Journal of Korea Multimedia Society Vol. 13, No. 2, February 2010(pp. 205-215)

IEEE 802.11 기반의 고속의 안전한 Mobile IPv6 핸드오프 메커니즘

강현선†, 박창섭††

요 약

802.11 기반의 환경에서 원활한 실시간 멀티미디어 서비스를 위해서는 신속하고 안전한 핸드오버가 반드시 제공되어야 한다. 본 논문에서는 802.11 WLAN 환경에서 L2 계층과 L3 계층을 통합한 FMIPv6 핸드오프 프로토콜을 제안한다. 해당 프로토콜에서는 핸드오버 메시지 보호를 위해 계층적 키 관리 기법 및 인증 메커니즘을 제안한다. 신속한 핸드오버를 위해서는 AAA와의 접속을 최소화한다. 또한 제안 프로토콜의 핸드오버 비용을 기존연구와 비교, 분석해 본다.

Fast and Secure Handoff Mechanism for Mobile IPv6 based on IEEE 802.11

Hyun Sun Kang†, Chang Seop Park††

ABSTRACT

It is necessary to provide a fast and secure handover for seamless real-time multimedia services based on IEEE 802.11. In this paper, we propose FMIPv6 handoff protocol integrating L2/L3 layer based on IEEE 802.11 WLAN environment. In that, we propose a hierarchical key management scheme and authentication mechanism for protecting the handover signaling messages. The number of connections with AAA server is minimized for the fast handover. It is also compared and analyzed the handover cost with previous method.

Key words: Handoff(핸드오프), FMIPv6(Fast Mobile IPv6), 802.11

1. 서 론

IEEE 802.11 기반의 WLAN (Wireless LAN)은 2000년도 초반에 지적된 보안상의 문제점 및 데이터 전송 속도문제를 해결하고 성숙단계에 진입했으며, 향후 WLAN 기반의 새로운 응용 서비스들의 등장을 예고하고 있다. 그림 1의 B와 같이 802.11 기반의 WLAN 환경에서 이동 노드(MN : Mobile Node)가 동일한 IP 서브넷 상의 인접한 AP(Access Point)로 이동할 경우 L2 핸드오버(Layer 2 handover)가 발생한다. 현재의 WLAN은 비록 무선이지만 인접한 AP 간에 끊김 없는 이동성 지원이 원활히 되고 있지는 않다. IEEE 802.11f[1] / 802.11i[2]에서 이러한 문제를 어느 정도 해결을 하였지만 VoIP 서비스와 같은 실시간 서비스가 WLAN 환경에서 제공되기 위해서는 단말기의 효율적이고 안전한 그리고 신속한 L2

※ 교신저자(Corresponding Author) : 강현선, 주소 : 충남 천안시 안서동 산29번지(330-714), 전화 : 041)550-3465, FAX : 041)550-3460, E-mail : sshskang@dankook.ac.kr
접수일 : 2009년 8월 6일, 수정일 : 2009년 10월 5일
완료일 : 2009년 10월 27일
† 정회원, 단국대학교 정보기술연구소 연구원
†† 정회원, 단국대학교 전자컴퓨터학부 교수
(E-mail : csp0@dankook.ac.kr)
※ 본 연구는 2008년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 수행되었음[KRF-2008-521-D00445].

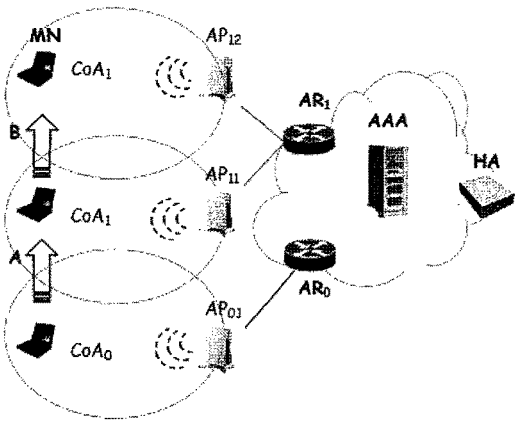

그림 1. 802.11 기반 WLAN 환경

핸드오버를 보장하는 기법이 보완되어야 한다.

반면, 그림 1의 A와 같이 이동 노드가 AR_0 (Access Router)을 기본 게이트웨이로 하는 IP 서브넷에서 AR_1의 IP 서브넷으로 이동할 경우에는 L3 핸드오버 (Layer 3 handover)가 발생한다. MIPv6 (Mobile IPv6)에서는 MN에게 부여되는 홈 네트워크에서의 홈 IP주소 그리고 외부 네트워크로 이동 후에 부여받는 CoA (Care-of Address) IP주소를 기반으로 L3 계층에서의 이동성을 지원하고 있다. 기본적인 MIPv6는 단지 MN의 위치변경에 따른 홈에이전트 (HA : Home Agent) 등록 및 상대노드 (CN : Corresponding Node)와 진행되는 세션을 유지하기 위한 경로 재설정만을 고려하고 있기 때문에, L2 계층에서와 마찬가지로 VoIP와 같은 실시간 서비스를 만족시킬 수준의 이동성 지원에는 한계가 있다. 이를 보완하기 위하여 IETF의 MIPSHOP (MIPv6 Signaling and Handoff Optimization) Working Group에서는 고속의 IPv6 핸드오버를 지원하기 위한 FMIPv6 (Fast MIPv6) [3] 표준안을 제정하였다. FMIPv6는 L2 계층으로부터 제공되는 정보를 이용하여 MN의 위치변경에 따른 신속한 네트워크 주소의 재설정을 통해 패킷 손실을 최소화하는 메커니즘이다.

신속한 핸드오버를 위해서는 L2 핸드오버 및 L3 핸드오버에 소요되는 지연이 최소화 되어야 하며, 결국 L2 및 L3 계층 간의 원활한 정보교환이 선행되어져야 한다. 최근에는 Infrastructure 모드로 운영되는 802.11 WLAN 기반의 MIPv6 및 FMIPv6에서의 핸드오버 지연을 최소화하기 위한 기법들[4-7]에 대한 연구가 진행되어지고 있다. 또한, L2 및 L3 개별 환경에서의 핸드오프 프로토콜이 다양한 보안공격의 가능성이 있기 때문에 L2에서의 핸드오버 메시지 보호 [7-10] 그리고 L3에서의 핸드오버 메시지 보호 [11-18]에 대한 연구 역시 진행되고 있다. 하지만 L2 핸드오버와 L3 핸드오버를 동시에 고려한 통합 환경에서의 핸드오버 메시지 보호에 대한 연구는 전무한 상태이다. 본 논문에서는 802.11 WLAN 기반의 FMIPv6 환경에서 L2 핸드오버와 L3 핸드오버에 소요되는 시그널링 메시지를 보호하기 위한 인증 메커니즘 그리고 통합된 키 관리 기법을 제안한다. 2장에서는 본 연구와 관련된 기존연구를 살펴보고, 3장에서는 제안 메커니즘의 동작원리를 설명한다. 4장에서는 제안 프로토콜을 분석하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 IEEE 802.11 WLAN에서의 인증 메커니즘과 L2 핸드오버

