에 접속하면 EAP-TLS 등과 같은 인증서버를 통한 기존 무선망의 인증 방

표 2. 프로토콜 표기법

표기	정의
ID_{Node}	$Node$의 식별자, 신원정보
PK_{Node}^{-} / PK_{Node}^{+}	$Node$의 RSA 비밀키/공개키
C_{Node}	$Node$의 인증값
T_{Ex}	인증값의 유효시간
T_{Cur}	메시지 생성시간
$x_{Node(i)}$/$y_{Node(i)}$	$Node$의 디피-헬만 비밀키/공개키, $y_{Node(i)} = g^{x_{Node(i)}} \bmod p$ 카멜레온 해쉬 비밀키/공개키로도 사용됨
$r_{Node(i)}$	충돌값, $r_{Node(i)} = r_{Node(0)} + x_{Node(0)} m_{Node(0)} - x_{Node(i)} m_{Node(i)}$ $r_{Node(0)}$은 임의의 비밀값
$m_{Node(i)}$	해쉬값, $m_{MN(i)} = h(y_{MN(i)} \| T_{Cur})$ $m_{Node(0)}$은 임의의 비밀값
$h(\bullet)$	일방향 해쉬 함수 (eg. SHA_1, SHA_256, MD5, ...)
$CH_y(r,m)$	카멜레온 해쉬 함수, $CH_y(r,m) = g^r g^{rm} \bmod p$

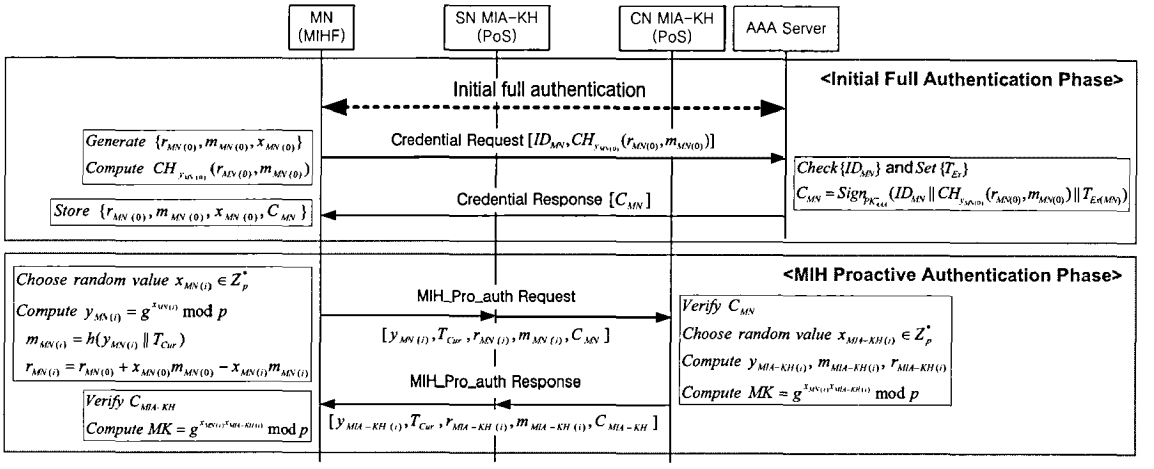


그림 2. 제안 기법의 프로토콜 수행 절차

식으로 인증을 수행한다. 이렇게 초기 인증이 완료되고 이동단말과 인증서버 간의 안전한 채널이 형성된 후 이동단말은 인증서버로부터 인증값을 분배받는 절차를 수행한다.

