情報保護學會論文誌
第18卷 第2號, 2008. 4

일반화된 계층적 MIPv6 환경에서의 안전한 바인딩 업데이트 및 Fast Handover를 위한 인증 메커니즘*

강 현 선‡, 박 창 섭†
단국대학교

Authentication Mechanism for Secure Binding Update and Fast Handover in the Generalized Hierarchical MIPv6*

Hyun-sun Kang‡, Chang-seop Park†
Dankook University

요 약

본 논문에서는 일반화된 계층적 MIPv6 환경에서의 안전하고 효율적인 바인딩 업데이트 및 핸드오버 프로토콜을 제안한다. 기존의 계층적 MIPv6 환경에서의 바인딩 업데이트는 보편적으로 foreign network가 소규모 MAP 도메인으로 구성된다. 하지만, 제안 프로토콜에서는 다수의 MAP들이 계층적으로 구성되어지는 대규모 네트워크 환경에서의 안전하고 신속한 이동성 지원을 위한 메커니즘을 소개한다. 또한 다양한 공격 시나리오를 통해 제안 메커니즘의 안전성을 분석한다.

ABSTRACT

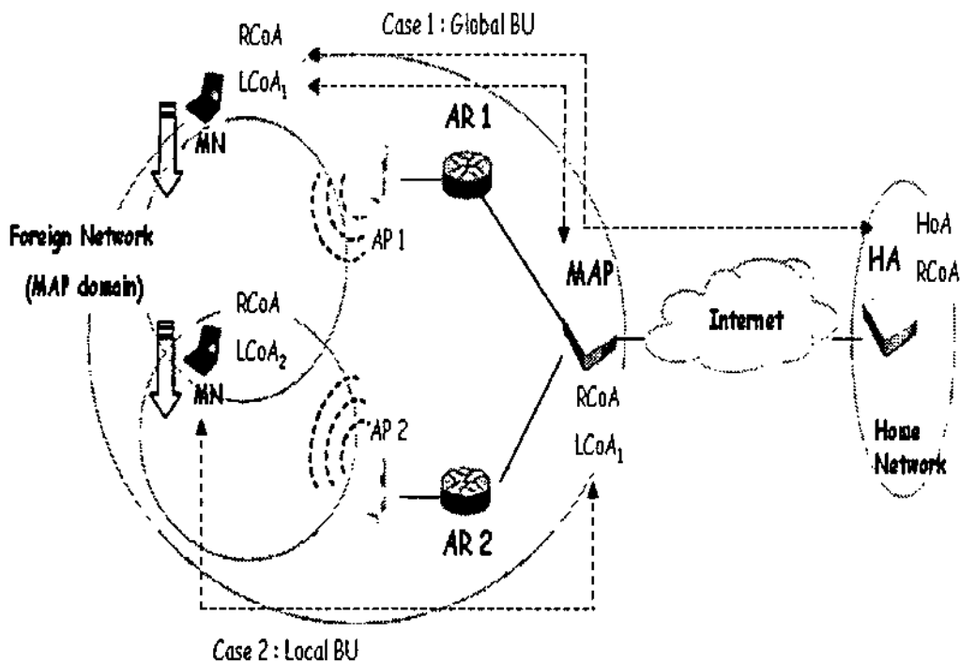
In this paper, a secure and efficient binding update protocol as well as a handover protocol are proposed in the generalized hierarchical MIPv6 environment. Contrary to the conventional hierarchical MIPv6 environment where a foreign network is a small-scaled MAP domain, a large-scaled MAP domain consisting of several MAPs which are connected hierarchically is considered in the proposed protocol for the mechanism to support fast and secure mobility. It is also analyzed the security of the proposed protocol under the various attack scenarios.

Keywords : *Hierarchical MIPv6, Fast handover, AAA server, Key management, binary tree*

Ⅰ. 서 론

Mobile IPv6(MIPv6)[1]에서는 두 개의 IPv6 주소를 통해서 모바일 노드(mobile node, MN)가 인터넷 상에서 자유롭게 이동할 수 있다. 그 중 하나는 MN의 홈 네트워크에서 정의된 고정된 HoA(home address)이고, 다른 하나는 MN이 외부 네트워크(foreign network)로 이동하였을 때, 사용하게 될 임시 주소인 CoA(care-of-address)이다. MN은 자신과 통신 중인 대응노드(correspondent node, CN)와 홈 에이전트(home agent, HA)에게 자신의 현재 위치를 알리기 위해 바인딩 업데이트(binding update, BU)메시지를 보내야 한다. 새로운 접속 라우터(access router, AR)로의 핸드오버가 수행될 때마다 발생하는 BU 메시지로 인한 지연은 패킷손실을 초래할 수 있으며, 이로 인해 네트워크 전체의 QoS(quality of serv-

접수일: 2007년 10월 28일; 채택일: 2007년 12월 28일
* 본 논문은 2006년도 정부재원으로 한국학술진흥재단의 지원을 받아 연구되었음 (KRF-2006-521-D00465).
† 주저자, csp0@dankook.ac.kr
‡ 교신저자, sshskang@dankook.ac.kr