그림 2에서와 같이 MN은 "① Probing"과정을 통해 새로운 AP를 발견하고, 형식적인 "② Open Authentication" 과정을 수행한다. AP를 통한 네트워크 접속을 위해 "③ Association" 과정을 통해서 MN은 AP에 자신의 MAC(Medium Access Control) 주소를 등록, "④ 802.1x EAP-TLS Authentication" 과정에서는 인증서버 AS(Authentication Server)와

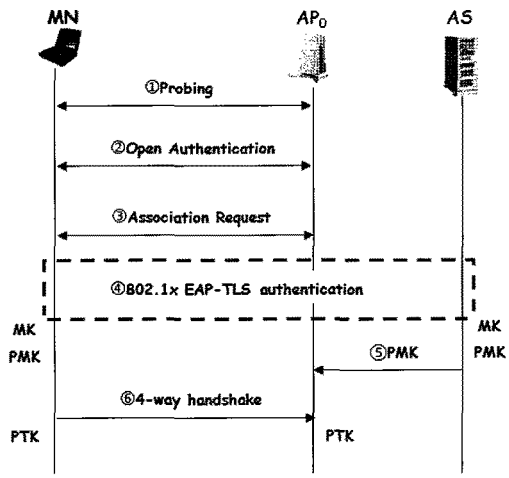

그림 2. 802.11 동작과정

802.1x 기반의 인증절차를 수행한다. 인증 과정을 통해 MN과 AS는 상호인증을 수행하고, MK(Master Key)를 생성한다. 생성된 MK를 기반으로 PMK (Pairwise Master Key)를 구성하고, "⑤ PMK"를 통해 AS는 PMK를 AP에게 안전하게 전달한다. PMK를 기반으로 MN과 AP는 "⑥ 4-way handshake" 과정을 수행하여 MN과 AP사이의 무선구간을 보호하기 위해 사용되는 세션키 PTK(Pairwise Transient Key)를 도출한다. 이러한 과정은 MN이 현재의 AP에서 새로운 AP로 이동할 때마다 반복적으로 수행하게 되는 절차인데, 이중에서 MN과 AS 사이에 수행되는 802.1x 기반의 인증절차에는 많은 시간이 소요된다. 또한 이로 인한 지연은 실시간 응용 환경에서는 심각한 문제점이 되고 있다.

AP간 핸드오버에 소요되는 인증 지연을 최소화하기 위해 기존에 제안된 다양한 기법들을 분석하면, 선인증(Pre-Authentication) 방식과[8,10] 사전 키분배(Proactive Key Distribution) 방식[1,7,9]로 분류된다. 선인증 방식은 MN이 현재의 AP에서 다른 AP로의 이동을 예상할 경우에 MN은 현재의 AP를 통해서 이동이 예상되는 AP와의 인증 작업을 미리 완료해 두는 기법을 의미한다. 물론 이 경우에 MN은 "현재 AP"그리고 "이동예상 AP"를 경유하여 AS와 새로운 802.1x 기반의 인증을 거치게 된다. 사전 키분배 방식은 MN이 특정 AP와의 Association과 Authentication이 완료되면 AS는 해당 AP와 인접해 있는 다른 AP들에게 MN이 그 AP로 이동시에 공유할 세션키를 미리 계산하여 분배시켜주는 개념이다. 따라서, AS는 자신이 관할하는 영역에 AP들이 어떻게 배치되어 있는지를 나타내는 Neighbor Graph [9]를 유지, 관리하고 있어야 한다. 위의 두 방식 모두 실제로 MN이 이동하게 될 AP 이외의 다른 AP들과 사전에 인증 작업을 불필요하게 수행하거나 또는 불필요한 세션키를 생성해서 전달해 주게 되는 단점을 내포하고 있다.

L2 계층에서의 신속한 핸드오버를 위해 IETF (Internet Engineering Task Force)에 의해 정의, 표준화된 프로토콜에는 CAPWAP, HOKEY 등이 있다 [19]. CAPWAP에서는 신속한 핸드오버를 위해 AP에서 발생하는 모든 핸드오버를 중앙의 AC(Access Controller)가 직접 처리한다. 즉, L2 핸드오버 발생시 MN은 AC와 직접 4-way handshake를 수행하고, 새로운 AP는 AC로부터 새로운 PTK를 제공받는다. 해당 프로토콜에서 AC는 해당 서브넷에서 발생하는 모든 핸드오버에 대한 정보를 유지, 관리해야하는 부담이 있으며 4-way handshake 수행으로 인해 상당한 오버헤드가 발생할 수 있다는 문제점을 안고 있다. HOKEY에서 MN은 초기 인증과정에서 생성한 키를 기반으로 AAA와의 단 한 번의 왕복 메시지로 새로운 AP와의 세션키를 생성한다. 해당 프로토콜은 802.11에 비해 AAA와의 송수신 메시지 수는 감소했지만, 핸드오버 시 AAA와의 접속으로 인해 지연이 발생한다는 문제는 여전히 남아있다.

2.2 FMIPv6에서의 L3 핸드오버 보호 메커니즘

MN이 새로운 IP 서브넷으로 이동할 경우 MN은 L2 계층으로부터 새로운 NAP(그림 1에서 AP_{11})에 대한 정보를 제공받는다. MN은 해당 정보를 기반으로 위치변경에 따른 신속한 L3 핸드오버를 위해 FMIPv6 절차를 수행한다. MN은 "❶ RtSolPr (Router Solicitation for Proxy)" 메시지를 통해 NAP가 연결되어 있는 라우터에 대한 정보를 요청하고, "❷ PrRtAdv(Proxy Router Advertisement)" 메시지를 통해 NAP가 연결되어 있는 새로운 NAR(그림 1에서 AR_1)에 대한 정보를 제공받는다. 이후 MN은 NAR에서 사용하게 될 새로운 네트워크 주소를 설정하고, 기존의 라우터 PAR(그림 1에서 AR_0)에게 새로운 주소로의 패킷 포워딩(forwarding)을 요청하기 위해 "❸ FBU (Fast Binding Update)" 메시지를 전송한다. PAR은 "❹ HI (Handover Initiate)" 메시지를 통해 NAR에게 MN의 핸드오버를 알리고, NAR은 "❺ HAck (Handover Acknowledge)" 메시지를 통해 HI 메시지에 응답한다. PAR은 FBU 메시지에 대한 응답으로 "❻ FBack (Fast Binding Acknowledgement)" 메시지를 MN과 NAR로 각각 전송하고, 이후 PAR로 수신되는 MN의 모든 패킷을 NAR로 포워딩한다. L2 핸드오버 절차를 완료한 MN은 NAR로의 접속을 알리기 위한 "❼ FNA (Fast Neighbor Advertisement)" 메시지를 전송하고, 해당 메시지를 수신한 NAR은 버퍼링된 패킷들을 MN으로 전송한다.