이동단말은 임의의 비밀값 $r_{MN(0)}$, $m_{MN(0)}$, $x_{MN(0)}$을 선택하고 식 (5)과 같이 카멜레온 해쉬값을 계산한다. 계산된 카멜레온 해쉬값과 이동단말의 신원정보 ID_{MN}를 포함한 인증값 요청 메시지는 안전한 채널을 통해 인증서버로 전달한다.

$$y_{MN(0)} = g^{x_{MN(0)}} \bmod p$$
$$CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)}) = g^{r_{MN(0)}} g^{x_{MN(0)} m_{MN(0)}} \bmod p \quad (5)$$

이동단말의 인증값 요청 메시지를 수신한 인증서버는 이동단말의 신원정보 ID_{MN}을 확인하고, 과금정책에 따라서 인증값의 유효시간 T_{Ex}를 결정한다. 이후 인증서버는 식 (6)과 같이 본인의 RSA 개인키 PK_{AAA}^{-}로 인증값 생성정보인 ID_{MN}, $CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)})$, T_{Ex}를 서명한 이동단말의 인증값 C_{MN}를 생성한다. 이렇게 생성한 이동단말의 인증값 C_{MN}을 인증값 응답 메시지에 포함하여 이동단말에게 전송한다.

$$C_{MN} = Sign_{PK_{AAA}^{-}}(ID_{MN} \| CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)}) \| T_{Ex}) \quad (6)$$

- MIH 선행 인증 단계

이동단말은 새로운 무선망으로 핸드오버가 필요하게 되면 MIH 프로토콜 절차를 수행하여 핸드오버 대상 네트워크의 정보를 얻고 자원 준비 절차를 수행한다. 이 과정을 통해 이동단말은 핸드오버 대상 네트워크를 결정할 수 있기 때문에 핸드오버 이전에 인증 및 키 교환을 수행하는 것이 가능하며, 이 절차는 MIH 선행 인증 프로토콜을 통해 이루어진다.

이동단말은 인증 및 키 교환을 위한 정보들을 생성한다. 먼저 이동단말은 새로운 디피-헬만 비밀키 $x_{MN(i)}$, 공개키 $y_{MN(i)} = g^{x_{MN(i)}} \bmod p$를 생성한다. 이때 생성된 디피-헬만 공개키는 수신측에서 메시지의 인증을 위한 카멜레온 해쉬 과정에서도 사용되는 해쉬 공개키가 된다. 이후 이동단말은 재전송 공격을 방어하기 위해서 메시지의 생성시간 T_{Cur}와 디피-헬만 공개키 $y_{MN(i)}$를 함께 일방향 해쉬한 결과값 $m_{MN(i)}$를 생성하고, 초기 임의의 비밀값 $r_{MN(0)}$, $m_{MN(0)}$, $x_{MN(0)}$과 새롭게 생성된 $x_{MN(i)}$, $m_{MN(i)}$을 이용하여 충돌값 $r_{MN(i)}$를 식 (7)과 같이 계산한다. 이 충돌값 $r_{MN(i)}$는 초기 임의의 비밀값과 새롭게 생성된 디피-헬만 비밀키를 아는 사용자 본인만 생성이 가능하다.

$$m_{MN(i)} = h(y_{MN(i)} \| T_{Cur})$$
$$r_{MN(i)} = r_{MN(0)} + x_{MN(0)} m_{MN(0)} - x_{MN(i)} m_{MN(i)} \quad (7)$$

이동단말은 인증 및 키 교환을 위해서 생성한 정보인 $y_{MN(i)}$, T_{Cur}, $r_{MN(i)}$, $m_{MN(i)}$와 인증값 C_{MN}을 MIH 선행 인증 요청 메시지인 MIH_Pro_auth Request 메시지에 포함하여 핸드오버 대상 네트워크의 MIA-KH로 전송한다. 이때 MIH 선행 인증 메시지는 IEEE 802.21 보안 그룹에서 제안한 두

가지 모델과 같이 핸드오버 대상 네트워크의 MIA-KH로 직접적으로 전달할 수 있고, 현재 서비스 네트워크의 MIA-KH를 경유하여 간접적으로 전달할 수도 있다.