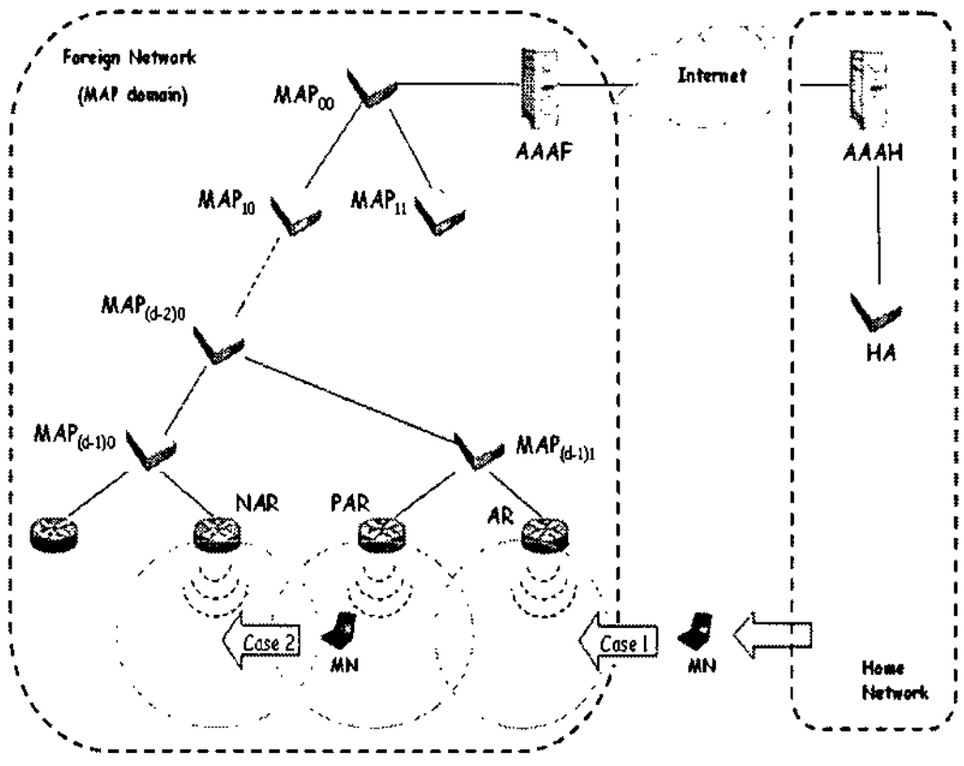


〔그림 1〕 HMIPv6 환경

ice)가 떨어질 수도 있다. Hierarchical Mobile IPv6(HMIPv6)[2]와 Fast Handover for MIPv6[3]는 BU 지연으로 인한 패킷 손실을 최소화하기 위해 제안되었다.

HMIPv6에서는 MIPv6에 새롭게 추가된 개체인 MAP(mobile anchor point)이 MN이 이동한 외부 네트워크에 대한 지역 HA 역할을 수행하며, 외부 네트워크에는 하나 또는 그 이상의 MAP이 존재할 수 있다. 새로운 MAP 도메인으로 진입하는 MN([그림 1]의 Case 1)은 AP(access point)를 통해서 AR이 광고하는 프리픽스(prefix) 정보를 기반으로 MAP 도메인 상의 임시 주소인 RCoA(regional CoA)와 링크 상의 임시 주소인 LCoA(link CoA, [그림 1]에서 LCoA1)를 설정한다. 자신의 새로운 주소를 홈 네트워크에 등록하기 위해서 MN은 HA에게 새로운 RCoA를 포함한 GBU(global BU) 메시지를 전송한다. 만약 MN이 MAP 도메인 내에서만 이동하여 RCoA는 변경되지 않고 단지 LCoA만 변경이 된다면, MN은 [그림 1]의 Case 2와 같이 새로운 LCoA를 MAP에 등록하여 자신이 이동한 후에도 서비스를 제공받기 위해 LBU(local BU) 메시지를 보내게 된다. 즉, MN이 같은 도메인 내에서 이동하는 경우에는 자신의 변경된 LCoA ([그림 1]에서 LCoA2)만을 MAP에게 등록하는 LBU를 이용한다면, MN이 이동 할 때마다 MAP을 거쳐 HA에게 MN의 이동 주소를 등록해야 하는 GBU로 인한 지연을 줄일 수 있게 된다. 하지만, LBU 역시 MN의 이동탐지(movement detection)와 MN이 이동한 후 새로운 CoA의 설정 등으로 인한 또 다른 형태의 지연을 초래할 수 있다. Fast Handover 기법은 LBU 동안 발생하는 지연을 감소시키기 위해 적용될 수 있으며, 4장에서 자세히 설명한다.

안전한 HMIPv6를 위해 LBU 메시지에는 인증 메커



〔그림 2〕 일반화된 HMIPv6 환경

니즘이 포함되어야 한다. 그렇지 않을 경우, 플러딩 공격, 리다이렉트 공격, DoS 공격 등이 발생할 수 있다.[4] 만약 공격자가 MN으로 향하는 패킷을 가로채기 위해 MN의 RCoA와 자신의 LCoA를 포함한 위조된 BU 메시지를 송신하는 경우, 해당 패킷은 공격자에게로 리다이렉트 될 것이다.

또한 수신을 원치 않는 또 다른 호스트로 대용량의 멀티미디어 패킷을 리다이렉트하여 플러딩을 이용한 DoS 공격을 유발시킬 수도 있다. 위와 같은 이유로 Fast Handover[5,6]기법에도 인증이 요구된다.

외부 네트워크의 MAP 도메인이 매우 클 경우, 그리고 오직 1개의 MAP만 존재할 경우에는 LBU에 따른 지연 역시 무시할 수 없는 요소이다. 따라서, 본 논문에서는 [그림 2]에서와 같은 대 규모의 외부 네트워크에 여러 개의 MAP들이 계층적으로 배치되어 있는 일반화된 HMIPv6 환경을 가정하여, 여기에서의 안전한 LBU 및 Fast Handover 기법을 고려하고 특히, 인증 메커니즘에 소요되는 일반화된 계층적 MAP 도메인에 적용 가능한 키 관리기법을 제안한다. 하지만 GBU는 별개의 주제이기 때문에 본 논문에서는 언급하지 않는다. 2장에서는 본 연구와 관련된 기존 연구를 살펴보고, 3장과 4장에서는 본 논문에서 제안하고 있는 프로토콜의 동작 원리를 그리고 5장에서는 안전성을 분석한다. 마지막으로 6장에서 결론을 제시한다.

Ⅱ. 관련연구

최근 IETF MIPSHOP(MIPv6 Signaling and Handoff Optimization) 워킹그룹에서는 HMIPv6 환경에서의

LBU 메시지에 대한 인증을 위해 CGA (Cryptographically-Generated Address)에 기반을 둔 인증 메커니즘과 관련된 2개의 draft[5,6]가 발표되었다. CGA에서는 MN의 공개키에 일방향 해쉬함수를 적용해 생성되는 64비트가 MN의 LCoA 및 RCoA의 IID(Interface IDentifier)로 구성된다. AR은 MN의 공개키를 통해서 세션키를 MN에게 암호화해서 전달하면, MN은 이 세션키를 LBU 메시지를 보호하기 위해서 사용한다는 개념이다. 하지만, 해당 프로토콜은 CGA의 부적절한 사용으로 인하여 DoS 공격에 노출되어진다[7].