기능 및 역할상의 중요성에 비하여 FMIPv6 자체에는 보안적인 메커니즘이 전혀 내포되어 있지 않기 때문에 다양한 유형의 보안공격에 노출되어 있다. 기

본적으로 IPv6 네트워크가 지니고 있는 문제점[20] 뿐만 아니라, FMIPv6에 의해서 추가되는 기능에 기인한 취약점 때문에 가장 대표적으로 서비스 거부 공격에 노출되어진다. MN, PAR, NAR 간에 교환되는 메시지에 대한 인증기능이 포함되어 있지 않기 때문에 정상적인 MN의 L3 핸드오버를 방해하여 공격자가 MN으로 가장을 할 수 있으며, 네트워크에 과부하를 초래하는 공격이 가능하다. FMIPv6이 지니고 있는 이러한 문제점을 보완하기 위해서 [16]과 [17]에서는 AAA (Authentication, Authorization and Accounting) 기능을 도입하여 MN이 L3 핸드오버를 시행 할 때마다 AAA 서버와 접속하여 MN에 대한 인증을 수행하는 기법을 제안하고 있으나, 핸드오버 시 마다 AAA 서버와 인증작업을 수행하는 것은 역시 상당한 지연을 초래한다는 문제점을 안고 있다.

2.3 802.11 기반의 FMIPv6

이번 절에서는 802.11 WLAN 기반의 FMIPv6 환경에서 L2와 L3 핸드오버를 함께 고려한 기존기법 [21]을 소개한다. 해당 기법에서는 세 가지 핸드오버 시나리오를 제안하는데, 각 시나리오의 수행절차를 그림 2와 그림 3에서 사용한 메시지 번호를 사용하여 살펴보기로 한다. 첫 번째 시나리오는 FMIPv6의 Predictive 방식으로, ①❶❷❸❹❺❻②③④⑤⑥❼ 순서로 핸드오버가 수행된다. MN은 현재의 AP에 연결된 상태에서 L2 계층으로부터 제공되는 정보를

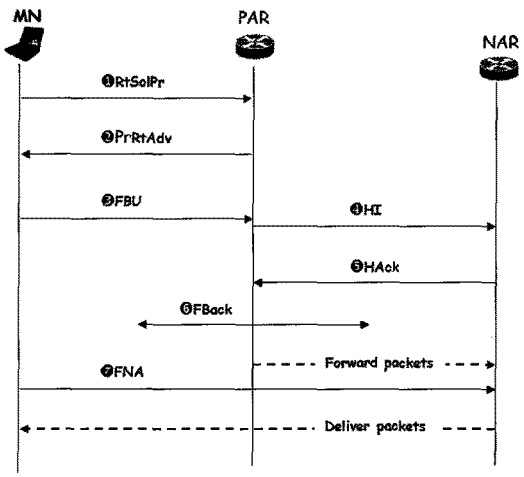

그림 3. FMIPv6 동작과정

이용하여 L3 핸드오버를 먼저 수행하고, 이어서 L2 핸드오버를 수행한다. 이 방식은 세 시나리오 중에서 핸드오버로 인한 패킷 손실을 최소화할 수 있는 시나리오이다. 두 번째와 세 번째 시나리오에서는 MN이 먼저 새로운 AP로 L2 핸드오버를 완료한 후에 L3 핸드오버를 수행한다. 두 번째 시나리오는 ❶❷①② ③④⑤⑥❸❹❺❻❼ 순서로 핸드오버를 수행한다. MN은 FMIPv6의 RtSolPr / PrRtAdv 메시지를 먼저 송수신하고 L2 핸드오버를 통해 새로운 AP에 접속한 후, 나머지 L3 핸드오버 절차를 수행한다. 세 번째 시나리오는 L2와 L3 핸드오버가 정확히 두 부분으로 나뉘어져 ①②③④⑤⑥❶❷❸❹❺❻❼ 순서로 각각 수행된다. 두 번째와 세 번째 방식은 L2 핸드오버를 완료한 후 L3 핸드오버를 수행하므로 L3 핸드오버를 수행하는 동안 패킷손실이 발생할 수도 있다는 문제점을 가지고 있다. 뿐만 아니라 앞서 설명한 모든 시나리오들은 L2와 L3 핸드오버를 함께 고려한 통합환경에서의 핸드오버 방식들이지만, 핸드오버 메시지 보호를 위한 인증 메커니즘은 전혀 제공되지 않는다.

3. 제안 메커니즘

3.1 네트워크 환경과 설계원리

본 논문은 802.11 기반의 FMIPv6 환경을 가정으로 한다. 즉, L2 계층은 802.11을 기반으로 하고, L3 프로토콜로는 FMIPv6이 사용되는 네트워크 환경을 말한다. 하나의 네트워크 도메인에는 그림 1과 같이 AAA 서버, AR, AP가 계층적으로 구성되어 있다. AAA 서버는 각 개체의 인증과 키 분배를 위해 사용되며, AP, AR 등의 네트워크 개체들과 각각 안전한 채널(secure channel)을 유지한다. 도메인 내에 존재하는 다수의 AR에는 각각 한 개 이상의 AP가 연결되어 있으며, 동일한 도메인 내의 모든 AR과 AR, 특정 AR과 AR에 연결되어 있는 AP 간에는 각각 안전한 채널이 유지됨을 가정한다. 본 논문에서 h( ) 는 일방향 해쉬함수를 나타내고, MAC(K)는 선행하는 메시지에 대해 공유키 K를 사용하여 계산한 MAC(Message Authentication Code) 값을 나타낸다. [M]K는 메시지 M을 키 K를 사용하여 암호화한 값을 나타낸다. NAI_A는 네트워크 개체 A의 NAI (Network Access Identifier)를 나타낸다.

