IP기반의 차세대 무선네트워크에서 끊김없는 이동성지원을 위한 인증기법

한동수* 안성진* 정종필*
*성균관대학교 정보통신대학원 컴퓨터공학과
e-mail: sijac00@naver.com

Authentication Scheme for Seamless Mobility Support in IP-Based Next-Generation Wireless Networks

Dongsu Han* Seong-Jin Ahn* Jongpil Jeong*
*Graduate School of Information and Communications,
Sungkyunkwan University

요 약

최근 스마트폰의 보급에 따라 이동통신에서의 무선 데이터망에 대한 수요가 늘어남에 따라서 이를 보완하기 위해서 무선 사업자들은 WiFi와 같은 대체 통신 인프라를 늘려 나가고 있다. 향후 4G라고 불리는 NGN에서는 음성을 비롯한 모든 정보들이 IP망에서 동작하게 될 것이다. 이러한 3G망과 GSM 그리고 WiFi, Wibro 등이 복합적으로 구성되어 있는 IP 네트워크에서 사용자로 하여금 끊김없는 서비스를 유지하려면 각 망간의 수평이동이 원활하게 되어야 하며 이를 위한 다양한 연구가 진행되어 왔다. 본 논문에서는 빠른 핸드오프 성능을 높일 수 있는 인증 개념을 도입하고자 한다. 인증하는 시간을 줄임으로서 끊김없는 서비스를 지원하는데 많은 도움이 될 것이다.

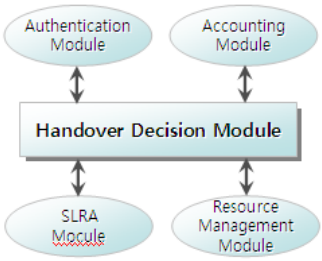
1. 서론

4세대/차세대 무선 네트워크(4G/NGWN)는 여러 가지 형태의 무선 접근 서비스들이 혼합된 형태로 구성된다. 4G/NGWN에서 사용자는 서로 다른 무선 네트워크 간에 끊김없는 로밍과 여러 가지 멀티미디어 서비스와 QoS 보장 등을 요구한다. UMTS나 cdma-2000과 같은 3G 셀룰러 서비스는 대역폭 용량이나 운영비용에 있어 약점이 있지만 넓은 지역을 커버할 수 있도록 구성되어 있다. 이와는 달리 WLAN이라고 불리는 IEEE 802.11 네트워크는 높은 대역폭과 적은 운영비용이 들지만 작은 지역만 서비스가 가능하다. 게다가 휴대용 기기의 혁명적인 기술 진보로 인하여 여러 가지 무선 접근 기술을 지원하는 단말기의 제조가 가능해졌다. 이로 인해 3G 무선 네트워크와 무료라는 강점이 있는 WLAN의 결합에 대한 관심이 많아졌다. 이러한 환경에서 효율적으로 서비스를 매끄럽게 하기 위한 많은 연구가 있었다. IISA(Integrated Intersystem Architecture)에서는 IDE(Internetworking Decision Engine)라는 엔진을 이용하여 WLAN, UTRAN 그리고 cdma-2000 망을 로밍 할 수 있는 구조를 제안하였다[1]. 이 구조는 모바일 노드(MN)가 각 네트워크의 MAP(Mobile Access Point)를 제어하고 네트워크 망간의 로밍을 홈네트워크의 AAA 서버나 홈 에이전트(HA)를 통해서 인증한 후에 서비스를 제공한다. IDE는 상황에 따라 MN이 이동해야만 하는 조건이 되면 인증 모듈과 함께 동작하여 로밍 절차를 수행한다[2]. 이것은 IP기반의 이종 네트워크에서 끊김없는 서비스를 제공할 수 있으나 네트워크 망간의 이동시에 인증에 소요되는 시간 때문에 서비스 지연이 발생할 수 있다. 이러한 단점을 보완하기 위해 모바일 IPv6에서는 프락시를 이용한 인증 방법을 도입할 수 있다. 모바일 프락시를 통하여 인근에 있는 이동 가능한 네트워크에 미리 인증을 완료하게 되면 해당 네트워크로의 이동이 일어났을 때 인증에 걸리는 시간을 최소화할 수 있다.