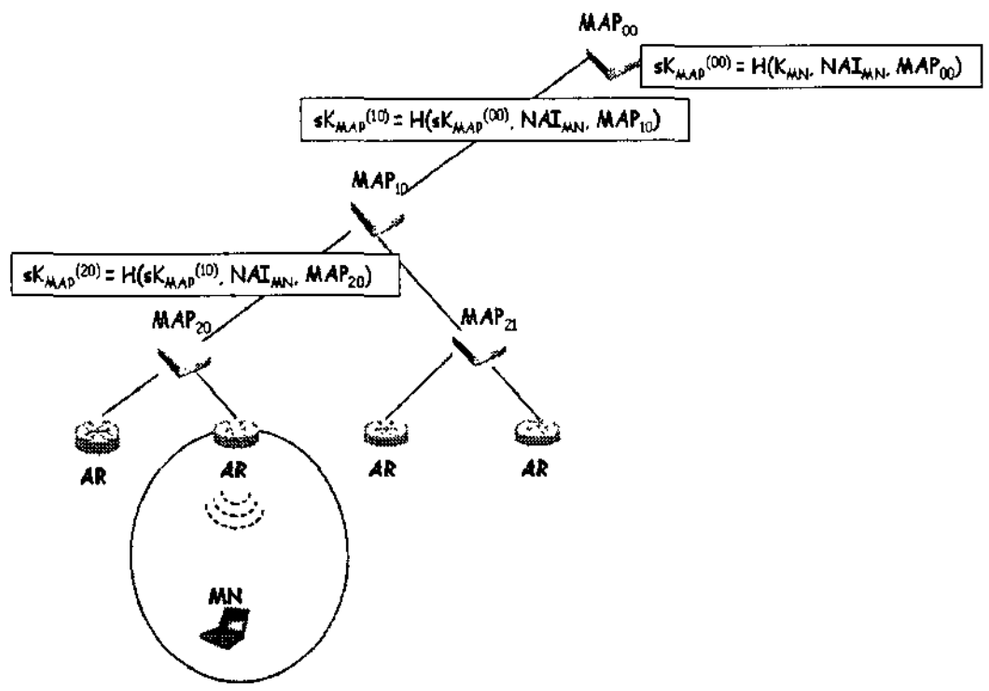
[8]에서는 AAA(Authentication, Authorization, and Accounting) 서버를 기반으로 하는 안전한 Fast Handover 방식을 제시하였다. 즉, MN은 PAR(MN이 이동하기 이전의 AR) 및 NAR(MN이 이동 후의 AR)과 여러 개의 메시지를 주고받아야 하는데, 이를 위해서 MN과 AAA가 사전에 공유하고 있는 비밀키를 기반으로 생성된 MN/PAR/NAR 간의 세션키가 사용된다는 원리이다. 하지만, 이 방식은 공격자가 MN과 NAR/PAR 간에 주고받는 여러 쌍의 메시지를 관측하면, 세션키를 모르고도 Fast Handover에 사용되는 메시지를 위조해낼 수 있다는 취약점을 가지고 있다[7]. [7]에서는 MAP이 1개 존재하는 외부 네트워크에서의 안전한 BU 및 Fast Handover 기법을 위한 인증 메커니즘을 Ticket 개념을 통해서 제시하였다. MN이 최초로 외부 네트워크에 진입할 경우, MAP은 MN의 AAA 서버와 접촉하여 MN이 MAP 도메인 내에서 사용할 세션키를 티켓 형태로 발급하여 MAP 도메인 내에서의 Handover 시에 사용하게 한다.

본 논문의 주제인 일반화된 HMIPv6 환경에서의 BU에 대한 연구는 양이 그리 많지 않고, 또한 일반화된 HMIPv6 환경에서의 인증 메커니즘과 관련한 논문은 저자들이 조사한 바에 의하면 전무한 상태이다. [9]는 HMIPv6 프로토콜의 성능향상을 위하여 micro-mobility 네트워크 내에서 MAP의 다 계층적 구조를 정의하여, IP 계층에서의 Handover 지연을 감소시키는 방안을 제시하였다. 새롭게 정의되는 multi-BU 메시지는 각각의 BU에 대한 확인 메시지 없이, MAP이 다음 계층 MAP 단계로 각각의 BU 메시지를 전달할 수 있게끔 하는 등록 메커니즘을 통하여 Handover를 가속화 시킨다. multi-BU 메시지에 대한 확인 메시지는 단지 마지막 계층의 MAP 또는 HA가 전송하게 함으로써 각각의 BU 메시지에 대한 확인 메시지를 수신하는 시간을 감소시킬 수 있다. [10]에서는 Cross-Over MAP 기반의 HMIPv6 (XMAP-HMIPv6)라는 환경을 기반으로 기존의 HMIPv6에서의 장점을 수용하고, 도메인 내에서의 이동시 신호처리 지연을 줄이는 방안을 제시하였다.

Ⅲ. MAP 등록 프로토콜

3.1 MAP 도메인의 구성과 기본적인 가정

일반적인 HMIPv6를 지원하는 네트워크에는 MAP과 다수의 AR로 구성된 MAP 도메인이 여러 개 존재할 수 있다. 제안 프로토콜에서는 MAP 도메인에 여러 개의 계층적인 하위 MAP 도메인들이 존재하며, MAP 도메인 내의 네트워크 토폴로지는 이진트리로 구성됨을 가정한다. 각 MAP의 고유번호는 [그림 2]에서 보는 바와 같이 최상위 MAP 고유번호 00을 기준으로 상위비트는 트리의 깊이와 일치하며, 하위비트는 좌측에 우선순위를 두어 하나씩 증가하는 규칙을 가지고 배열된다. MAP 도메인 내에 존재하는 모든 MAP과 AR은 자신이 포함된 네트워크 토폴로지에 대해 잘 알고 있으며, 도메인 내의 MAP간의 링크 및 MAP과 AR간의 링크에는 보안이 설정된 채널(secure channel)이 존재함을 가정한다. 제안 프로토콜에서는 안전한 바인딩 업데이트를 위해 AAA를 기반으로 한다. AAA 서버에는 홈 네트워크 서비스 제공자가 운영하는 AAAH와 외부 네트워크 서비스 제공자가 운영하는 AAAF가 있다. MN은 홈 네트워크 서비스 제공자에게 가입함으로써 AAAH와의 SA(security association)를 설정한다. 즉, AAAH에는 MN의 MIPv6와 관련한 파라미터인 HA (home agent address), HoA 등과 함께 대칭키 K_{MN}이



〔그림 3〕 일반화된 HMIPv6에서의 계층적 세션키 생성

저장된다. 또한 AAAH와 AAAF 간에는 로밍협약 체결 시 SA가 설정되어 서로 송수신되는 메시지를 보호할 수 있게 된다. 다음에서 ','은 연결을 나타내고, H( )는 일방향 해쉬함수, MAC(K)는 선행하는 모든 필드값을 대칭키 K로 계산한 MAC(message authentication code) 값을 나타낸다. 제안 프로토콜에서 네트워크 개체이름은 IPv6 주소를 지칭한다.