본 논문에서는 독립적으로 수행되는 L2와 L3 핸

드오버를 통합하고, L2와 L3 계층 간의 통합된 키관리 기법을 사용한다. 즉, L2 계층에서 정보를 제공받아 L3 핸드오버에 사용하고, L3 계층의 키를 기반으로 L2 계층의 키를 유도함으로써 신속하고 안전한 핸드오버를 제공하게 된다. 제안 프로토콜에서는 L3 핸드오버 키와 L2 핸드오버 키가 사용된다. L3 핸드오버 키는 MN과 AR 간의 송수신 메시지 보호를 위해 사용되고, L2 핸드오버 키는 MN과 AP 간의 송수신 메시지 보호를 위해 사용된다. MN이 처음 네트워크로 접속할 경우, MN은 초기 프로토콜을 수행한다. 초기 프로토콜에서 MN은 AAA 서버와 접속하여 802.1x EAP-TLS 인증 과정을 수행하고, 이 과정에서 MK를 생성한다. MK는 해당 네트워크에서 MN과 AR, MN과 AP가 각각 공유하게 될 핸드오버 키를 생성하는데 사용된다. 본 논문의 계층적 키 관리와 관련한 사항은 4.1절에서 자세히 설명한다.

3.2 초기 프로토콜

MN이 처음으로 네트워크에 접속할 경우, MN은 초기 프로토콜을 수행한다. 초기 프로토콜에서 MN은 AP를 통해 네트워크에 접속하고, L3에서 사용하게 될 임시주소인 CoA를 설정, HA와 바인딩 업데이트(binding update) 프로토콜을 수행한다. 다음 그림 4는 초기 프로토콜의 동작과정을 나타낸다.

MN은 "① Probing" 과정을 통해 AP_{01}을 발견한다. 이때 MN은 AP_{01}과 AP_{01}이 연결되어 있는 라우터 AR_0에 대한 정보(IPv6 주소)를 함께 제공받는다. "② Open Authentication"과 "③ Association" 과정을 수행한 MN은 AAA 서버와 "④ 802.1x EAP-TLS Authentication" 과정을 수행한다. 이 과정에서 MN

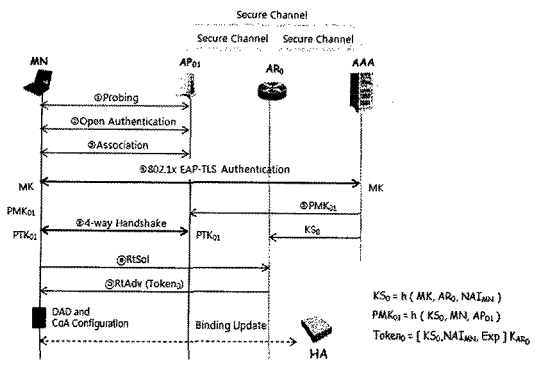

그림 4. 초기 프로토콜

은 AAA 서버와 상호인증을 수행하고, 마스터 키 MK를 생성한다. MN은 생성된 MK로부터 AR_0과 공유할 L3 핸드오버 키 $KS_0 = h(MK, AR_0, NAI_{MN})$를 생성하고, KS_0를 기반으로 AP_{01}과 공유할 L2 핸드오버 키 $PMK_{01} = h(KS_0, NAI_{MN}, AP_{01})$를 생성한다. 이와 동일한 방법으로 AAA 서버는 KS_0과 PMK_{01}을 생성하고, 안전한 채널을 통해 AR_0과 AP_{01}로 각각 전달한다. 이후 MN과 AP_{01}은 PMK_{01}을 기반으로 "⑥ 4-way handshake" 과정을 통해 송수신 데이터 암호화에 사용하게 될 세션키 PTK_{01}을 생성한다.

①~⑥ 단계를 거쳐 AP_{01}에 접속을 완료한 MN은 "ⓐ RtSol (Router Solicitation)" 메시지를 통해 라우터 광고를 요청한다. AR_0은 "ⓐ RtSol" 메시지의 응답으로 subnet prefix와 Token0이 포함된 "ⓑ RtAdv(Router Advertisement)" 메시지를 MN으로 전송한다. 여기서 $Token_0 = [KS_0, NAI_{MN}, Exp]K_{AR0}$은 차후 MN이 AR_0로의 송신 메시지 인증을 위해 사용하게 된다. MN은 제공된 subnet prefix를 기반으로 라우터 AR_0이 관할하는 서브넷에서 사용하게 될 새로운 주소 CoA를 DAD(Duplicate Address Detection) 과정을 거쳐 설정하고, HA와 바인딩 업데이트 프로토콜을 수행한다. 본 논문에서는 바인딩 업데이트 프로토콜에 대한 설명은 주제와 밀접한 관련이 없으므로 생략하기로 한다.

3.3 핸드오프 프로토콜

MN이 새로운 IP 서브넷으로 이동할 경우 MN은 핸드오프 프로토콜을 수행한다. 프로토콜의 수행절차는 ①❶❷❸❹❺❻②③⑥❼ 순서로, 수행절차에 사용된 번호는 각각 그림 2와 그림 3에서 사용된 메시지 번호를 나타낸다. MN은 현재의 AP에 연결된 상태에서 새로운 AP로부터 제공받은 정보를 이용하여 L3 핸드오버를 먼저 수행하고, 이어서 L2 핸드오버를 수행한다. 다음 그림 5는 핸드오프 프로토콜의 수행절차를 나타낸다.

그림 1에서 현재 AP_{01}에 연결되어 있는 상태에서 이동하기 시작한 MN은 먼저 "① Probing" 메시지를 통해 새로운 AP_{11}을 발견한다. MN은 신속한 L3 핸드오버를 위해 "❶ $RtSolPr(AP_{11}, Token_0, MAC(KS_0))$" 메시지를 AR_0으로 송신하여 AP_{11}이 연결되어 있는 라우터에 대한 정보를 요청한다. 메시지를 수신한 AR_0은 먼저 $Token_0$을 열어 KS_0을 구하고

