IP기반의 모바일 네트워크에서 비용효율적인 이동성을 위한 계층적 인증기법

정하권*, 정종필**
*성균관대학교 정보통신대학원 컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail:junhg7@skku.ac.kr

An Hierarchical Authentication Scheme for Cost Effective Mobility in IP-Based Mobile Networks

Ha-Gwon Jung*, Jongpil Jeong**
*Dept of Computer Engineering, Graduate School of Information and Communications Sungkyunkwan University
**Dept of Computer Engineering, School of Information and Communications Sungkyunkwan University

요 약

IETF(Internet Engineering Task Force)는 신속하고 안전한 이동성 서비스를 위하여 네트워크 자원의 사용을 안전하게 하고 법적으로 보장하는 핵심기술 같은 많은 의미있는 작업들을 해오고 있으며 기존의 MIPv6(Mobile IPv6)에서 핸드오버 지연과 시그널링 오버헤드 같은 문제를 보완하기 위하여 HMIPv6(Hierarchical Mobile IPv6)를 제안하였다. 현재 HMIPv6에 관한 연구의 대부분은 HMIPv6와 AAA(Authentication, Authorization, Accounting) 프로토콜 사이의 상호작용 절차를 최적화하기 위한 방법에 초점을 맞추고 있다. 해당 논문에서는 AAA 절차에서 인증대기를 최소화하는데 중점을 둔 비용효율적인 계층 인증 기법을 제안한다. 이 기법에서는 MAP(Mobility Anchor Point)에 배포되어진 AAA 서버들, 그리고 홈 도메인 안에 있는 AAA 서버를 대신하는 브로커들의 계층적 AAA 아키텍처를 제안한다. 이 시뮬레이션 결과는 제안된 기법이 이전의 전통적인 인증 조합 모델링과 비교하여 핸드오프 지연과 인증대기 시간이 상당히 줄어들었음을 보여준다.

1. 서론

IETF(Internet Engineering Task Force)는 차세대 네트워크를 위한 기본 프로토콜로서 Mobile IPv6(MIPv6)[1]의 이동성 지원을 제안하였으며, MIPv6을 위한 두 가지 대표적인 확장 기법인 Fast Handover MIPv6(FMIPv6)와 Hierarchical MIPv6(HMIPv6)의 이동성관리[2][3]가 나중에 제안되었다. MIPv6는 이동단말이 홈 망에서 사용하는 홈 주소 외에 이동단말의 현 위치를 알려주는 CoA(Care of Address)를 가지며 이를 위치 변경 시마다 이동단말로부터 먼 곳에 위치할 가능성이 있는 홈 에이전트나 상대노드(CN)에 등록(Binding Update)을 수행하여야 한다. 이 경우 이전 서브넷에서 새로운 서브넷으로의 등록이 완료되기 전까지 상대노드에 대한 연결성을 잃어버리게 되며 이로 인한 패킷 손실과 지연을 가져오게 된다. 이러한 패킷 손실과 지연은 VoIP와 같은 실시간성이 요구되는 응용에서는 수용할 수 없는 정도가 될 수도 있다.

본 논문에서는 이러한 문제를 해결하기 위하여 이동단말이 홈망에서 먼거리에 위치한 경우 인증요청 메시지를 홈 도메인에 있는 AAA 서버(AAAH)로 전달하는 대신 본 논문에서 제안하는 AAAH의 모든 역할을 수행하면서 이동단말과 더 가까운 거리에 위치하고, 보안적인 측면에서 신뢰관계를 형성하고 있는 브로커(Broker)에게 전달하여 보다 나은 성능을 달성할 수 있음을 보인다.

논문의 구성은 다음과 같다. 2장에서 관련연구에 대해서 살펴본다. 3장에서는 제안하는 계층적 AAA 아키텍처, 시스템 모델링에 따른 비용분석에 대해서 설명한다. 4장에서는 제안한 아키텍처의 비용분석을 통한 성능평가를 보인다. 5장에서는 결론과 향후 연구내용을 기술한다.