2. 관련연구

2.1 NGWN 아키텍처[1]

3GPP/3GPP-2-WLAN 상호모델에서 IISA라고 불리는 제안은 새로 인프라를 개발하는 것이 아니라 IISA는 현재의 인프라를 확장하여 사용자들이 모바일 환경에서 항상 최적의 연결을 할 수 있도록 제공한다. IISA는 일반적인 요구사항들(예: 확장성, 투명성, 경제성 그리고 보안) 등을 전부 고려한다. 여기다 인접한 네트워크 간의 상호작용도 같이 한다. BLR/BIU와 같은 환경에서 IISA는 오직 IDE라고 하는 한 개의 새로운 노드를 추가하고 다른 기능들은 기존 네트워크의 구성과 같이 구현된다. 또 BLR/BIU 구조와 다른 점은 제어 트래픽을 시그널링과 데이터 트래픽으로 구분하여 제안한다. 실제로 오직 시그널링 트래픽만 IDE로 직접 전달되게 된다. BLR/BIU 구조에서는 데이터와 시그널링 트래픽이 BLR/BIU를 통해서 전달되어서 시스템에서 병목을 만들게 된다.



(그림 1) IDE (Interworking Decision Engine) 구조

IPv6 기반의 이동관리 프로토콜을 지원하기 위해서 3G 무선 네트워크에서 몇 가지의 기능적 요소들이 확장되었다. SGSN(Serving GPRS Support Node)과 패킷 제어 기능이 AR 기능과 같이 개선되었고, AEN(Access Edge Node)이라고 불린다. 유사하게 GGSN(Gateway GPRS Support Node)와 Packet Data Serving Node도 MPA 혹은 HA와 같이 확장되었고 BEN(Border Edge Node)이라고 불린다. WIG는 경로와 메시지의 규격변환을 담당한다. 확장된 기능들은 현재의 네트워크 요소로 통합되거나 독립적으로 구현된다. 서로 다른 이종 네크워크 간의 상호작용은 효과적인 통합이 요구된다. 3G 무선 네트워크의 HLR나 홈 가입자 서버가 WLAN에서의 AAA 서버와의 매핑은 사용자가 양쪽 지역에서 인증과 빌링을 수행하는데 필요하다. IDE는 이종 네트워크 간의 상호작용과 핸드오프를 가능하게 한다고 소개했다. 시스템 오퍼레이터나 서비스 제공자는 모든 다른 오퍼레이터에 대해서 개별적으로 SLA를 만드는 것보다는 단지 하나의 SLA와 IDE만 설치하면 된다. IDE는 핸드오프 중에 AAA과정과 이동관리를 수행할 때 일어나는 시그널링 트래픽과 서비스의 끊김을 줄여주는 역할을 한다. IDE의 부하를 줄이기 위해서 IDE는 시스템 간이나 다른 도메인 간의 핸드오프에만 관여해야 한다.

NGWN에서의 이동성은 논리적/물리적이라고 할 때 사용자 프로파일과 선호도(Preference)는 수평적 핸드오프 시에 매우 중요하다. 그래서 4G/NGWN에서 RSS 레벨은 핸드오프를 결정하는데 적합하지 않다. 핸드오프 결정을 위한 핸드오프 결정함수는 통화비용, 대역폭, 세션 우선순위, 전력소비 그리고 네트워크 상태 등의 여러 가지 인자들을 계산하여 결정한다.

2.3 모바일 노드의 인증[2]

MN이 핸드오프를 수행하고 등록을 요청할 때마다 AAA에 요청하는 오버헤드 신호를 줄이기 위해서 우리는 토큰(Token) 기반의 접근을 제안한다. IDE를 준수하는 도메인 엑세스 네트워크인 MAP/BEN 안에서 로밍을 할 때 MN은 IDE에서 획득한 토큰으로 존재한다. 이것은 AAAH 서버와 함께 인증과 권한부여를 하는 것보다 적은 등록 지연효과가 생긴다. 만일 MAP/BIN이나 AR/AEN이 성공적으로 토큰을 확인하면 인증을 시작한다. MN의 인증과 관련된 HA의 기능은 keying, 세션키, 보안 관련 내용과 이동성 관리 등을 MN이 외부 네트워크에서 로밍하고 있을 때 IDE에 보내게 된다. 차후의 인증은 MAP/BEN이나 AAAL 서버에서 관리된다.