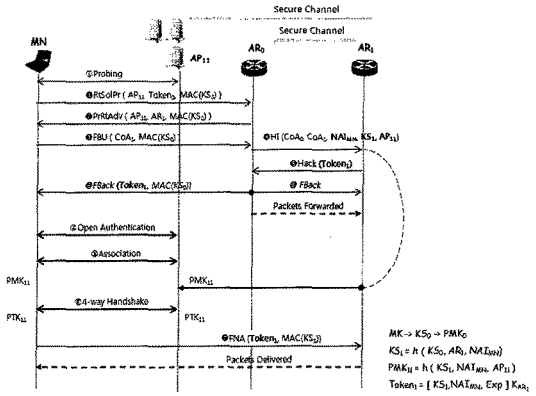

그림 5. 핸드오프 프로토콜

MAC 값을 확인한다. 확인에 성공한 AR_0은 "❷ PrRtAdv(AP_{11}, AR_1, MAC(KS_0))" 메시지를 MN으로 전송함으로써 라우터 AR_1에 대한 정보를 제공한다. 메시지를 수신하여 MAC 값을 확인한 MN은 AR_1에서 사용할 새로운 주소 CoA_1을 설정하고, AR_1과의 L3 핸드오버 키 $KS_1 = h(KS_0, AR_1, NAI_{MN})$를 생성, KS_1을 기반으로 AP_{11}과의 L2 핸드오버 키 $PMK_{11} = h(KS_1, NAI_{MN}, AP_{11})$를 생성한다. 이 후 MN은 AR_0으로 수신되는 모든 패킷을 새로운 주소로 포워딩을 요청하기 위한 "❸ FBU(CoA_1, MAC(KS_0))" 메시지를 전송한다. AR_0은 수신한 메시지의 MAC 값을 확인하고, MN과 동일한 방법으로 KS_1을 생성한다. 그리고 AR_1과의 안전한 채널을 통해 "❹ HI(CoA_0, CoA_1, NAI_{MN}, KS_1, AP_{11})" 메시지를 송신함으로써 MN의 핸드오버를 알린다. 메시지를 수신한 AR_1은 전달받은 KS_1을 기반으로 MN과 AP_{11} 간의 L2 핸드오버 키 $PMK_{11} = h(KS_1, NAI_{MN}, AP_{11})$를 생성, 안전한 채널을 통해 AP_{11}로 전송한다. 또한 AR_1은 "❺ HAck($Token_1$)" 메시지를 AR_0으로 송신한다. 여기에서 $Token_1$은 MN과의 송수신 메시지 보호를 위한 L3 핸드오버 키를 자신의 공개키로 암호화한 것으로, 해당 토큰은 "❸ FBU" 메시지에 대한 응답인 "❻ FBack($Token_1$, MAC(KS_0))" 메시지에 포함되어 MN으로 전송되며 차후 MN의 송신 메시지 인증에 사용된다. 이후 AR_0으로 수신되는 MN의 모든 패킷은 AR_1로 포워딩된다. AR_1의 서브넷으로 이동한 MN은 ②③⑥ 메시지를 통해 L2 핸드오버 절차를 완료하고 AR_1로 "❼ FNA($Token_1$, MAC(KS_1))" 메시지를 전송함으로써 AR_1로의 접속을 알린다. 메시지를 수신한 AR_1은 $Token_1$을 열어 KS_1을 구한 후, MAC 값을 확인하고, 버퍼링된 패킷들을 MN으로 전송한다. 본 논문의 핸드오프 프로토콜에서는 기존의 L2 핸드오버 절차에서 MN과 AAA 서버와의 802.1x를 통한 상호인증과정 및 세션키 생성과정(④,⑤)이 생략됨으로써 핸드오버에 소요되는 상당한 지연시간을 단축하게 된다.

4. 제안 프로토콜 분석

4.1 L2/L3 통합 환경에서의 계층적 키 관리

제안 프로토콜에서는 통합된 L2/L3 환경에서의 핸드오버 메시지 보호를 위해 계층적으로 키를 관리한다. 초기 프로토콜에서의 MK를 기반으로 L3 핸드오버 키를 생성하고, L3 핸드오버 키를 기반으로 L2 핸드오버 키를 생성하게 된다. MN은 L2/L3 핸드오버 키를 기반으로 L2/L3 핸드오버가 발생할 때마다 필요한 키를 다음의 그림 6과 같이 계층적으로 생성해서 사용한다.

본 논문의 계층적 키 관리의 마스터키인 MK는 초기 프로토콜(그림 4)의 "④ 802.1x EAP-TLS Authentication" 과정에서 생성된다. 생성된 MK는 "① Probing" 단계에서 AP_{01}로부터 제공받은 AR_0에 대한 정보와 함께 MN과 AR_0과의 L3 핸드오버 키 $KS_0 = h(MK, AR_0, NAI_{MN})$를 생성하는데 사용된다. MK를 기반으로 생성된 KS_0은 MN과 AR_0에 연결되

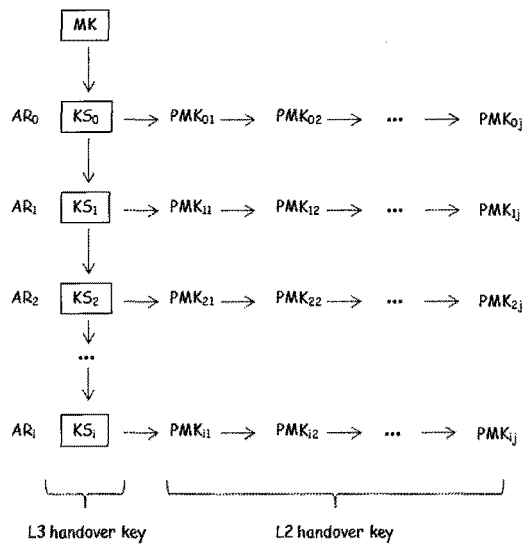

그림 6. 통합된 키 관리 및 키 생성과정

어 있는 AP_{01}과의 L2 핸드오버 키 PMK_{01} = h(KS_0, NAI_{MN}, AP_{01})를 생성하는데 사용된다. 일반적인 "① Probing" 단계에서는 AP_{01}에 대한 정보만을 제공한다. 하지만 제안 프로토콜에서는 KS_0 생성에 AR_0에 대한 정보가 필요하고, 실제 AP_{01}은 자신이 연결되어 있는 AR_0에 대한 정보를 알고 있으므로 "① Probing" 단계에서 미리 제공받음을 원칙으로 한다.

이 후, MN의 이동으로 L2/L3 핸드오버가 발생할 경우, KS_0과 PMK_{01}은 새로운 핸드오버 키를 생성하는데 사용된다. 예를 들면, 현재 AR_0에 연결되어 있는 AP_{01}과 접속 중인 MN이 AR_1로 이동하여 AP_{11}과 접속할 경우, MN은 KS_0을 기반으로 KS_1 = h(KS_0, AR_1, NAI_{MN})를 생성하고, KS_1을 기반으로 PMK_{11} = h(KS_1, NAI_{MN}, AP_{11})를 생성해서 사용하게 된다. 만약 MN이 또 다시 동일한 서브넷 AR_1에 연결된 새로운 AP_{12}로 이동할 경우, MN은 KS_1은 그대로 사용하고, KS_1을 기반으로 L2 핸드오버 키 PMK_{12} = h(KS_1, NAI_{MN}, AP_{12})를 생성하여 사용하게 된다. 즉, MN이 AR_0에서 순서대로 L3 핸드오버 하는 임의의 라우터를 AR_1, AR_2, …, AR_i로 가정할 때, L3 핸드오버 키 KS_1, KS_2, …, KS_i는 핸드오버 바로 이전에 사용 중이던 L3 핸드오버 키 KS_0, KS_1, …, KS_{i-1}을 기반으로 생성된다. 그리고 생성된 새로운 L3 핸드오버 키 KS_1, KS_2, …, KS_i를 기반으로 L2 핸드오버 키 PMK_{11}, PMK_{21}, …, PMK_{i1}을 생성한다. 또한 만약 MN이 동일한 서브넷(예를 들어, AR_1)에서 순서대로 L2 핸드오버 하는 임의의 AP를 AP_{12}, AP_{13}, …, AP_{1j}로 가정할 때, L2 핸드오버 키 PMK_{12}, PMK_{13}, …, PMK_{1j}는 핸드오버 바로 이전에 사용 중이던 L2 핸드오버 키 PMK_{11}, PMK_{12}, …, PMK_{1j-1}을 기반으로 생성된다. i는 순차적인 L3 핸드오버 순서이고, j는 각 핸드오버 이후에 발생하는 순차적인 L2 핸드오버 순서를 나타낸다.

