계층적 Mobile IPv6에서의 안전한 MAP 검색 기법

(Secure MAP Discovery Schemes in Hierarchical MIPv6)

최 종 현 † 문 영 성 ††
(Jonghyoun Choi) (Youngsong Mun)

요 약 계층적 Mobile IPv6 (HMIPv6)는 기존의 Mobile IPv6의 핸드오프 성능 향상을 위해 IETF에서 제안되었다. 기존의 Mobile IPv6는 핸드오프를 하기위해 교환하는 메시지가 핸드오프의 지연을 발생시키고, 홈 에이전트 (HA: Home Agent)에 핸드오프의 처리 부하가 집중되는 문제가 있다. 계층적 Mobile IPv6는 MAP(Mobility Anchor Point)이라는 노드를 이동 노드(MN: Mobile Node)가 접속하는 지역에 위치시켜, 지역 HA처럼 동작시켜 핸드오프 성능을 향상시킨다. MN과 HA의 연결은 IPsec으로 안전한 반면, MN과 MAP과의 관계는 아직 보안이 미흡하다. MN과 MAP간의 보안이 없다면, 서로에게 정당한 MN인척, 혹은 정당한 MAP인척 하여 여러 가지 보안의 문제를 발생시킬 수 있다. 본 논문은 계층적 Mobile IPv6에서 안전한 MAP을 검색하는 방법을 제안하고, 수학적으로 성능을 분석한다.

키워드 : Mobile IPv6, Hierarchical MIPv6, 보안, Random-Walk 이동 모델, 마코프 체인

Abstract The Hierarchical Mobile IPv6 (HMIPv6) has been proposed to accommodate frequent mobility of the Mobile Node and to reduce the signaling load. A Mobility Anchor Point is a router located in a network visited by the Mobile Node. The Mobile Node uses the Mobile Anchor Point as a local Home Agent. The absence of any protections between Mobile Node and Mobile Anchor Point may lead to malicious Mobile Nodes impersonating other legitimate ones or impersonating a Mobile Anchor Point. In this paper, we propose a mechanism of the secure Mobile Anchor Point discovery in HMIPv6. The performance analysis and the numerical results presented in this paper show that our proposal has superior performance to other methods.

Key words : Mobile IPv6, Hierarchical MIPv6, Security, Random-Walk Mobility Model, Markov Chain

1. 서 론

HMIPv6 환경에서 MN이 새로운 AR(Access Router) 도메인으로 이동할 경우, MN은 2가지 종류의 위치 등록(Binding Update) 과정을 수행한다. MAP 도메인 사이의 이동일 경우 글로벌 위치 등록(Global Binding Update, Inter-MAP)을, MAP 도메인 내의 이동일 경우 지역 위치 등록(Local Binding Update, Intra-MAP)을 수행하게 된다. MAP(Mobility Anchor Point)은 MN이 접속한 외부 도메인에서 지역 HA처럼 작동하며, MN의 위치 관리를 한다. 외부 도메인 내에 MAP은 여러 개가 존재할 수도 있다.

HMIPv6 환경에서는 MN은 RCoA, LCoA 라는 2 가지의 임시 주소(CoA:Care Of Address)를 갖는다. RCoA(Regional CoA)는 MAP 도메인 내에서 사용되는 임시 주소이며, LCoA(On-Link CoA)는 기존의 MIPv6에서의 CoA와 같은 것이며, RCoA와 구분된다. MN이 새로운 MAP 도메인으로 진입하게 되면, MN은 위의 2가지 임시 주소를 설정한다. 주소 설정 후, MN은 RCoA를 기반으로 MAP에게 위치 등록 절차를 수행한다. 이 과정은 LCoA와 RCoA를 바인딩(Binding)하는 효과를 갖는다. 이후 MAP은 MN이 접속한 외부 도메인에서 HA처럼 동작한다.

MAP 등록 절차가 끝나면, MN은 새로운 RCoA를 자신의 HA에게 등록하게 되는 위치 등록 절차를 또 한 번 수행한다. 이 과정은 RCoA와 홈 주소(Home Add-

· 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원 사업의 연구결과로 수행되었음(IITA-2006-C1090-0603-0040)
† 학생회원 : 숭실대학교 컴퓨터학부
wide@sunny.ssu.ac.kr
†† 종신회원 : 숭실대학교 컴퓨터학부 교수
mun@comp.ssu.ac.kr
논문접수 : 2006년 9월 11일
심사완료 : 2006년 11월 28일

ress)를 연결(바인딩)하는 효과를 갖는다. 이 위치 등록 절차는 MN이 MAP 도메인 내에서 이동 할 경우는 생략된다.