2.3 HPIN (Handoff Protocol Integrated Network)에서의 Handoff 수행

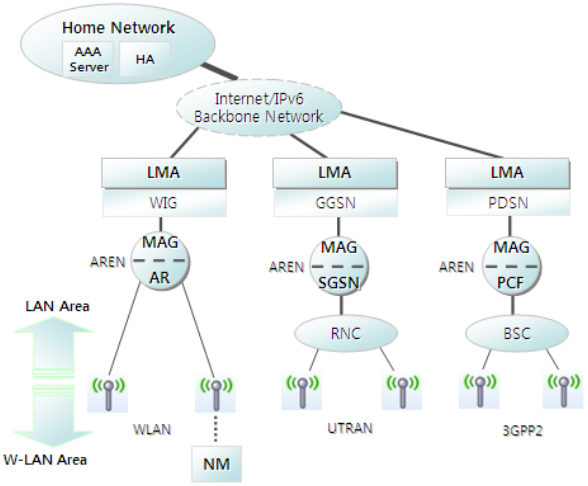
MN은 새로운 서브넷/하부시스템으로 이동한다는 것을 MAP/BEN에 알리기 위해 현재 서비스하는 MAP/BEN에 FBU 메시지를 보낸다. FBU 메시지를 받은 후에 MAP/BEN은 HI 메시지를 미리 정의된 NLCoA와 MAP/BEN과 NAR/AEN 간의 양방향 터널을 생성하고 핸드오프 중에 라우팅 실패를 막기 위한 것을 가지고 있는 NAR/AEN에게 보냄으로써 빠른 핸드오프 절차를 시작한다. HI 메시지의 응답으로서 HAck 메시지를 보내기 전에 NAR/AEN은 DAD 절차를 수행한다. HAck 메시지를 받은 후에 MAP/BEN은 FBAck를 이용하여 MN에게 결과를 보낸다. 정확한 시간에 MN은 L2 핸드오프를 수행하고 FBAck 메시지는 이전 링크와 다음 링크 양쪽으로 보내진다. 이것은 성공적인 바인딩을 확인함으로써 MN이 PAR/AEN이나 NAR/AEN으로부터 FBAck를 받은 것을 보장한다. 게다가 MAP/BEN은 PLCoA와 NLCoA를 바인딩하고 PLCoA로 보내진 모든 패킷을 NAR/AEN 서브넷에 있는 NLCoA로 보낸다. NAR/AEN는 포워딩된 패킷을 MN이 NAR/AEN 링크에 붙을 때까지 버퍼링한다.

MN은 새로운 링크에서 FNA와 RS(Router Solicitation) 메시지를 NAR/AEN으로 보냄으로서 자신을 알린다. 이 FNA 메시지는 또한 MN이 이전 링크에서 FBAck 메시지를 받지 못했을 때 NLCoA의 사용을 확인하는 데도 쓰인다.

3. 제안기법

3.1 인증 아키텍쳐

인증 방법은 DIAMETER 프로토콜과 Mobile IPv6 인증 프로토콜을 기반으로 한다.