3.2 MAP 도메인 상의 계층적 세션키의 생성

MN이 외부 네트워크의 MAP 도메인에 진입할 경우 다음 절에서 언급할 MAP 등록(초기 LBU) 및 Fast Handover에 사용될 계층적 세션키가 생성된다. 즉, MN은 자신이 서비스를 받고 있는 최하위 MAP으로부터 최상위 MAP인 MAP_{00}에 이르는 경로에 존재하는 각각의 MAP과 공유하게 될 다음과 같은 세션키를 계산하고, 각각의 MAP은 상위 MAP으로부터 해당 세션키를 전달받게 된다. MAP_{ij}가 MN의 최하위 MAP일 경우,

$sK_{MAP}^{(00)} = H(K_{MN}, NAI_{MN}, MAP_{00})$
for $k = i$ to 1
  $sK_{MAP}^{(kj)} = H(sK_{MAP}^{(k-1,\lfloor j/2 \rfloor)}, NAI_{MN}, MAP_{kj})$;
  $j = \lfloor j / 2 \rfloor$;

MAP_{00}과 MN이 공유하게 될 $sK_{MAP}^{(00)} = H(K_{MN}, NAIMN, MAP_{00})$의 경우 MAP_{00}은 K_{MN}을 모르기 때문에 이를 직접 계산할 수가 없다. 따라서, MAP_{00}은 다음 절에서 설명하는 MAP 등록과정에서 AAA 서버를 경유해 전달받게 된다. [그림 3]의 경우, MN은 MAP_{00}, MAP_{10}, MAP_{20}과 각각 $sK_{MAP}^{(00)}$, $sK_{MAP}^{(10)}$, $sK_{MAP}^{(20)}$을 공유하게 된다. MN은 MAP의 중재를 통해서 AR과도 세션키를 공유할 수 있다. 즉, $sK_{MAP}^{(ij)}$을 MN과 MAP_{ij} 간에 공유된 세션키 그리고 AR이 MAP_{ij}에 속하는 경우에, MN과 AR간에 공유되는 세션키는 sKAR = $H(AR, sK_{MAP(ij)})$이다. 본 논문에서는 이를 "Fast Handover 키"로 명명하고 이 세션키의 용도는 4장에서 설명한다.

3.3 안전한 MAP 등록 프로토콜

[그림 2]의 Case 1과 같이 새로운 MAP 도메인으로 이동한 경우, MN은 현재 자신의 LCoA를 알리기 위한 목적의 MAP 등록 (초기 LBU) 프로토콜을 수행해야 한다. 그 과정은 다음과 같다.

(Step 1) AR ➡ MN : *Prefix*, MAP_{00}

새로운 MAP 도메인에 진입한 MN은 AR로부터 MAP 도메인의 프리픽스 정보와 최상위 MAP인 MAP_{00}의 IPv6 주소가 포함된 RtAdv(router advertisement) 메시지를 수신한다. 이때 MN은 RtAdv 메시지의 프리픽스 정보를 기반으로 *LCoA*와 *RCoA*를 설정하고, BU를 위한 파라미터, *BUpara = (H/M, TimestampMN, Lifetime)*를 준비한다. ***M***은 해당 BU 메시지가 MAP 등록을 위한 메시지임을 나타내기 위한 플래그(flag)이고, $Timestamp_{MN}$은 MN이 생성한 타임스탬프, *Lifetime*은 해당 바인딩의 만기까지 남은 시간을 나타낸다.

(Step 2) MN ➡ MAP_{00}
: *BUpara, Address,* $MAC(sK_{MAP}^{(00)})$

MN은 현재의 MAP 도메인에서의 최상위 MAP인 MAP_{00}에게 MAP 등록 (초기 LBU) 메시지를 전송한다. *BUpara*와는 별도로 등록 메시지에 *Address = (NAIMN, RCoA, LCoA)*가 포함된다. MN은 MAP_{00}과 공유하게 될 세션키 $sK_{MAP}^{(00)}$를 다음과 같이 계산한다.

$sK_{MAP}^{(00)} = H(KMN, NAIMN, MAP_{00})$

등록 메시지는 MAC에 의해서 보호되지만, MAP_{00}은 $sK_{MAP}^{(00)}$를 모르기 때문에 이 MAC 값을 당장 확인할 수는 없다. 따라서 MAP_{00}은 AAAF와 MN의 홈 네트워크상의 AAAH를 경유하여 $sK_{MAP}^{(00)}$를 전달받을 때까지 확인을 보류한다.

(Step 3) MAP_{00} ➡ AAAF ➡ AAAH
: NAI_{MN}, MAP_{00}, *TimestampMN*

앞서 설명한 바와 같이 MN과 MAP 간에는 사전에 설정된 SA가 없기 때문에, MAP_{00}은 MAC 값을 현 시점에서 확인하지 못한다. 따라서 MAP_{00}은 AAAF를 통해 AAAH에게 MAC 값을 확인할 세션키를 생성하여 전송할 것을 요청한다. AAAF와 AAAH는 이미 언급한 바와 같이 로밍협약에 따른 SA가 설정되어 있음을 가정한다.

Timestamp는 MN-Network간의 정확한 동기화를 필요로 하지 않으며, MN이 생성한 Timestamp는 MAP/AAA에 저장되어 있는 이전 MN의 Timestamp와 비교하는 목적이다. 즉, 현재 LBU에 포함된 $Timestamp_{MN}$이 MAP/AAA에 저장된 MN의 $Timestamp_{MN}$보다 최신의 것인지를 점검한다.

(Step 4) AAAH ➡ AAAF ➡ MAP_{00} : $sK_{MAP}^{(00)}$

AAAH는 NAI_{MN}을 기반으로 $sK_{MAP}^{(00)} = H(K_{MN}, NAI_{MN}, MAP_{00})$를 생성하여 AAAF를 경유, MAP_{00}에게 전송한다. MAP_{00}은 Step 2에서 MN으로부터 전달받은 *RCoA*에 대한 DAD(Duplicate Address Detection) 검사를 수행하고, 유보된 $MAC(sK_{MAP}^{(00)})$에 대한 확인 작업을 수행한다. 만약 모든 테스트에 성공하면, MAP_{00}은 MN의 *LCoA*주소, 세션키 그리고 $Timestamp_{MN}$을 포함하는 BCE(binding cache entry)를 생성한다.