현재 Mobile IP 네트워크의 가장 큰 이슈는 이동 성능의 향상과 보안 문제 해결이라 할 수 있다. HMIPv6 환경에서도 많은 보안 위협이 존재하는데, 그중에 MN과 MAP 사이의 보안이 가장 큰 문제이다. 두 노드 사이의 상호 인증 절차가 없을 경우, 악의를 가진 MN이 정당한 MN인 것처럼, 혹은 악의를 가진 노드가 MAP인 것처럼 동작하여, MN의 정보를 가로채는 문제가 발생할 수 있다[2]. 만약 MN에서 MAP에게 전송되는 위치 등록 메시지(BU Message : binding up-date message)가 인증되지 않는다면, 공격자는 쉽게 리다이렉트 공격(Redirect Attack)을 할 수 있다. 리다이렉트 공격은 MAP에게 전송받는 트래픽을 공격자가 선택한 노드로 변경하여 정보가 누출되는 공격이다[2,11]. 본 논문에서는 안전한 방법으로 정당한 MAP을 검색하는 방법을 제안하고, 기존의 방법들과 수학적 방법을 사용해 성능을 분석한다.

2. 관련 연구

현재 HMIPv6 환경에서 앞서 언급한 문제들을 해결하고자 많은 연구가 진행 중이다. 현재 IETF에 제안된 방법은 다음과 같이 3가지 종류가 있다.

2.1 위치 등록 메시지를 보호하여 MN과 MAP 상호 인증하는 방법[11]

이 문서에서 저자는 Global PKI 같은 보안 인프라없이 MN에서 MAP으로 전송되는 위치등록 메시지를 보호하는 방법과, MAP이 MN을 인증하는 방법을 제안하고 있다. IETF 워킹 그룹의 보안 요구사항에 의해, 아래와 같이 2가지 시나리오에 대해 2가지 모델을 제안하고 있다[11].

- 인증 서비스만 제공하는 모델(Authentication-only model)

이 모델은 MAP에게 이미 등록된 MN이 이동해서 새롭게 위치 등록을 할 경우, 이전에 등록한 MN임을 보장할 수 있는 모델이다. 이 모델에서는 MN이 MAP에 접근할 수 있는 권한 여부를 검증하지는 않는다.

- 인증, 허가 서비스를 제공하는 모델(Authentication and Authorization model)

이 모델은 위의 모델에서 제공하는 서비스 뿐만 아니라, MN이 MAP에 접근할 수 있는 권한 여부도 검증한다. 이 모델에서는 MN과 MAP 상호간의 신뢰관계(Trusted)를 성립하게 된다.

아래의 그림은 두 가지 모델의 메시지 교환 순서를 보여준다.

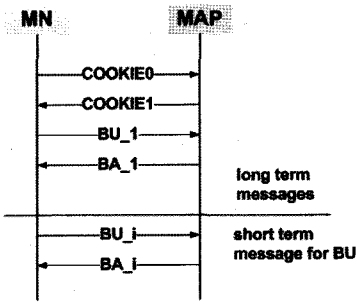

그림 1 Authentication-only model

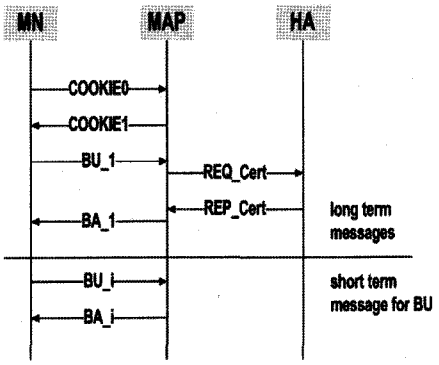

그림 2 Authentication and Authorization model

2.2 CGA와 CBI을 이용하여 MN과 MAP간의 SA를 체결하는 방법[12]

이 문서에서 저자는 기존에 제안된 CGA(Crypto-graphically Generated Address)와 CBID(Crypto-Based Identifiers)를 이용하여 MN과 MAP간에 보안 관계(SA, Security Aassociation)를 체결한다. SA를 체결하는 방안은 다음과 같이 4단계로 나누어진다[12].

1단계 : Router Solicitation [CGA Sign. + CBID]
2a단계: Router Acknowledgement [Ks] (RtAdv)
2b단계: Pre-Binding Update [Ks]
3단계 : Local Binding Update
4단계 : Binding Acknowledgement [Km + HKs]

아래의 그림 3은 제안하는 방법의 메시지 교환 순서이다.