$$KS_{i+1} = h(\ KS_i,\ AR_{i+1},\ NAI_{MN}\ ),\ i = 0, 1, 2, 3, \cdots$$
$$PMK_{ij} = h(\ KS_i,\ NAI_{MN},\ AP_{ij}\ ),\ j = 1, 2, 3, \cdots$$

제안 프로토콜에서는 AR의 L3 핸드오버 키의 저장 및 관리에 대한 부담을 없애기 위해 토큰(token)을 사용한다. 토큰은 인증을 위한 방법 중 하나로, 인증자로부터 분배받은 토큰을 차후 인증과정에서 제시함으로써 인증에 활용하는 방식을 말한다. 본 논문에서는 핸드오프 프로토콜에서 NAR에 의해 생성된 토큰이 MN으로 전달되고, 차후 발생하는 L3 핸드오버에서 MN의 메시지를 NAR이 인증하기 위한 목적으로 사용된다. 예를 들어 MN과 AR_i간의 L3 핸드오버 키가 KS_i라고 할 때, AR_i에 의해서 $Token_i$ = $[KS_i, NAI_{MN}, Exp]K_{AR}$이 생성되어 MN으로 전달된다. 차후 MN은 송신 메시지와 함께 해당 토큰을 제시함으로써 메시지 인증을 위해 토큰을 사용한다. 앞에서 Exp는 해당 토큰의 유효기간을 나타낸다.

4.2 안전성 분석

4.2.1 위조된 PrRtAdv 메시지 공격에의 대응

FMIPv6에서 PrRtAdv 메시지는 RtSolPr 메시지에 대한 응답으로, PAR은 MN이 새로운 서브넷으로 이동할 때 필요한 라우터에 대한 정보를 제공한다. MN은 제공받은 정보로 새로운 서브넷에서 사용할 주소를 생성, NAR로의 핸드오버를 수행한다. 이 때, 만약 공격자가 거짓의 서브넷 정보를 포함한 위조된 PrRtAdv 메시지를 MN으로 보낸다면 MN은 올바르지 않은 정보로 이후의 프로토콜을 계속 수행하고, 결국은 정상적인 핸드오버에 실패하게 될 것이다. 본 논문의 핸드오프 프로토콜에서는 MN과 PAR 간에는 미리 설정해 놓은 L3 핸드오버 키가 존재하고, 송수신 메시지는 해당키를 사용하여 계산한 MAC 값을 확인하는 인증과정을 거치게 된다. 즉, MN의 현재 라우터는 AR_n이고 AR_{n+1}로 이동한다고 할 때 MN이 AR_n으로부터 서브넷 정보를 포함한 PrRtAdv 메시지를 수신하면 가장 먼저 AR_n과의 L3 핸드오버 키 KS_n으로 MAC 값을 확인함으로써 유효성을 검사한다. 검사에 성공하면 나머지 프로토콜을 진행시키고 실패하면 해당 메시지를 무시한다. 해당 MAC 값은 MN과 AR_n과의 L3 핸드오버 키 KS_n을 모르면 생성할 수 없으므로 위조된 PrRtAdv 메시지를 통한 공격은 제안 프로토콜에서는 유효하지 않다.

4.2.2 위조된 FBU 메시지 공격에의 대응

FBU 메시지는 MN이 새로운 서브넷에서 사용하기 위해 생성한 주소에 대해 바인딩을 요청하기 위해 사용된다. FBU 메시지를 수신한 PAR은 HI 메시지를 통해 NAR에게 MN의 핸드오버를 알리고, 단지 NAR의 새로운 주소 확인과정만을 거친 후 PAR로 수신되는 MN의 모든 패킷을 NAR로 포워딩한다.

FBU 메시지에 대해 인증 메커니즘이 전혀 포함되어 있지 않다고 가정하자. MN을 가장한 공격자는 다수의 위조된 FBU 메시지를 PAR로 보낼 수 있으며, 결국 위조된 FBU 메시지에 포함되어 있는 주소로 전송되는 모든 패킷이 NAR로 포워딩됨으로써 NAR에 대한 플러딩(flooding) 공격이 성공하게 된다. 본 논문에서는 FBU 메시지는 MN과 PAR 간의 공유된 L3 핸드오버 키를 통하여 인증과정을 거친다. 즉, MN의 현재 라우터는 AR_n이고 AR_{n+1}로 이동한다고 할 때 AR_n으로 송신되는 FBU 메시지는 가장 먼저 MN과 AR_n과의 L3 핸드오버 키 KS_n으로 MAC 값을 통한 인증과정을 거친다. AR_n은 검사에 성공하면 나머지 프로토콜을 진행시키고 실패하면 해당 메시지를 무시한다. 해당 MAC 값은 MN과 AR_n과의 L3 핸드오버 키 KS_n을 모르면 생성할 수 없으므로 위조된 FBU 메시지를 통한 공격은 제안 프로토콜에서는 유효하지 않다.

4.3 비교 분석

4.3.1 비용분석 모델

본 논문에서는 제안 프로토콜의 이동성 분석모델로 육각 셀룰러 망 아키텍처를 사용한다. 해당 아키텍처는 가장 안쪽에 중심 셀이 있고, 중심셀을 둘러싼 ring들로 구성된다. 중심셀의 라벨은 0이고, 중심셀을 둘러싼 첫 번째 ring의 라벨은 1이고, 첫 번째 ring을 둘러싼 두 번째 ring의 라벨은 2로 나타낸다.