(Step 5) MAP_{00} ➡ MN

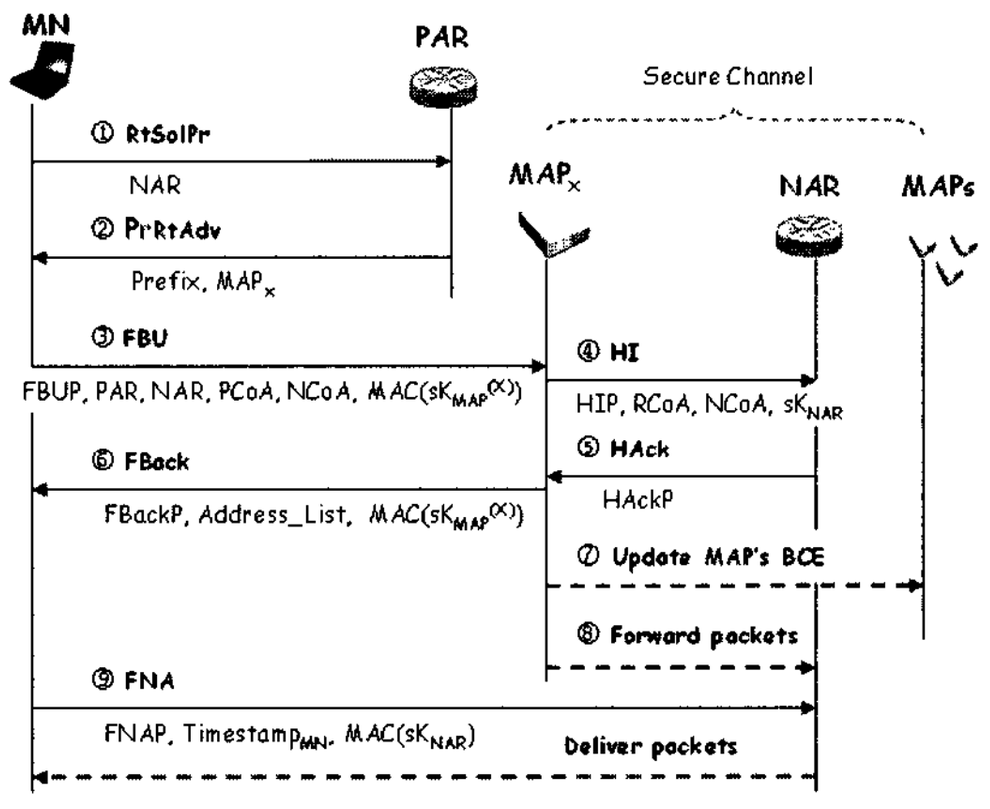
: *BApara, Address-List,* $MAC(sK_{MAP}^{(00)})$

MAP_{00}은 MN에게 *BApara=(Status,* $Timestamp_{MN}$, *Lifetime), Address-List,* $MAC(sK_{MAP}^{(00)})$으로 구성되는 LBA(local binding acknowledgement) 메시지를 전송한다. 이 메시지에 포함된 *Address-List*는 최상위 MAP으로부터 MN까지 도달하는 경로에 위치하는 모든 MAP들의 IPv6 주소 리스트 정보이다. MN은 이 정보를 기반으로 3.2 절의 설명과 같이 모든 MAP들과의 세션키를 계산할 수가 있다. 최상위 MAP으로부터 MN이 서비스를 받는 최하위 MAP까지의 경로에 있는 MAP들은 자신의 상위 MAP으로부터 MN과 공유할 세션키를 전달받는다. 이때, 각 MAP은 세션키를 포함한 MN의 BCE를 생성한다.

Ⅳ. 일반화된 HMIPv6에서의 안전한 Fast Handover

이번 장에서는 앞 절에서 언급한 MAP 등록 및 키 관리기법을 기반으로 일반화된 HMIPv6에서의 Fast Handover에 적용 가능한 인증기법을 소개한다. MN이 두 AR 사이를 이동할 때, IP 계층에서의 핸드오버 지연을 최소화하기 위해 Fast Handover 기법이 필요하게 된다.

본 논문에서 제안하고 있는 계층화된 MAP 환경에서



〔그림 4〕 일반화된 HMIPv6에서의 안전한 Fast Handover

는 [그림 2]의 Case 2와 같이 최상위 MAP 내에 위치한 다른 하위 MAP간의 핸드오버를 고려한다. NAR(new access router)은 MN의 핸드오버 이후의 라우터, PAR previous access router)은 핸드오버 이전의 라우터이다. MAPx는 MN이 다른 AR로 이동하여 핸드오버가 발생되는 경우 PAR과 NAR을 공통으로 포함하는 MAP 중 가장 하위단계에 위치하고 있는 MAP을 나타낸다. 이때, MAPx를 기점으로 MN이 이동전의 최하위 MAP까지에 존재하는 MN의 BCE를 삭제하는 대신에, MN이 이동 후의 새로운 최하위 MAP까지의 MAP들에 새로운 BCE를 생성하게 된다. 물론, 새로운 MAP과 공유할 세션키도 생성된다. [그림 2]의 Case 2 경우 MAPx = $MAP_{(d-2)0}$에는 MN이 MAP(d-1)0으로 이동한 정보가 갱신되고, $MAP_{(d-1)1}$에 있는 MN의 BCE는 삭제된다. 그리고 $MAP_{(d-1)0}$에 MN의 BCE가 새로이 생성된다.

일반화된 HMIPv6에서의 안전한 Fast Handover 기법은 [그림 4]를 기반으로 설명한다. MN이 PAR에 연결되어 있는 상태에서 이동을 시작하여 새로운 NAR을 발견한다고 가정하자. 이때, MN은 새로운 MAP으로 이동하였는지를 알 수가 없기 때문에 MN은 PAR에게 NAR이 새로운 MAP에 연결된 라우터인지를 문의하는 RtSolPr(router solicitation for proxy advertisement) 메시지 (①번 메시지)를 전송한다. PAR과 NAR은 동일 관리 도메인에 속해있는 라우터이기 때문에 PAR은 NAR에 대한 정보를 가지고 있다. 따라서, PAR은 PrRtAdv(router solicitation for proxy advertisement) 메시지 (②번 메시지) 전송을 통해서, MN이 진입한 NAR의 네트워크 프리픽스 정보 *Prefix*와 PAR과 NAR를 공통으로 포함하고 있는 최하위 MAP 정보인 MAP_X

를 MN에게 알려준다. MN은 *Prefix*를 기반으로 새로운 링크에서의 CoA인 *NCoA*를 구성하고, MAP_X와 이미 공유하고 있는 세션키 $sK_{MAP}^{(X)}$를 준비한다.