2. 관련연구

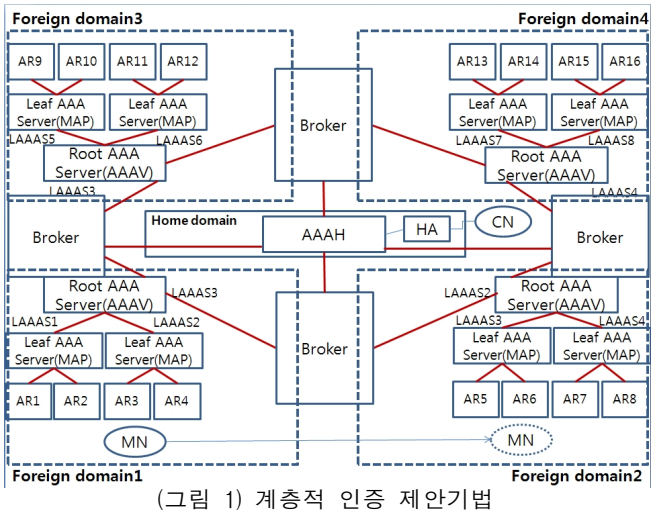
현재 HMIPv6에 관한 연구의 대부분은 HMIPv6와 AAA의 프로토콜 사이의 상호작용 절차를 최적화하는 방법에 초점을 맞추고 있다[4-7]. [5]는 Root AAA서버(RAAAS)를 이용하여 도메인 내 이동 시 인증과 등록에 대한 지연이 줄어들 것임을 보여주고 있으며, [6]는 모바일 IPv6 및 AAA의 결합된 프로그램을 제시했다. 이는 AAA 프로토콜에서 핸드오프 메시지 이동으로서 상호작용 및 비용이 줄어들 것임을 보여준다. [7]은 L2 핸드오프 시간의 전체를 사용하여 AAA의 프로세스를 수행할 수 있게 최적화된 빠른 핸드오프 절차를 보여주고 있다. [8]는 HMIPv6 아키텍처로 통합하여 지역이동을 위한 지연 및 신호 메시지의 양을 줄일 수 있는 인증 체계를 제안했

다. 그러나 이 기법은 단지 내부 지역 이동에 응용할 수 있고, 이동단말들이 도메인 간 이동이 잦을 때 효과가 적다. 게다가 [9]는 MIPv6의 보안 이슈에 책임이 있고, 모든 AAA 참여자들의 토폴로지에 관심이 많은 TAON (Topological-aware AAA Overlay Network) 모델을 제공했다. 그러나 그것들의 배포와 비용을 만드는 추가기능을 위한 안내가 없다. [10]의 전체 비용과 시간 지연에 대한 비교분석은 더 큰 범위로 줄어들게 된다. 하지만 여전히 이동단말의 이동성을 고려하는 동안 추가 조사를 해야 한다. 지금까지 언급한 참고 문헌에서, 기존의 연구들이 근본적으로 핸드오프 및 인증대기를 정말로 줄여줄 수 없다고 결론지을 수 있으며, 이 논문에서는 보다 나은 성능을 달성하기 위한 효율적인 인증 기법을 제안한다.

3. 계층적 비용효율적인 인증 제안기법

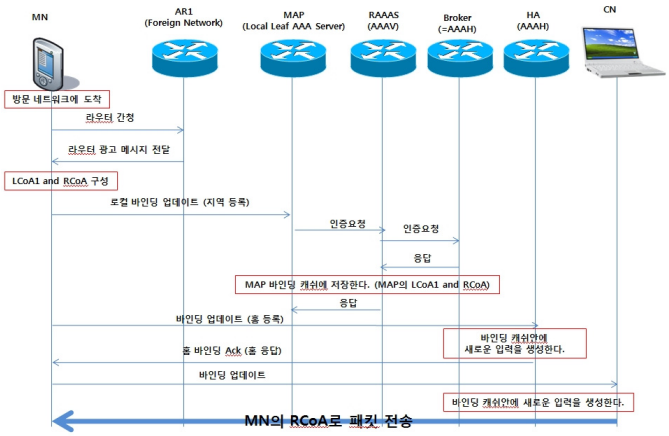
3.1 계층적 AAA 제안 아키텍처

홈 도메인 내에서 이동단말이 이동할 때 홈 도메인에 있는 AAA 서버(AAAH)에서 네트워크에 대한 액세스를 얻기 위해 AAA 서비스를 해야 한다. 이동단말의 방향이 홈 도메인 밖으로 이동하여 이동단말이 변경될 때 마다 방문한 도메인 (AAAV)에서 AAA의 서버에 의해 인증되어야 하며, 아래와 같은 명확한 인증 절차를 거쳐야 한다.