이동단말의 MIH 선행 인증 요청 메시지를 받은 MIA-KH는 메시지에 포함된 $r_{MN(i)}$, $m_{MN(i)}$을 변수로 하고 $y_{MN(i)}$를 카멜레온 해쉬 공개키로 하는 카멜레온 해쉬값을 계산하고, 이 값이 인증값에 포함된 카멜레온 해쉬값과 같은지 비교하여 이동단말을 인증한다. 우선 재전송 공격이 이루어졌는지 확인하기 위하여 식 (8)과 같이 이동단말의 디피-헬만 공개키 $y_{MN(i)}$와 메시지 생성 시간 T_{Cur}을 일방향 해쉬한 값이 $m_{MN(i)}$과 같은지 확인한다.

$$m_{MN(i)} = h(y_{MN(i)} \| T_{Cur}) \tag{8}$$

이후 MIA-KH는 식 (9)와 같이 수신한 메시지에 포함된 정보 $y_{MN(i)}$, $r_{MN(i)}$, $m_{MN(i)}$를 이용하여 카멜레온 해쉬값 $CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)})$를 계산하고, 식 (10)과 같이 인증값 C_{MN}를 인증서버의 공개키 PK^{+}_{AAA}로 검증하여 얻은 $CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)})$와 같은지 비교한다. 식 (11)과 같이 두 값이 같은 것을 확인하여 이동단말은 인증된다.

$$CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)}) = g^{r_{MN(i)}} g^{x_{MN(i)} m_{MN(i)}} \bmod p \tag{9}$$

$$Verify_{PK^{+}_{AAA}}(C_{MN}) \equiv (ID_{MN} \| CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)}) \| T_{Ex}) \tag{10}$$

$$CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)}) = CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)}) \tag{11}$$

정상적인 이동단말이 생성한 값인 $y_{MN(i)}$, T_{Cur}, $r_{MN(i)}$, $m_{MN(i)}$일 경우에만 계산된 카멜레온 해쉬값 $CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)})$이 인증값에 포함된 카멜레온 해쉬값 $CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)})$과 같은 것을 식 (12)에서 확인할 수 있다.

$$\begin{aligned} CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)}) &= g^{r_{MN(i)}} g^{x_{MN(i)} m_{MN(i)}} \bmod p \\ &= g^{r_{MN(0)} + x_{MN(0)} m_{MN(0)} - x_{MN(i)} m_{MN(i)}} g^{x_{MN(i)} m_{MN(i)}} \bmod p \\ &= g^{r_{MN(0)}} g^{x_{MN(0)} m_{MN(0)}} \bmod p \\ &= CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)}) \end{aligned} \tag{12}$$

이동단말을 인증하고 이동단말의 디피-헬만 공개키를 획득한 MIA-KH는 본인의 디피-헬만 비밀키 $x_{MIA-KH(i)}$, 공개키 $y_{MIA-KH(i)} = g^{x_{MIA-KH(i)}} \bmod p$를 생성한다. 이후 MIA-KH는 인증을 위한 정보들은 이동단말에서 수행했던 방법과 동일하게 생성한다. MIA-KH는 이렇게 생성한 $y_{MIA-KH(i)}$, T_{Cur}, $r_{MIA-KH(i)}$, $m_{MIA-KH(i)}$와 본인의 인증값 C_{MIA-KH}를 MIH 선행 인증 응답 메시지인 MIH_Pro_auth Response 메시지에 포함하여 이동단말로 전송한다. MIH 선행 인증 응답 메시지를 수신한 이동단말은 앞에서 설명한 방법과 동일하게 MIA-KH의 디피-헬만 공개키를 인증한다.

이렇게 상호 인증을 수행한 이동단말과 MIA-KH는 디피-헬만 알고리즘을 통해서 식 (13)과 같이 동일한 마스터키를 공유하게 된다.

$$\begin{aligned} MK_{MN(i)} &= (g^{x_{MIA-KH(i)}} \bmod p)^{x_{MN(i)}} \bmod p \\ MK_{MIA-KH(i)} &= (g^{x_{MN(i)}} \bmod p)^{x_{MIA-KH(i)}} \bmod p \\ \Rightarrow MK_{(i)} &= MK_{MN(i)} = MK_{MIA-KH(i)} \\ &= g^{x_{MN(i)} x_{MIA-KH(i)}} \bmod p \end{aligned} \tag{13}$$

이후 MIA-KH는 계층적 키를 $MK_{(i)}$로부터 생성하여 MSA-KH로 전달하고 이동단말도 동일한 계층적 키를 생성한다. 이동단말이 새로운 네트워크로 핸드오버하면 MSA-KH와 공유한 키를 이용하여 Security Association 프로토콜 절차를 수행하여 공유한 키의 확인 및 무선 구간 보호를 위한 새로운 키를 생성한다.