핸드오버의 발생이 예상된다면 MN은 PAR의 링크로부터 새롭게 이동된 MAP_X로 FBU(fast binding update) 메시지 (③번 메시지)를 전송한다. 이때, *FBUP* = (*H/M, TimestampMN, Lifetime*). *PCoA*는 MN의 이전 링크에서의 CoA를 나타낸다. MAP_X는 $MAC(sK_{MAP}^{(X)})$을 확인, FBUP 내의 $Timestamp_{MN}$을 검사한다. 만약 모든 검사에 성공한다면, MAP_X는 MN에 대한 타임스탬프를 갱신하고 *PCoA*도 *NCoA*로 대체한다.

MAP_X는 NAR로 HI(handover initiate) 메시지 (④번 메시지)를 전송한다. NAR은 *NCoA*가 링크 상에서 중복되는가에 대해 검사한다. 이미 MAP_X와 NAR간에 보안이 설정된 채널이 존재하기 때문에 인증을 위한 MAC 값을 포함하지 않아도 메시지의 무결성은 보장될 수 있으며, *HIP*는 HI 메시지 관련 파라미터(*HIP* = (*Code,* $Timestamp_{MAPx}$))이다. HI 메시지는 NAR에게 RCoA로 향하는 패킷을 링크상의 NCoA로 포워딩해 줄 것을 요청하기 위한 목적으로 사용된다. 또한, MAP_X는 NAR에게 "Fast Handover 키" sK_{NAR} = $H(NAR, sK_{MAP}^{(X)})$를 전송하는데, 이는 나중에 MN과 NAR간에 교환되는 메시지 보호를 위해 사용된다. NAR은 HI 메시지의 처리 결과를 HAck(handover acknowledgement) 메시지 (⑤번 메시지)를 통해 MAP_X에게 알린다. *HAckP* = (*Code,* $Timestamp_{MAPx}$)는 HAck 메시지와 관련된 파라미터이다.

MAP_X가 정상적인 HAck 메시지를 수신하면, MN에 대한 BCE에 *RCoA*와 *NCoA*간의 바인딩을 생성하고, MN에게 FBU 메시지의 처리결과를 알리기 위해 FBack (fast binding acknowledgement) 메시지 (⑥번 메시지)를 전송한다. *FBackP*=(*Status,* $Timestamp_{MN}$, *Lifetime*)는 FBack 메시지 관련 파라미터이다. 이때, MAP_X는 MN에게 MAP_X의 모든 하위 MAP들의 IPv6 정보가 포함된 *Address-List*를 전달함으로써, MN으로 하여금 하위 MAP들과 공유할 세션키를 생성하도록 한다. MAP_X는 ⑦번 메시지를 통해서 MAP_X로부터 MN의 PAR까지의 모든 하위 MAP들에 등록되어 있던 MN에 대한 BCE를 모두 삭제하고, MAP_X로부터 MN의 NAR까지의 모든 하위 MAP들이 MN의 LCoA 및 MN과 공유할 세션키를 포함하는 새로운 BCE를 생성하게 한다.

이 과정에서 만약 RCoA로 향하는 패킷이 MAP_X로 도착되었다면, 해당 패킷은 NAR로 전달되고 버퍼링 된다(⑧번 메시지). 최종적으로 MN이 새로운 링크로 완전히 이동하였을 경우, MN은 FNA(fast neighbor advertisement) 메시지 (⑨번 메시지)를 NAR로 전송하여 NAR에 버퍼링 되어 있는 패킷들을 MN에게 전달해 줄 것을 요청하게 된다. *FNAP* = (*Code*)는 FNA 메시지와 관련된 파라미터이며, FNA 메시지는 $MAC(sK_{NAR})$으로 보호된다.

V. 안전성 및 비교분석

5.1 RtAdv 메시지에 대한 위조공격

MAP 등록과정에서 MN은 AR로부터 Prefix 정보 및 최상위 MAP 주소정보를 제공받는다. 이 경우에, MN과 AR간에는 어떠한 SA도 공유가 되어 있지 않기 때문에 공격자에 의해서 위조된 정보가 MN에게 제공될 가능성이 있다. 첫째, MN은 위조된 Prefix 정보를 기반으로 RCoA/LCoA를 생성하여 정상적인 최상위 MAP에게 MAP 등록 메시지를 보낸다고 가정하자. 최상위 MAP은 RCoA/LCoA의 Prefix 정보가 유효하지 않을 경우에는 해당 메시지를 단순히 폐기하면 된다. 둘째, 위조된 최상위 MAP 주소정보가 제공될 경우, 비정상적인 최상위 MAP과 MN의 AAAH 간에는 정상적인 프로토콜이 진행될 수가 없다. 따라서, MAP과 MN 간에는 세션키가 공유될 수가 없고 결과적으로 MAP 등록 메시지에 포함될 유효한 MAC 값이 만들어질 수가 없기에, MN은 비정상적인 최상위 MAP이 전송하는 LBA 메시지를 폐기하면 된다.