(그림 1) 계층적 인증 제안기법

첫 번째로 이동단말은 Local Leaf AAA 서버(LAAAS)로 인증 요청을 보내고, LAAAS는 요청 메시지를 AAAV 역할로서 행동하는 Root AAA 서버(RAAAS)로 전달한다. 두 번째로 외부도메인에서 이동단말이 처음으로 도착하는 경우 아무 관련 없는 식별 정보가 Local RAAAS 내에 저장되고 AAAH에서 인증과 권한 허가를 필요로 하게 된다. 그러므로 인증요청 메시지는 AAAH로 전달되어지고 마침내 관련된 응답메시지를 RAAAS를 통하여 이동단말에게 전달되어지게 된다. 그러나 이때 이동단말이 홈 망에서 먼 거리에 위치한 경우 이와 같은 인증 방식은 긴 등록 시간을 유발하여 망에 불필요한 트래픽을 유발시키게 됨으로 인증 요청 메시지를 AAAH로 전달하는 대신 AAAH의 대리인으로서 모든 역할을 수행하고 이동단말과 보다 가까운 거리에 위치하면서 보안적인 측면에서 신뢰관계를 형성하고 있는 그림 1의 Broker에게 전달되어 지고 마침내 관련된 응답 메시지를 RAAAS를 통하여 이동단말에게 전달되어 진다. 그 후 이동단말이 외부도메인 밖으로 이동하지 않는 경우, 단지 다른 LAAAS 관리 도메인 안에서 이동은 RAAAS의 인증만을 요구하게 된다. 외부도메인 안에서 RAAAS는 이동단말을 위한 AAA 서비스를 제공하는 AAAH의 대리인으로서 활동한다. 또한 예전 RAAAS 관리 도메인에서 이동단말이 밖으로 이동하여 새로운 외부도메인에 도착할 때 인증 매개 변수를 포함한 관련 정보가 외부도메인에 처음 도착한 이동단말의 인증 절차와 동일하게 Broker를 통하여 새로운 RAAAS에 전송된다. 그림 2는 제안기법의 홈 도메인 내 등록절차를 보여준다.



(그림 2) 제안 기법의 홈 도메인 내 등록 절차

3.2 시스템 모델링에 따른 비용분석

지역이동의 총비용 C_{total} 은 세 가지 항목으로 구성된다. 등록 신호의 전송비용(C_{reg}), 인증 신호의 전송비용(C_{auth}), 패킷 전송비용(C_{trans}). 본 논문에서등록과 인증신호의 전송비용은 C_{RA} 로 정의한 것과 함께 고려되어지며 C_{trans} 는 패킷 처리와 전송비용을 의미한다.

$$C_{total} = C_{reg} + C_{auth} + C_{trans} = C_{RA} + C_{trans} \quad (1)$$

본 논문에서 홉은 거리의 단위이며 유선링크의 전송비용은 거리의 직접적인 비율이다. 또한 거리단위 전송 비용은 η 으로 정의되고, 무선 링크 전송비용은 유선링크 만큼의 θ 시간으로 나타낸다. 수식은 아래와 같이 표현 할 수 있다.

$$C_{first} = RA_B + RA_R + 2\eta(\theta + 2L_{RL} + L_{BR}) \quad (2)$$
$$C_{other} = RA_R + 2C_{ML} + 2C_{LR}$$
$$C_{each} = RA_H + RA_R + 2\eta(\theta + 2L_{RL} + L_{HR})$$

제안된 기법의 등록과 인증신호 전송비용을 나타내는 $C_{proposed-RA}$와 이전 기법의 등록과 인증신호 전송비용을 나타내는 C_{Pre-RA}의 외부관리 도메인 내의 등록과 인증신호 전송 평균비용은 아래와 같이 각각 계산되어 질 수 있다.

$$C_{\Pr oposed-RA} = \frac{C_{first} + (E(m)-1)\times C_{other}}{(E(m)-1)\times T} \quad (3)$$

$$C_{\Pr e-RA} = \frac{E(m)\times C_{each}}{(E(m)-1)\times T} \quad (4)$$

이전 기법과 제안된 기법의 패킷 전송비용은 아래와 같이 각각 계산되어 질 수 있다.

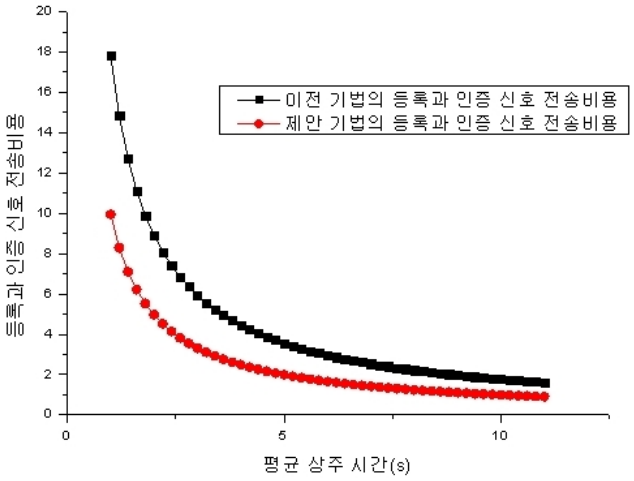
$$C_{pre-trans} = \mu \times (P_H + P_R + \eta \times (L_{HR} + L_{RL}))$$
$$C_{trans} = \mu \times (P_B + P_R + \eta \times (L_{BR} + L_{RL})) \quad (5)$$