Ⅳ. 분 석

본 논문에서 제안하는 기법은 한번 할당받은 인증값을 이용해서 매번 새롭게 생성된 디피-헬만 공개키에 대한 인증을 제공하기 때문에 인증서버와의 인증절차를 줄일 수 있으며, 카멜레온 해쉬를 기반으로 하기 때문에 PKI 환경이 요구되지 않는다. 이처럼 제안 기법은 인증절차를 줄이고 PKI 환경을 요구하지 않기 때문에 기존 기법에 비해서 네트워크 혼잡도 및 통신비용을 감소시키는 효과를 가진다. 또한 제안 기법은 핸드오버 인증에 대한 기본적인 보안 요구사항을 만족하고, 기존 인증값 전달 방식의 인증 기법에서 제공하지 못하는 PFS/PBS와 같은 향상된 보안 서비스를 제공한다.

4.1 효율성 분석

제안 기법의 네트워크 혼잡도에 대한 효율성을 분석하기 위하여 인증 메시지에 대한 각 네트워크

표 3. 각 인증 기법의 통신비용 비교

구분	EAP-TLS [4]	EAP-Kerberos Ⅱ [5]	ERP [6]	PKI based [8]	The proposed scheme
T_{MN-SN}	10α	7α	2α	3α	2α
T_{SN-CN}	10β	7β	2β	2β	2β
T_{SN-AAA}	8γ	2γ	2γ	-	-
T_{Total}	$10\alpha+10\beta+8\gamma$	$7\alpha+7\beta+2\gamma$	$2\alpha+2\beta+2\gamma$	$3\alpha+2\beta$	$2\alpha+2\beta$

구간별 통신비용의 합으로 총 통신비용을 계산하고, 기존의 인증 기법과 비교한다. 이때 비교를 위한 인증 기법은 MIH 환경에 적용해서 이동단말과 핸드오버 대상 네트워크의 MIA-KH와 선행 인증을 수행하는 것으로 가정한다. 각 네트워크 구간별로 전송된 인증 메시지에 대한 통신비용을 이동단말과 현재 네트워크 (Serving Network, SN) 간 통신비용은 T_{MN-SN}, 현재 네트워크와 핸드오버 대상 네트워크 (Candidate Network, CN) 간 통신비용은 T_{SN-CN}, 핸드오버 대상 네트워크와 인증서버 간 통신비용은 T_{SN-AAA}라고 한다. 각 인증 기법의 전체 메시지에 대한 총 통신비용은 식 (14)와 같다.

$$T_{Total} = T_{MN-SN} + T_{SN-CN} + T_{CN-AAA} \quad (14)$$

단위 인증 메시지에 대한 각 구간별 통신비용 T_{MN-SN}, T_{SN-CN}, T_{SN-AAA}를 α, β, γ라고 할 때, 각 인증 기법들의 전체 인증 메시지에 대한 통신비용 T_{Total}은 표 3과 같다. (각 기법의 통신비용의 비교를 위한 인증 절차는 이동단말과 MIA-KH 간 인증 및 마스터키를 공유하는 절차까지로 정의한다.) 표 3과 같이 제안 기법이 기존 기법에 비해서 통신비용이 작은 것을 확인할 수 있다.

4.2 안전성 분석

본 논문에서 제안하는 기법은 다음과 같은 보안 요구사항을 만족한다. (본 절에서는 안전성 분석의 손쉬운 이해를 위해 수식을 일반화하여 설명한다.)