5.2 MAP 등록 메시지에 대한 위조 및 재생공격

MN이 새로운 MAP 도메인으로 이동하였을 경우, MN은 새로운 주소를 포함한 MAP 등록 메시지를 해당 도메인의 최상위 MAP에게 전송한다. 인증과정이 전혀 수행되지 않는 일반적인 MAP 등록 프로토콜에서는 위조된 MAP 등록 메시지를 통해 리다이렉트 공격, 플러딩 공격 등의 DoS 공격이 발생할 수 있다. 만약 공격자가 MN의 RCoA와 함께 자신의 LCoA 또는 임의의 공격대상 호스트의 LCoA를 포함하여 위조된 MAP 등록 메시지를 최상위 MAP으로 전송한다고 가정하자. MN으로 향하는 모든 패킷은 공격자에게 리다이렉트 되거

나 수신을 원치 않는 또 다른 호스트로 리다이렉트 될 것이다. 이때 공격자가 대량의 멀티미디어 스트림의 수신을 위조된 MAP 등록 메시지를 통해 공격대상 호스트로 리다이렉트 한다면 해당 호스트에 대한 플러딩 공격도 쉽게 성공할 수 있게 된다. 하지만, 제안 프로토콜에서 MAP 등록 메시지는 MN과 최상위 MAP 간의 공유키 $sK_{MAP}^{(00)}$으로 계산한 MAC 값을 통해 인증 받는다. 따라서 MN과 MAP 간의 공유키를 모르는 공격자는 정당한 MAP 등록 메시지를 작성할 수 없게 된다. 또한 만약 공격자가 임의의 키를 사용하여 작성한 위조된 메시지를 송신한다면, 인증과정에서 실패하게 되므로 제안 프로토콜에서 위조된 MAP 등록 메시지로 인한 공격은 불가능하게 된다. 위조된 MAP 등록 메시지를 통한 DoS 공격의 경우, 공격자는 다수의 위조된 MAP 등록 메시지를 전송하여 프로토콜을 수행하는 동안 많은 계산량을 유도하게 된다. 하지만 제안 프로토콜에서는 인증을 위해 단지 한 번의 공유키를 통한 해쉬 계산만이 소요되므로 제안 프로토콜에서 DoS 공격은 유효하지 않다.

기본적인 HMIPv6에 대한 재생공격은 정당한 MN이 전송한 MAP 등록 메시지를 저장해 두었다가 일정시간이 지난 후 해당 메시지를 재생하여 MN의 이전 LCoA를 등록함으로써 MN이 서비스를 받지 못하도록 하는 공격이다. 제안 프로토콜에서는 LBU 메시지에 현재성을 검사하기 위한 $Timestamp_{MN}$를 포함하고 있기 때문에 재생공격에 대응할 수 있다. 만약 공격자가 정당한 MN의 MAP 등록 메시지를 저장하였다가 일정시간이 흐른 후 재생한다고 가정하자. 해당 메시지를 수신 받은 최상위 MAP은 BUP 내의 $Timestamp_{MN}$과 자신의 BCE 내에 저장되어 있는 이전의 Timestamp와의 비교를 통해서 현재성 검사를 수행하기 때문에 위와 같은 재생공격은 성공할 수 없게 된다. 순번(Sequence Number) 대신 Timestamp를 이용하게 된 동기는 순번의 "Rollover"문제와 MN/MAP/AAA 등에서 순번에 대한 기록이 오작동으로 인하여 삭제될 경우에 이를 복구하기 위한 추가의 조처가 필요하기 때문이다. 하지만 본 논문의 Timestamp는 MAP/AAA에 이미 저장되어 있는 Timestamp가 최근에 도착한 Timestamp보다 앞선 시간의 것이라는 보장만을 원하기 때문에, 양측 간의 시간에 대한 엄격한 동기화는 요구되지 않으며 또한 앞서 언급한 기계의 오작동 시 순번을 사용할 때 발생하는 추가 조처는 필요하지 않게 된다.

5.3 RtSolPr / PrRtAdv 메시지에 대한 위조공격

RtSolPr 및 PrRtAdv 메시지의 역할은 MN이 PAR에서 NAR로 이동하기 위한 선행 작업에 필요한 정보를 제공하는 데에 있다. 즉, MN은 NAR에서의 LCoA인 NCoA를 설정하고 PAR과 NAR을 공통으로 포함하는 최하위 MAP (MAP_X)에 대한 정보를 획득하게 된다. 비록 두 메시지에 대한 무결성 보장이 메시지 자체에는 포함되어 있지는 않지만, RtAdv 메시지에서처럼 정상적인 프로토콜의 동작을 저해하는 유효한 공격은 불가능하다. 만약 공격자가 PrRtAdv 메시지를 통해 정확하지 않은 MAP_X 정보를 MN에게 전달할 경우에 이는 FBU 메시지 처리과정에서 해결이 가능하다. FBU 메시지에는 NAR과 PAR이 포함되기 때문에 MAP_X는 자기 자신이 이 두 AR을 포함하는 가장 최하위 MAP인지에 대한 판단을 할 수 있기에, 만약 그렇지 않을 경우에는 해당 메시지를 폐기 하거나 오류 메시지로 응답을 할 수가 있게 된다.

5.4 FBU 메시지에 대한 위조 및 재생공격

Fast Handover 과정에서 MN의 FBU 요청을 받은 MAP_X는 NAR로 HI 메시지를 보내고 NAR로부터 HAck 메시지를 수신함으로써 MN의 패킷을 NAR로 전달하게 된다. 만약 MN과 PAR 간의 메시지에 대한 무결성이 보장되지 않는다고 가정하자. 공격자는 다수의 위조된 FBU 메시지를 PAR로 전송할 수 있으며, PAR은 해당 메시지를 NAR로 전달한다. NAR은 단지 DAD 테스트 후 HAck 메시지를 PAR로 전송할 것이다. 이 후 위조된 FBU 메시지에 포함된 주소로 전송되는 모든 트래픽이 NAR로 전달되며, 결국 NAR에 대한 플러딩 공격을 성공하게 된다. 하지만 제안 프로토콜에서 FBU 메시지는 MAP 등록과정에서 MN 그리고 PAR과 NAR을 공통으로 포함하는 MAP_X 간에 공유된 세션키 $sK_{MAP}^{(X)}$을 기반으로 계산한 MAC으로 인증 받는다. 따라서 MN과 MAP_X 간의 공유키를 모르는 공격자는 정당한 FBU 메시지를 작성할 수 없게 된다. 인증된 Fast Handover 기법이라도 정당한 MN이 송신한 FBU 메시지를 저장해 두었다가 일정시간이 지난 후 해당 메시지를 재생하는 재생공격에는 여전히 노출된다. 제안 프로토콜에서는 FBU 메시지에 현재성을 검사하기 위한 $Timestamp_{MN}$를 포함하고 있다. 따라서, 만약

공격자가 정당한 MN의 FBU 메시지를 저장하였다가 일정시간이 흐른 후 재생한다 해도 해당 메시지를 수신한 MAP_X은 FBUP 내의 $Timestamp_{MN}$와 BCE 내에 저장되어 있는 이전의 Timestamp의 비교를 통해서 현재성 검사를 수행하기 때문에 위와 같은 재생공격은 성공할 수 없게 된다.