4. 성능평가

다음에 나오는 시뮬레이션 결과는 표 1에 정의된 값들에 부합되게 얻어진다. 그림 3은 이전 기법과 제안된 기법의 기간 내 평균 상주시간 γ에 대해 등록과 인증신호전송비용에 대한 영향을 나타낸다.

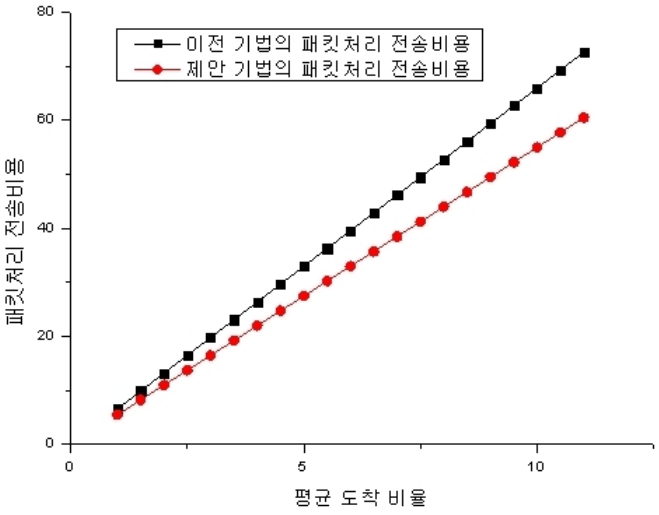
(표 1) 매개변수들의 값

				P_B					L_{HR}	L_{BR}	
6	4	3	4	3	2	0.05	10	4	8	6	4



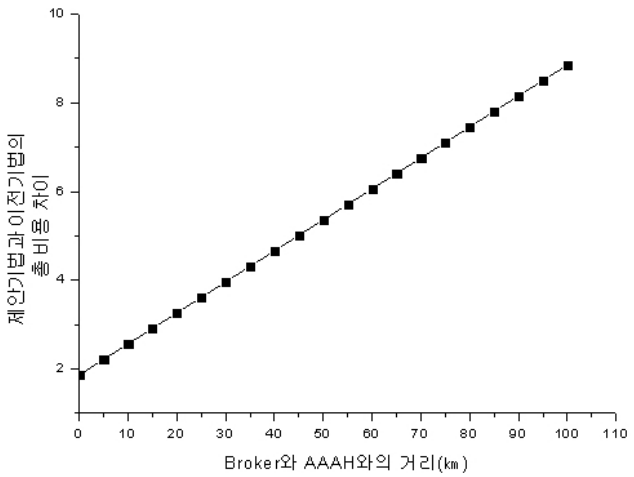
(그림 3) 이전 기법과 제안된 기법 사이의 인증신호와 등록 전송비용의 비교

그림 3의 데이터 변화 흐름으로부터 평균 상주시간 γ의 증가 값에 따라 등록과 인증신호 전송 비용이 항상 줄어드는 것을 볼 수 있으며, 이것은 이동단말의 상주시간의 증가에 따라 총 시스템 비용이 줄어드는 것을 의미하며 이전 기법과 비교해서 제안된 기법을 사용하였을 때 총 비용이 적어도 45% 감소할 수 있음을 보여준다.



(그림 4) 이전 기법과 제안된 기법 사이의 패킷 처리 전송비용의 비교

그림 4는 이전 기법과 제안된 기법의 이동단말의 평균 도착 비율 μ에 대해 패킷처리 전송 비용에 대한 영향을 나타낸다. 그림 4의 데이터 변화 흐름으로부터 이동단말이 하부 네트워크로부터 다른 네트워크로 이동하는 평균 도착 비율의 증가와 함께 패킷처리 전송비용이 증가하는 것을 볼 수 있으며, 이전 기법과 비교하여 제안된 기법을 사용하였을 때 평균 도착 비율의 증가와 함께 패킷 처리 전송 비용이 큰 폭으로 감소하는 것을 보여준다. 또한 이론적인 분석으로부터 총 비용은 이동단말의 평균 도착 비율과 상주하는 시간에 의해서 영향을 받는 것으로 결론지을 수 있다.