(그림 2) 제안하는 무선 통신망의 인증 구조

MN은 글로벌하게 유일한 NAI에 의해 식별된다. 이는 AAA 서버와 LMA, MAG가 미리 설정된 키를 가진다고

가정한다. AAA 서버와 MAG 간의 신뢰 관계는 DIAMETER 프로토콜을 통해 유지된다. PMIPv6 도메인의 AAA 서버는 DIAMETER 호환된 방식으로 어떠한 MN에도 인증이 가능하다. AAA 서버는 MN의 프로파일을 가지고 있고, 이는 MN과 긴 시간 키를 공유한다. MAG는 MN에 방문하기 위한 인증 절차를 맡는다. AAA 클라이언트는 MAG에 위치한다. MN 이 새 세션을 초기화할 때, MN은 인증됨을 필요로 한다(초기 인증). MAG는 MN 인증을 위한 Attendant로서 보조하고, Attendant 광고 메시지를 광고한다. MAG가 MN으로부터 인증 요청을 받을 때, MAG는 AAA 서버로 인증 프로토콜을 트리거하고, AAA 서버와 협력하면서 MN의 ID를 검증한다. MN이 접속점(PoA)을 바꿀 때, MN은 새 MAG에 접속하기 전에 인증될 것을 요구한다(핸드오프 인증).

3.2 초기 인증 절차

1) MN은 MAG 같은 Attendant에 AS(Attendant solicit) 메시지를 보낸다. AS와 AA(Attendant Advertisement) 메시지는 두 개의 ICMP 메시지로 RS와 RA 메시지와 유사하다.
2) AS 메시지에 대응하여, MAG는 LC(Local Challenge)를 포함하는 AA 메시지를 보낸다. LC는 MAG 에 의한 challenge issue 이다. 이는 인증 절차에 대한 랜덤넘버이다. AS 메시지가 없더라도 MAG는 주기적으로 AA 메시지를 광고한다.
3) MN은 받은 LC값을 AAA 서버와 MN의 긴 시간 키를 이용하여 암호화하고 CR을 만든다. 이는 MN의 AAA 서버가 MN을 인증하는데 사용한다.

$$CR = E\_KAAA(LC)$$

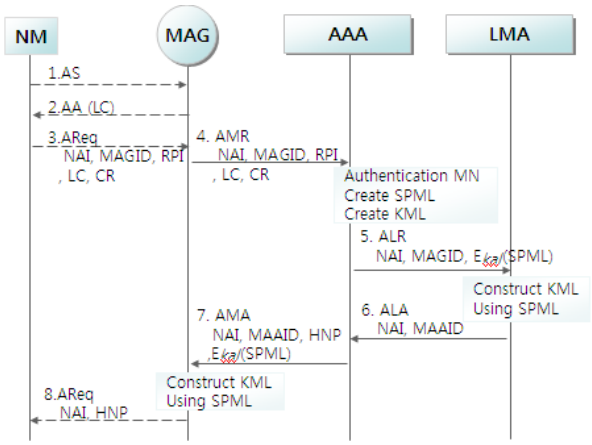
그런 다음, L2에서 L3로 Link-Up 트리거를 받은 뒤, MN은 LC와 CR을 포함한 인증 요청(AReq) 메시지를 MAG로 보낸다. AReq 메시지는 또한 MN의 NAI와 MAGID, RPI(Replay Protection Indicator)를 포함하는데, 이는 AAA 서버가 MN을 식별하고 Replay 공격을 막기 위한 것이다. RPI는 타임스탬프나 랜덤넘버이다.

4) MAG가 AReq 메시지를 받을 때, MAG는 이를 AMR(AA-MAG-Request) 메시지 내에 변환고, 그런 다음 MAG는 AMR 메시지를 AAA 서버에 보낸다.
5) AAA 서버가 AMR 메시지를 받을 때, AAA 서버는 미리 설정된 SA를 이용하여 LC를 암호화하고 CR 값과 결과를 비교한다. 만일 두 값이 동일하다면, MN은 성공적으로 인증된 것이다. 그러면 AAA 서버는 KML을 구축하는데 키 생성 임시어인 SPML 또한 생성한다. 우리의 프로토콜에서 KML은 MAG와 LMA 사이 동적 키를 의미한다. AAA 서버는 MAG와 LMA 간에 양방향 터널을 위한 KML을 생성한다.