다음의 분석모델은 MN의 이동에 적당한 random-walk mobility 모델[22-25]과 1차원 마코프 체인(Markov chain) 모델을 기반으로 한다. 마코프 체인에서의 상태 r은 MN이 위치한 ring의 인덱스를 나타낸다. 즉, MN이 r에 위치한다는 것은 MN이 현재 r번째 ring의 임의의 셀에 위치함을 암시한다. 이 모델에서 MN의 다음 위치는 이전 위치에 임의의 분포에서 독립적으로 결정된 임의의 값을 더한 값과 같다. MN은 q의 확률을 가지고 현재 셀에 남아 있고, 1-q의 확률을 가지고 인접 셀로 이동한다고 가정하자. MN이 임의의 한 셀에 위치한다고 할 때, 중심셀로부터 거리가 증가/감소할 확률 $p^+(r)$, $p^-(r)$과 변이확률 $\alpha_{r,r+1}$, $\beta_{r,r-1}$은 다음과 같다.

$$p^+(r)=\frac{1}{3}+\frac{1}{6}r,\quad p^-(r)=\frac{1}{3}-\frac{1}{6}r$$

$$\alpha_{r,r+1}=(1-q),\quad if\, r=0\, then\,(1-q)(\frac{1}{3}+\frac{1}{6}r)$$

$$\beta_{r,r-1}=(1-q),\quad if\, r=0\, then\,(1-q)(\frac{1}{3}-\frac{1}{6}r)$$

R개의 ring으로 구성되어 있음을 가정할 때, $\pi_{r,R}$을 상태 r의 steady-state이라고 할 때, $\pi_{r,R}$은 변이확률을 이용하여 다음과 같이 나타낼 수 있다. 마코프 체인의 속성으로부터 steady-state 확률의 합은 1이며, 이를 기반으로 $\pi_{0,R}$은 다음과 같이 나타낼 수 있다.

$$\pi_{r,R}=\pi_{0,R}\prod_{i=0}^{r-1}\frac{\alpha_{i,i+1}}{\beta_{i+1,i}}\quad \text{for } 1\le r\le R$$

$$\pi_{0,R}=\frac{1}{1+\sum_{r=1}^{R}\prod_{i=0}^{r-1}\frac{\alpha_{i,i+1}}{\beta_{i+1,i}}}$$

본 논문에서는 성능분석을 위해 임의의 라우터가 R+1개의 ring (R>=1)으로 구성되었음을 가정으로 하며, 각 ring은 해당 라우터에 연결되어 있는 AP라고 가정한다. 만약 MN이 R+1번째 ring을 벗어나면 L3 핸드오버가 수행되고, R+1 ring의 안쪽에서 ring 간 이동이 발생하면 L2 핸드오버가 수행된다.

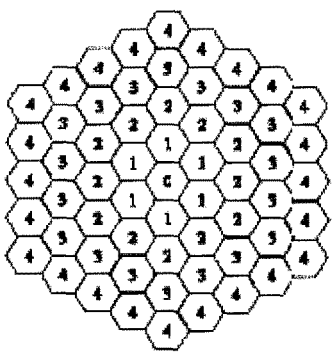

그림 7. 육각 셀룰러 망 아키텍처

4.3.2 비용분석

제안 프로토콜에서는 임의의 관리 도메인에 진입한 MN의 이동으로 인해 L2 또는 L3 핸드오버 프로토콜을 각각 수행한다. 이 때 L2 핸드오버 시 발생하는 비용 C_{L2}와 L3 핸드오버 시 발생하는 비용 C_{L3}는 그림 5 핸드오프 프로토콜에서의 각각의 메시지 전송비용과 각 노드에서의 처리비용으로 계산할 수 있다. 메시지의 전송비용은 유선과 무선으로 각각 구분할 수 있으며, 유선과 무선 링크에서의 전송비용을 T_w와 T_c라고 하고, 각 노드와 AAA 서버와의 전송비용을 T_a라고 하자. 각 노드에서의 키 생성 비용을 G_k,

해쉬계산 비용을 H_{shal}라고 하자. 이와 같을 때, 제안 프로토콜의 C_{L2}와 C_{L3}는 다음과 같이 나타낼 수 있다.

$$C_{L2} = 8T_w+2T_c+G_k$$
$$C_{L3} = 5(T_w+T_c)+3T_c+8T_w+G_k+10H_{shal}$$

다음 절에서는 제안 프로토콜과 기존연구[21]의 비용을 분석, 비교한다. [21]에서는 L2 핸드오버 시 802.11 기반의 인증과정을 수행하고, L3 핸드오버 시에는 FMIPv6 기반 핸드오버를 수행한다. 다음은 [21]의 핸드오버 비용 C_{L2}와 C_{L3}을 나타낸다.

$$C_{L2} = 4(T_w+T_a)+10T_w+T_a+G_k$$
$$C_{L3} = 4(T_w+T_a)+5(T_w+T_c)+3T_c+8T_w+T_a+G_k$$

random-walk mobility 분석모델에서 MN가 이동함에 따라 L3 핸드오버가 발생할 확률은 $\pi_{R,R} \cdot \alpha_{R,R+1}$ 이다. 만약 AR이 R ring으로 구성되고, MN이 R번째 ring에 위치한다면 MN은 L3 핸드오버를 수행하고, 그렇지 않은 경우는 L2 핸드오버를 수행한다. MN이 AP에 머무는 평균 셀 거주시간을 E라고 할 때, 단위 시간당 핸드오버 비용 C_{HC}은 다음과 같이 나타낼 수 있다.

$$C_{HC} = \frac{\pi_{R,R} \cdot \alpha_{R,R+1} \cdot C_{L3} + (1-\pi_{R,R} \cdot \alpha_{R,R+1}) C_{L2}}{E}$$

4.3.3 분석결과

이번 절에서는 random-walk mobility 모델을 기반으로 한 비용분석에 대한 수치적 결과를 제시하고, MN의 이동확률, 평균 AP 거주시간, AR의 크기와 핸드오버 비용과의 연관성을 살펴본다. 일반적으로 네트워크 분석에서 많이 적용되는 실제 파라미터 상수를 다음과 같이 정의하여 사용한다. 전송비용을 위한 유·무선에서의 전송비용과 AAA로의 전송비용을 각각 T_c=5ms, T_w=15ms, T_a=20ms를 사용[19]한다. 암호학적인 계산에서 발생하는 처리비용은 Bosselaers[26]의 결과에 따르면 G_k,=6μs, H_{shal}=3μs으로 매우 경미하다. 따라서 본 논문에서의 핸드오버 시 발생하는 비용 C_{L2}와 C_{L3} 계산에서 제외하기로 한다. 상수로 사용되는 기본값으로는 E=100ms, q=0.2, R=4로 사용한다.