- 카멜레온 해쉬 비밀키 추측 공격

기존의 카멜레온 해쉬 함수는 동일한 카멜레온 해쉬 비밀키를 사용하기 때문에 최초 생성한 카멜레온 해쉬값 $CH_y(r_{(0)}, m_{(0)})$를 이용하여 이후의 메시지에 대한 인증을 반복적으로 수행한다면, 수집된 메시지를 통해서 카멜레온 해쉬 비밀키를 추측하는 공격이 가능하다. 공격자는 첫째 메시지에 포함된 $r_{(1)}$, $m_{(1)}$과 카멜레온 해쉬 공개키 y를 이용하여 카멜레온 해쉬값 $CH_y(r_{(1)}, m_{(1)})$을 계산하고, 둘째 메시지에 포함된 $r_{(2)}$, $m_{(2)}$와 카멜레온 해쉬 공개키 y를 이용하여 카멜레온 해쉬값 $CH_y(r_{(2)}, m_{(2)})$을 계산한 후, 두 해쉬값이 같다는 성질을 이용하여 식 (15)와 같은 과정으로 카멜레온 해쉬 비밀키 x를 추측해 낼 수 있다.

$$\begin{aligned} & CH_y(r_{(1)}, m_{(1)}) = CH_y(r_{(2)}, m_{(2)}) \\ & \Rightarrow \begin{cases} CH_y(r_{(1)}, m_{(1)}) = g^{r_{(1)}} y^{m_{(1)}} \bmod p \\ CH_y(r_{(2)}, m_{(2)}) = g^{r_{(2)}} y^{m_{(2)}} \bmod p \end{cases} \\ & \Rightarrow r_{(1)} + m_{(1)} x = r_{(2)} + m_{(2)} x \\ & \Rightarrow x = \frac{r_{(2)} - r_{(1)}}{m_{(1)} - m_{(2)}} \end{aligned} \quad (15)$$

제안 기법은 매번 새롭게 생성한 디피-헬만 비밀키를 카멜레온 해쉬 비밀키로 사용하기 때문에 메시지 수집에 의한 비밀키의 추측 공격은 식 (16)과 같이 $x_{(1)}$, $x_{(2)}$에 대한 이원일차방정식 문제가 되고, 따라서 카멜레온 해쉬 비밀키를 추측하기는 힘들다.

$$\begin{aligned} & CH_{y_{(1)}}(r_{(1)}, m_{(1)}) = CH_{y_{(2)}}(r_{(2)}, m_{(2)}) \\ & \Rightarrow \begin{cases} CH_{y_{(1)}}(r_{(1)}, m_{(1)}) = g^{r_{(1)}} g^{x_{(1)} m_{(1)}} \bmod p \\ CH_{y_{(2)}}(r_{(2)}, m_{(2)}) = g^{r_{(2)}} g^{x_{(2)} m_{(2)}} \bmod p \end{cases} \\ & \Rightarrow r_{(1)} + m_{(1)} x_{(1)} = r_{(2)} + m_{(2)} x_{(2)} \end{aligned} \quad (16)$$

또한 카멜레온 해쉬 및 디피-헬만 공개키는 비밀키의 이산 거듭제곱 (discrete exponentiation) 연산으로 생성되기 때문에 공개키로부터 비밀키를 추측하는 것은 일반 이산 로그 문제 (generalized discrete logarithm problem)가 되어 매우 어렵다. 따라서 제안 기법은 비밀키 추측 공격에 대해서 안전하다.