5.5 FNA 메시지 보호를 위한 Fast Handover 키 사용

NAR이 HI(handover initiate) 메시지 (④번 메시지)를 수신하게 됨으로써 MN과 NAR간에는 세션키 (Fast Handover 키)가 공유된다. MN도 $sK_{NAR} = H(NAR, sK_{MAP}(X))$을 계산할 수 있다. 이 세션키는 MN이 NAR에 버퍼링된 패킷들을 전달해 달라고 NAR에게 요청하는 FNA 메시지 보호를 위해서 사용된다. 만약 이 메시지가 보호되지 않는다면 MN에게 전달될 패킷들이 의도되지 않은 목적지로 잘못 전달 될 수도 있게 된다.

5.6 성능평가 및 비교분석

HMIPv6 환경에서의 안전한 바인딩 업데이트 및 Fast Handover를 위해서 제안된 기법 중에서 CGA에 기반을 둔 [5, 6]은 공개키 암호화 및 디지털 서명이 사용되기 때문에 계산량 측면에 있어서 대칭형 암호 및 MAC 함수를 사용하는 [7, 8] 그리고 본 논문의 제안방식에 비해서는 비효율적이다. 특히, 이미 언급한 바와 같이 CGA에 기반을 둔 방식은 DoS 공격에 취약함이 입증되었다. MAP 등록 프로토콜에 수반되는 메시지 수의 경우에, [5, 7] 및 본 논문의 제안방식 모두 5개, Fast Handover에 수반되는 메시지 수는 [8]은 13개, [7]은 7개, 그리고 본 논문의 제안방식은 8개이다. 본 논문의 제안방식이 [7]에 비해서 교환되는 메시지 수가 1개가 더 많은 이유는 본 논문의 MAP 환경은 [7]에서 가정하는 MAP 환경을 일반화 시킨 환경이다. 즉, [7]에는 1개의 MAP만 존재하지만 본 논문에서는 계층화된 다수의 MAP이 존재하기 때문에 Fast Handover에 따라 영향을 받는 MAP에 BCE 갱신 메시지를 보내 주어야 하기 때문이다. 이 경우에 개별적인 갱신 메시지를 유니캐스트 방식으로 보내면 메시지 개수가 많아지기 때문에, 멀티캐스트 메시지로 보내면 메시지 개수를 1개로 제한할 수가 있게 된다. MN과 AR과의 SA 설정방식에 있어서 [5, 6]은 공개키 암호, [7]은 티켓 개념을 이용하였고, 본 논문에서는 Fast Handover 키의 개념을 제시하였다. 반면에, [8]에서는 MN과 AR간에는 이미 SA가 설정되어 있음을 가정하고 있다.

Ⅵ. 결론

본 논문에서는 일반화된 HMIPv6 환경에서의 안전한 바인딩 업데이트 및 Fast Handover를 지원하는 인증 메커니즘을 설계, 제안하였다. 특히, 대상이 되는 네트워크 환경에서는 외부 네트워크에 다수의 MAP들이 존재할 수 있는데, 최상위 MAP을 기점으로 하위 MAP들을 이진트리 방식으로 구성시켜서 MN이 다양한 MAP 세션키를 용이하게 공유할 수 있는 키 관리기법도 제안하였다. 본 연구의 기본적인 동기는 앞으로의 네트워크 환경은 다양화, 대형화되어짐에 따라서 다수의 MAP들이 존재하는 네트워크에서 MN에게 이동성 서비스를 제공할 수 있는 가능성이 높아진다는 사실에 기인한다. 본 논문에서 제안하는 방식이 이러한 대규모 네트워크 환경에서 MN에게 신속하고 안전한 이동성 서비스를 제공하기 위한 하나의 대안이 될 수도 있다고 판단된다.

참고문헌

[1] A. Jari, J. David B., P. Charles E., Mobility Support in IPv6, RFC 3775, 2004.

[2] B. Ludovic, C. Claude, M. Karim, S. Hesham, Hierarchical Mobile IPv6, RFC 4140, 2005.

[3] K. Rajeev, Fast Handovers for Mobile IPv6, RFC 4068, 2005.

[4] H. Kang, C. Park, MIPv6 Binding Update Protocol Secure Against Both Redirect and DoS Attacks. CISC, Lecture Notes in Computer Science, Vol.3822 of LNCS, Springer-Verlag, pp. 407-418, 2005.

[5] H. Wassim, K. Suresh, Combining Cryptographically Generated Address and Crypto-Based Identifiers to Secure HMIPv6, Internet Draft, draft-had-dad-mipshop-hmipv6-security-06, 2006.

[6] K. James, K. Rajeev, Bootstrapping a Symmetric IPv6 Handover Key from SEND, Internet Draft, draft-kempf-mobopts-handover-key-01.txt. 2005.

[7] 김민경, 강현선, 박창섭, HMIPv6 환경에서의 안

전한 Fast Handover를 위한 인증 메커니즘, 한국정보보호학회 논문지, 제17권, 제3호, pp.91-100, 2007. 6.

[8] C. Jaejuck, J. Souhwan, Access Authentication Protocol in FMIPv6, Internet Draft, draft-jung-mipshop-access-auth-00.txt,. 2006.

[9] S. Dmitry, X. Bangnan, H. Joachim, R. Veselin, On the Performance of Enhanced Hierarchical Mobile IPv6, IEEE 16th International Symposium on Personal, Indoor and Mobile Radio *Communications, 2005.*

[10] H. Mahtab, K. Kanchana, L. Klong, A Handover Management Scheme for Mobile IPv6 Networks, IEEE Computer Communications and Networks, 2005. ICCCN 2005. Proceedings, 2005.

〈著者紹介〉

강 현 선 (Hyun-Sun Kang) 학생회원

2002년 2월 : 단국대학교 전자계산학과 졸업
2004년 2월 : 단국대학교 전자계산학 석사
2007년 2월 : 단국대학교 전자계산학 박사
2007년 3월~현재 : 단국대학교 인재개발원 강의전임강사
<관심분야> 암호이론, 보안 프로토콜, IPv6

박 창 섭 (Chang-Seop Park) 종신회원

1983년 : 연세대학교 경제학과 졸업
1983년 : 한국 IBM 근무
1990년 : 미국 Lehigh Univ. 전자계산학 박사
1990년~현재 : 단국대학교 전자컴퓨터학부 교수
<관심분야> 네트워크 보안, 암호 프로토콜