(그림 5) Broker와 AAAH와의 거리에 따른 제안기법과 이전기법의 총 비용 차이

그림 5는 Broker와 AAAH와의 거리차이에 따른 제안 기법과 이전기법의 총 비용차이 변화를 보여준다. 그림 5의 데이터 변화 흐름으로부터 Broker와 AAAH와의 거리가 증가할수록 제안 기법과 이전 기법의 총 비용의 차이가 증가하는 것을 볼 수 있으며 Broker와 AAAH의 거리가 제안기법의 총 비용에 영향을 주는 것을 보여준다. 이는 Broker와 AAAH의 거리가 RAAAS로부터 가까이에 위치할수록 총 비용이 감소하는 것을 보여준다.

5. 결론

계층적 인증구조를 분석하고 수립함에 있어 본 논문은 핸드오프와 인증대기를 줄이기 위한 비용효율적인 인증기법을 제공한다. 이론적인 분석으로부터 총 비용은 평균 상주시간, 평균 도착 비율, Broker와 RAAAS 사이의 거리 및 기타 등등 여러 가지 매개변수에 의해서 영향을 받는다는 것을 보여준다. 그리고 시뮬레이션 결과는 제안된 방식이 이전 기법에 비해 더 우수한 결과를 보여준다. 게다가 본 논문에서 제안한 Broker는 AAAH의 모든 기능을 수행하며 지리적으로 RAAAS에 가까이 위치하여 보다 적은 비용을 통해 효율적인 이동성을 지원할 수 있음을 보여준다. 또한 Broker의 배포위치와 네트워크 토폴로지의 추가적인 의무 요구사항이 없고, 더 강한 발전성이 있는 정책을 만들 수 있다. 향후 연구과제로 효율적인 보안 인증 응용서비스를 연구해 볼 계획이다.

ACKNOWLEDGMENT

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

참고문헌

[1] Johnson D, Perkins C and Arkko J. "Mobility Support in IPv6," IETF RFC3775, 2004.

[2] Youngsong Mun and Kyunghye Lee, "Fast Macro Mobility Handovers in HMIPv6," draft-mun-mipshop-fhmacro-05.txt, 2010.

[3] Soliman H S, et al., "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," IETF RFC 5380, October 2008.

[4] Wei D, Liu Y H, Yu X G, et al., "Research of Mobile Ipv6 Application Based on Diameter Protocol," 2006 International conference on Multi-Symposiums, Computer and Computational Sciences (IMSCCS'06), 2006.

[5] WANG Li, SONG Mei and SONG Jun-de, "An efficient hierarchical authentication scheme in mobile IPv6 networks," pp.9 - 13, September 2008.

[6] Laurent M and Dupont F., "Inter-domain security for mobile Ipv6," The 2nd European Conference on Universal Multiservice Networks (ECUMN 2002)," pp.238 - 245, 2002.

[7] Lee S Y, Huh E N, Kim S B, et al., "An Efficient Performance Enhancement Scheme for Fast Mobility Service in MIPv6," 2005 International Conference on Computational Science and its Applications (ICCSA 2005), pp.628 - 637, 2005.

[8] Kim M Y, Kim M S and Mun Y S., "A Hierarchical Authentication Scheme for MIPv6 Node with Local Movement Property," 2005 International Conference on Computational Science and its Applications (ICCSA 2005), pp.550 - 558, 2005.

[9] Li J, Ye X M and Tian Y., "Topologically-Aware AAA Overlay Network in Mobile IPv6 Environment," The 5th International Conference on IFIP-TC6 Networking, pp.293 - 306, May 2006.

[10] Xiao W S and Zhang Y J., "Hierarchical AAA in mobile IPv6 networks," The Journal of China Universities of Posts and Telecommunications, pp.50-55, 2006.

[11] Pack S and Choi Y., "Performance Analysis of Hierarchical Mobile IPv6 in IP-based Cellular Networks," IEEE 2003 International Conference of PIMRC, 2003.

[12] Chiang K and Shenoy N., "A Random Walk Mobility Model for Location Management in Wireless Networks," IEEE 2003 International Conference of PIMRC, 2003.

[13] Jiang X and Akyildiz L F., "A novel distributed dynamic location management scheme for minimizing signaling costs in mobile IP," IEEE 2002 International Conference on Mobile Computing, pp.163-175, 2002.