- PFS/PBS 제공

제안 기법에서는 송신자가 매번 새롭게 생성한

디피-헬만 공개키 $y_{(i)}$에 대한 유효한 충돌값 $r_{(i)}$ 및 해쉬값 $m_{(i)}$를 계산하여 인증 메시지에 인증요소로 포함하여 전송하고, 수신자는 수신한 인증요소를 변수로 하는 카멜레온 해쉬값 $CH_{y_{(i)}}(r_{(i)},m_{(i)})$와 인증값에 포함된 서명된 카멜레온 해쉬값 $CH_{y_{(0)}}(r_{(0)},m_{(0)})$를 비교하여 송신자의 디피-헬만 공개키 $y_{(i)}$를 인증 및 검증한다. 제안 기법은 이와 같은 인증된 디피-헬만 키 교환을 수행하여 매번 새로운 임의의 마스터키 $MK_{(i)}$를 생성하기 때문에 사용하던 마스터키가 노출되는 경우라도 이전의 통신내용 및 이후의 통신내용에 대해서 안전을 보장하는 완전한 전방향 및 역방향 비밀성을 제공한다.

• 중간자 공격

공격자는 이동단말과 MIA-KH 사이에서 디피-헬만 키 교환 알고리즘의 문제점인 중간자 공격을 시도할 수 있다. 그러나 제안 기법은 카멜레온 해쉬 기반의 인증값을 이용해서 디피-헬만 공개키에 대한 인증을 제공하기 때문에 중간자 공격으로부터 안전하다.

• 사용자 위장 공격

공격자는 임의의 사용자로 위장하기 위하여 인증 메시지 생성을 시도할 수 있다. 그러나 임의의 사용자의 인증값 생성을 위한 초기 비밀값 $r_{(0)}$, $m_{(0)}$, $x_{(0)}$를 알지 못하기 때문에 새롭게 생성한 디피-헬만 공개키 $x_{(i)}$의 유효한 충돌값 $r_{(i)}$ 생성을 위한 $r_{(0)}+x_{(0)}m_{(0)}-x_{(i)}m_{(i)}$의 계산이 불가능하다. 따라서 제안 기법은 사용자 위장 공격으로부터 안전하다.

• 재전송 공격

공격자는 이동단말의 인증 메시지를 수집한 후 재사용하여 거짓된 인증을 하는 재전송 공격을 시도할 수 있다. 그러나 제안 기법의 인증 메시지에는 메시지 생성 시간 T_{Cur}와 디피-헬만 공개키 $y_{(i)}$에 대한 일방향 해쉬한 결과 값 $m_{(i)}=h(y_{(i)}\|T_{Cur})$를 인증 요소로 포함하기 때문에 이러한 재전송 공격으로부터 안전하다.

• 강한 신원 확인

각 노드가 분배받은 인증값은 사용자의 신원정보인 노드의 ID와 카멜레온 해쉬값, 유효시간이 포함되며, 이 값들을 인증 서버의 개인키로 서명된 값이다. 노드가 매번 새롭게 생성한 디피-헬만 공개키 및 인증요소 $y_{(i)}$, T_{Cur}, $r_{(i)}$, $m_{(i)}$를 변수로하는 카멜레온 해쉬값 $CH_{y_{(i)}}(r_{(i)},m_{(i)})$와 노드의 인증값에 포함된 카멜레온 해쉬값 $CH_{y_{(0)}}(r_{(0)},m_{(0)})$를 비교함으로써 노드가 인증이 되며, 인증값이 해당 노드의 유효한 인증값인 것이 검증된다. 이렇게 검증된 노드의 인증값에는 사용자의 신원정보 ID가 포함되어 있기 때문에 제안 기법은 각 노드 간에 강한 신원 확인이 제공된다.

V. 결 론

본 논문에서는 매번 새롭게 생성된 디피-헬만 공개키에 대한 인증이 가능한 인증값을 이용해서 선행 인증을 수행하는 MIH 프로토콜을 제안하였다. 기존 기법인 EAP 기반의 인증 기술은 인증서버를 통한 인증 절차의 복잡성을 가지고 있으며, PKI 기반의 인증 기술은 인증서의 안전한 배포 및 인증서의 관리와 같은 문제점을 가지고 있다. 제안 기법은 인증서버 및 PKI 환경 구축 없이 카멜레온 해쉬 기반의 인증값을 이용하여 단말과 MIH 키 홀더 간에 선행 인증을 수행한다. 제안 기법은 핸드오버 과정에서 인증서버의 개입이 필요하지 않고 카멜레온 해쉬 기반의 인증된 디피-헬만 공개키 교환을 하기 때문에 인증 메시지 발생에 따른 통신비용을 감소시키고, 추가적으로 기본 보안 요구사항을 만족함과 동시에 마스터키에 대한 완전한 전방향 및 역방향 비밀성도 제공한다.