$$KML = KMAC\_SHA1(KAAA, (SPML||NAI||MAGID||LMAID||128))$$

HMAC-SHA1(K,m)은 m 메시지를 K 키로 계산하는 해쉬함수이다. 앞의 수식은 MAG를 위한 인증 메소드가 MN 대신 PBU를 보내는 것을 보여준다. MAG가 KML 생성을 가능하게 하기 위해, AAA 서버는 SPML를 MAG에 보낸다. SPML은 긴-시간 키를 이용하여 암호화된다. 이는 다른 네트워크 엔티티에 노출될 가능성을 피하기 위한 것이다. KAM은 AAA 서버와 MAG 간에 미리 공유된 키를 의미한다. AAA 서버는 MN의 NAI와 ALR (AA-LAM-Request) 메시지에 의한 SPML를 LMA에 알린다. 키 생성 임시어인 SPML은 긴-시간 키를 이용하여 암호화된다. 이는 다른 네트워크 엔티티로의 노출 가능성을 피하기 위한 것이다. KAL은 AAA 서버와 LMA 간의 미리 공유된 키를 나타낸다.

6) LMA는 SPML을 이용하여 KML를 구축하고, 확증으로서 ALA(AA-LMA-Answer)를 답한다.
7) AMA(AA-MAG-Answer) 메시지는 AAA 서버가 인증 결과를 MAG로 알리기 위해 사용되는 메시지이다. AMA 메시지를 받을 때, MAG는 MN이 인증되었고 MN의 네트워크 엑세스가 허락됨을 안다. MAG는 AAA 서버에 긴-시간 키를 이용하여 메시지를 복호화하고, KML을 구축한다. 추가로 MAG는 HNP를 포함하여 인증 응답 메시지(ARep)로 결과를 MN에 알린다.



(그림 3) 초기 인증 절차

그림 3은 초기 인증 절차를 서술한 것이다. 핸드오프 인증 절차와 다른 점은 다음과 같다.

3 : MN 내의 L2에서 L3로 Link-Going-Down 트리거를 받을 때, MN은 PMAG로 새로운 MAG의 ID를 포함한 NMAGID AReq 메시지를 보낸다.
3': PMAG는 AReq 메시지를 포함한 HI 메시지를 NMAG에 보낸다.
8': HI를 받기 위해 NMAG는 ARep를 포함하는 HAck 메시지를 PMAG에 보낸다.

4. 성능평가

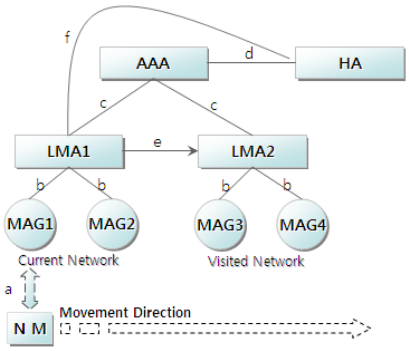
이 장에서는 PMIPv6에서 핸드오프 시에 소요되는 시간을 계산하여 HPIN에 비하여 PMIPv6가 핸드오프 시에 걸리는 시간이 적음을 증명함으로서 끊김없은 서비스를 구현할 수 있다는 사실을 보여준다.

4.1 인증과 핸드오프 지연의 계산

다음 매개변수들은 핸드오프 지연과 인증 시간을 계산하기 위해서 정의된 것들이다. t_{L2}는 L2 핸드오프 지연을 나타내고 $t_{X,Y}$는 노드 X와 Y의 메시지 크기이고, s는 단방향 전송지연을 나타낸다. 만약 양 끝단중의 한 개가 MN이면 $t_{X,Y}$는 다음과 같이 계산된다.

$$t_{X,Y}(s)=\frac{1-q}{1+q}\left(\frac{s}{B_{wl}}+L_{wl}\right)+(d_{X,Y}-1)\left(\frac{s}{B_w}+L_w+\varpi_q\right) \quad (1)$$

q는 무선링크가 실패날 확률이고 ϖ_q는 인터넷의 각 라우터에서의 평균 큐잉지연이다. B_{wl}은 무선 링크구간의 대역폭을 나타낸다.