다음 그래프는 random-walk mobility 모델에서 q, R, T 값의 변화에 따른 핸드오버 비용의 결과를 나타낸다. 그림 8에서 (a)는 random-walk 모델에서

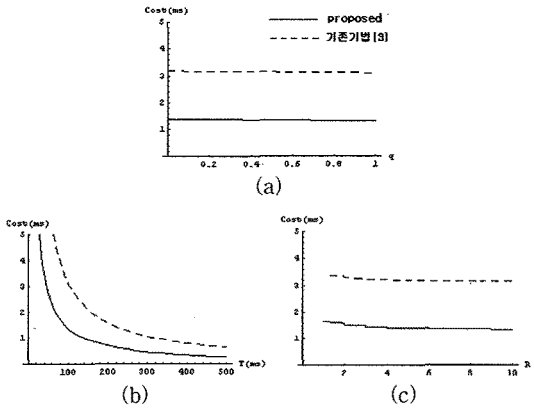

그림 8. 핸드오버 비용 결과비교

MN의 이동확률에 따른 비용을 나타내고, (c)는 R의 크기에 따른 비용을 나타낸다. q와 R의 크기는 핸드오버 비용에 그다지 큰 영향을 주지 않음을 알 수 있다. (b)는 MN의 셀 유지 시간에 따른 비용을 나타낸다. MN의 셀 유지시간이 증가할수록 MN의 핸드오버 비용이 크게 감소함을 볼 수 있다. 그래프에서 볼 수 있듯이 L2에서는 인증과정을 수행하지만 L3에서는 인증과정을 지원하지 않는 기존기법[21]에 비해 제안기법이 핸드오버 비용이 적음을 알 수 있다.

5. 결 론

본 논문에서는 802.11 WLAN 환경에서 L2 계층과 L3 계층을 통합한 FMIPv6 핸드오프 프로토콜에 적용 가능한 키 관리 및 인증 메커니즘을 제안하였다. 제안 프로토콜의 키관리 기법은 L2 계층에서의 마스터키를 기반으로 안전한 L3 핸드오버에 사용되는 키와 L2 핸드오버에 사용되는 키를 생성하고, 생성된 키를 사용하여 핸드오버 메시지를 보호하는 인증 메커니즘을 포함시킴으로써 안전한 핸드오버를 수행한다. 또한 인증 메커니즘으로 인한 지연을 최소화하기 위해 MAC을 이용하였고, AAA 서버와의 접속을 최소화하였다. 따라서 제안 프로토콜은 802.11 기반의 실시간 응용 서비스 환경에 적합할 것으로 사료된다.

참 고 문 헌

[1] IEEE Std 802.11f, IEEE Trial-Use Recommended Practice for Multi-Vendor Access

Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. 2003.

[2] IEEE Std 802.11i, IEEE Standard for Wireless LAN Medium Access Control and Physical Layer Specifications (Amendment 6: Medium Access Control Security Enhancements), 2004

[3] R. Koodli, "Fast Handovers for Mobile IPv6," RFC 4068, 2005.

[4] J. Xie and I. Shibeika, "IEEE 802.11-based Mobile IP Fast Handoff Latency Analysis," Proc. of IEEE ICC 2007, Dec. 2007.

[5] S. Mohanty and I. F. Akyildiz, "A cross-layer handoff management protocol for next generation wireless systems," *IEEE Trans. Mobile Computing*, Vol.5, No.10, pp. 1347-1360, Oc. 2006.

[6] D. Su and S.-J. Yoo, "Fast handover failure-case analysis in hierarchical Mobile IPv6 networks," *IEICE Trans. Communications*, Vol.E89-B, No.6, pp.1892-1895, June 2006.

[7] A. Mishra, M.H. Shin, N.L. Petroni Jr., T.C. Clancy, and W.A. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs," *IEEE Wireless Comm.*, Vol.11, No.1, pp. 26-36, Feb. 2004.

[8] S. Pack and Y. Choi, "Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN," *IEEE Networks*, pp. 15-26, Aug. 2002.

[9] A.Mishra M. Shin and W. Arbaugh, "Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network," IEEE INFOCOM conference, Hong Kong, Mar. 2004.

[10] S. Pack and Y. Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model," IFIP TC6 Personal Wireless Communications, pp. 175-182, Oct. 2002.

[11] J. Kempf and R. Koodli, "Bootstrapping a Symmetric IPv6 Handover Key from SEND," draft-kempf-mobopts-handover-key-01, 2005.

[12] H.S. Kang and C.S. 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.

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

[14] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents," RFC 3776, June 2004.

[15] G. O'Shea and M. Roe, "Child-proof Authentication for MIPv6," *ACM Computer Communications Review*, 31 (2), pp. 4-8, July 2001.

[16] V. Narayanan, "Handover Keys Using AAA," *draft-vidya-mipshop-handover-keys-aaa-01*, 2005.

[17] S. Jung, "Access Authentication Protocol in FMIP6,"*draft-mipshop-access-auth-00*, 2006.

[18] M. Nakhjiril, "A Keying hierarchy for managing Wireless Handover security," *draft-nakhjiri-hokey-hierachy-01*, 2006.

[19] T. Charles "Secure Handover in Enterprise WLANs:CAPWAP, HOKEY, and IEEE 802.11r," *IEEE Wireless Communication*, pp. 80-85. Oct. 2008.

[20] P. Nickander, "IPv6 Neighbor Discovery Trust Models and Threats," RFC 3756, 2004.

[21] P. McCann, "Mobile IPv6 Fast Handovers for 802.11 Networks," RFC 4260, 2005.

[22] Ian F., Akyildiz, Joseph, S.H. "Mobile user location update and paging under delay constraints," *ACM-Baltzer J. Wireless Networks*, Vol.1, pp. 413-425, Dec. 1995.

[23] Yi-Bing, Lin "Reducing location update cost in a PCS network," *IEEE/ACM Trans.*

Networking, Vol.5, pp. 25-33, Feb. 1997.

[24] Ian F., Akyildiz, Wenye, W. "A dynamic location management scheme for next-generation multitier PCS systems," *IEEE Trans. Wireless Commu.*, Vol.1, No.1, pp. 178-189, Jan. 2002.

[25] Sangheon, P., Yanghee, C. "A study on performance of hierarchical mobile IPv6 in IP-based cellular networks," *IEICE Trans. Commun.*, Vol.E87-B, No.3, pp. 462-469, Mar. 2004.

[26] Antoon, B., Ren, G., Joos, V. "Fast hashing on the Pentium," In N. Koblitz, editor, Advances in cryptology, Proceedings Crypto'96, Springer. Vol.1109, pp. 298-312. 1996.

강 현 선

2002년 단국대학교 전자계산학과 학사
2004년 단국대학교 전자계산학 석사
2007년 단국대학교 전자계산학 박사
2009년 단국대학교 인재개발원 강의전임
2009년~현재 단국대학교 정보기술연구소 연구원
관심분야 : 암호학, 프로토콜 보안

박 창 섭

1983년 연세대학교 경제학과 졸업
1983년 한국 IBM 근무
1990년 미국 Lehigh Univ. 전자계산학 박사
1990년~현재 단국대학교 전자컴퓨터학부 교수
관심분야 : 부호이론, 암호학