따라서 제안 기법은 PKI 구축이 어려운 실제 이기종 무선망이 혼재된 환경에 적용이 용이하고, 네트워크 통신비용을 줄임으로써 네트워크 혼잡도를 개선할 수 있기 때문에 끊김 없는 이동 서비스의 제공을 가능하게 한다.

참 고 문 헌

[1] IEEE Std 802.21TM-2008, IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover Services, January, 2009.

[2] IEEE 802.21a, "Proactive Authentication and MIH Security," 21-09-0102-03-0Sec, November, 2009. <https://mentor.ieee.org/802.21/documents>

[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, Extensible Authentication Protocol (EAP), IETF RFC 3748, June, 2004.

[4] IEEE Std 802.11iTM-2004, IEEE Standard for Information technology - Telecommunic- ations and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) speci- fications Amendment 6: Medium Access Control (MAC) Security Enhancements, July, 2004.

[5] S. Eum, and H. Choi, "EAP-Kerberos II: An Adaptation of Kerberos to EAP for Mutual Authentication," in Proc. ITST 2008, Oct., 2008.

[6] V. Narayanan, and L. Dondeti, EAP Extensions for EAP Re-authentication Protocol (ERP), IETF RFC 5296, August, 2008.

[7] J. Salowey, L. Dondeti, V. Narayanan, and M. Nakhjiri, Specification for the Drivation of Root Keys from an Extended Master Session Key (EMSK), IETF RFC 5295, August, 2008.

[8] H. Sun, Y. Lin, S. Chen, and Y. Shen, "Secure and Fast Handover Scheme Based on Pre-Authentication method for 802.16 / WiMAX Infrastructure Networks," in Proc. TENCON 2007, Oct., 2007.

[9] H. Krawczyk, and T. Rabin, "Chameleon Signatures," in Proc. NDSS 2000, pp.143-154, 2000.

[10] J. Choi, and S. Jung, "A Handover Authentication Using Credentials Based on Chameleon Hashing," IEEE Communications Letters, Vol.14, No.1, Jan., 2010.

[11] W. Diffie, and M. Hellman, "New Directions in Cryptograhpy," IEEE Transactions on Information Theory, Vol.22, No.6, pp.644-654, Nov., 1976.

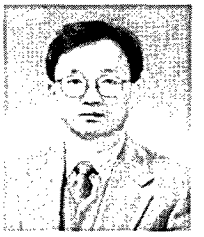
채 강 석(Kangsuk Chae) 준회원

2008년 2월 숭실대학교 정보통신전자공학부 학사
2010년 2월 숭실대학교 전자공학과 석사
2010년 3월~현재 숭실대학교 전자공학과 박사과정
<관심분야> 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안

최 재 덕(Jaeduck Choi) 정회원

2002년 2월 숭실대학교 정보통신전자공학부 학사
2004년 2월 숭실대학교 정보통신공학과 석사
2004년 1월~12월 (주)애드팍테크놀러지 S/W 연구원
2009년 2월 숭실대학교 전자공학과 박사
2009년 3월~2010년 1월 숭실대학교 전자공학과 박사후 연구원
2010년 2월~현재 ETRI 부설연구소 연구원
<관심분야> 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안

정 수 환(Souhwan Jung) 종신회원



1985년 2월 서울대학교 전자공학과 학사
1987년 2월 서울대학교 전자공학과 석사
1996년 6월 University of Washington 박사
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
2009년~현재 지식경제부 지식정보보안 PD
<관심분야> 이동 네트워크 보안, 차량 네트워크 보안, VoIP 보안, RFID/USN 보안