(그림 4) 성능평가를 위한 네트워크 구조

4.1.1 HPIN 방식

MAP/BEN내 로밍의 경우 : 데이터 패킷을 제외한 인증 및 핸드오프의 컨트롤 패킷을 계산하면

$$D^l_{HPIN}=t_{L2}+2t_{MN,CAR2}+4t_{MN,MAP}+6t_{MAP,CAR2}+2t_{MAP,IDE} \quad (2)$$

MAP/BEN간 로밍의 경우 : 인증과 핸드오프에 필요한 컨트롤 메시지를 기본으로 지연 시간을 계산하면

$$\begin{aligned}N^g_{HPIN}=&\ t_{L2}+4(t_{MN,MAP1}+t_{MAP2,CAR1})\\&+2(t_{MN,CAR1}+t_{MAP1,MAP2})+4t_{MAP2,IDE}\\&+t_{MAP2,HA}+t_{MN,HA}\end{aligned} \quad (3)$$

4.1.2 PMIPv6 방식

MAP/BEN내 로밍의 경우 : 도메인 안에 있으므로 추가로 AAA 서버에 인증할 필요가 없다.

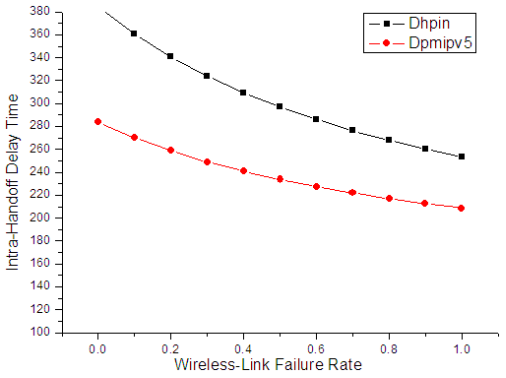
$$D^l_{PMIPv6}=t_{L2}+4t_{MN,PMAG} \quad (4)$$

MAP/BEN간 로밍의 경우 : 인증과 핸드오프에 필요한 컨트롤 메시지를 기본으로 지연 시간을 계산하면

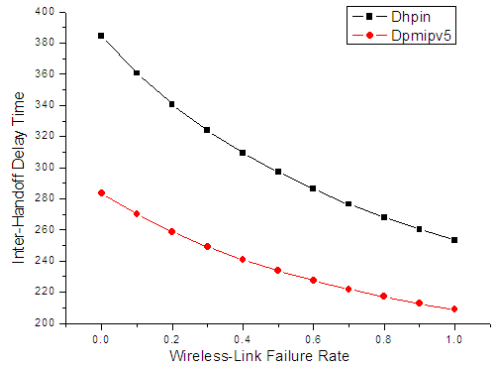
$$N^g_{PMIPv6}=t_{L2}+2(t_{PMAG,NMAG}+t_{NMAG,AAA}+t_{AAA,LMA})+4t_{MN,PMAG} \quad (5)$$

4.2 성능평가

거리변수 a=1, b=2, c=d=e=f=10 로 정의한다.



(그림 5) Intra-핸드오프 시에 핸드오프 지연시간



(그림 6) Inter-핸드오프 시의 핸드오프 지연시간

5. 결론

이 논문에서 보듯이 PMIPv6 프로토콜 방식을 사용하면 인증서버에 시그널 메시지만 전달함으로서 Replay 공격이나 키 노출 공격을 방지할 수 있다. 또한 핸드오프 시에 HPIN과 비례하여 핸드오프 지연시간을 줄일 수 있어서 목적하는 끊김없는 서비스를 구현하는데 큰 도움이 될 수 있다. 향후의 연구로는 Proxy 기반에서 MN의 움직임을 예측하여 미리 인증을 함으로써 더욱 빠른 핸드오프를 구현할 수 있도록 할 것이다.

ACKNOWLEDGMENT

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2010-0024695). 교신저자: 정종필.

참고문헌

[1] Chiristian Makaya, Samuel pierre, "An Architecture for Seamless Mobility Support in IP-Based Next-Geration Eireless Networks, IEEE Transactions onVehicular Technology, Vol.57, pp.1209-1225, March 2008.

[2] Huachun Zhou and Hongke Zhang, "An Authentication Protocol for Proxy Mobile IPv6," The 4th Internatioinal Conference on Mobile Ad-hoc and Sensor Networks 2008(MSN 2008), pp.129-136, December 2008.