2.3 IPSec을 이용한 방법[2]

이 방법은 IETF의 HMIPv6 표준문서에 포함되어 있는 방법이다. 표준문서에서는 막연히 IPSec을 사용하여 보안 관계를 성립하도록 권고하고 있다. 자세한 적용 방법을 제시하고 있지 않아 본 논문에서는 IPSec과 IKE를 사용했을 경우 다음과 같은 순서로 메시지를 교환하여 MN과 MAP간의 SA를 체결하는 것으로 분석하였다[2].

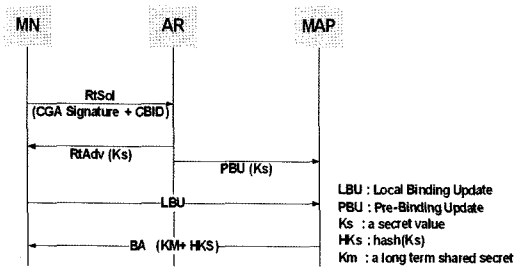

그림 3 CGA와 CBI 기반으로 SA 체결 방법

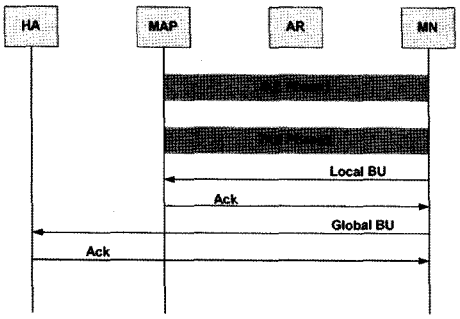

그림 4 MAP내에서 이동일 경우(Inter-MAP)

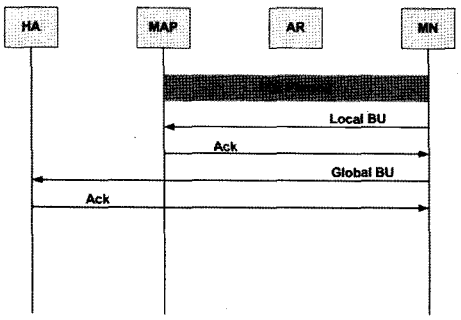

그림 5 MAP간 이동일 경우(Intra-MAP)

IKE는 2가지 단계가 있는데[3,8,9], 처음 통신하게 되는 상대와는 반드시 2가지 단계를 모두 수행하여야한다. 그리고 IPsec은 이미 잘 알려진 보안 프로토콜로서 강력한 보안 서비스를 제공하지만, 과도한 프로세싱 비용으로 이동 단말에는 다소 무리를 주는 단점이 있다.

3. 제안 방안

본 논문에서는 안전하고 신뢰할 수 있는 MAP을 검색하는 방법을 제안한다. 제안하는 방법은 MN-HA 사이의 링크는 IPsec에 의해 보안이 이미 체결된 링크이며[1], 모든 IPv6 링크는 SEND(SEcure Neighbor Discovery)[13]를 사용하여 보호 받는 링크라는 조건을 가진다. 이러한 가정이 의미하는 것은 제안 시스템에서

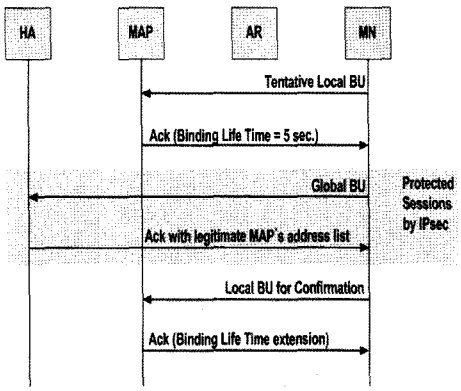

그림 6 제안 시스템의 메시지 교환 순서

는 IP 스푸핑(Spoofing) 공격과 리다이렉트(Redirect) 공격이 있을 수 없다는 것을 의미한다. 그림 6은 제안하는 시스템에서 보안 체결을 위한 메시지 교환 순서이다.

제안 시스템의 동작 과정은 다음과 같다. 우선 MN은 검색된 MAP에게 임시 위치 등록 메시지를 전송하여 등록한다. 이때 MAP이 정당한 노드인지는 알 수가 없으므로 임시로 등록하는 것이다. 그러므로 임시 등록의 유효 시간은 5초로 제한하여 DOS 공격에 대한 피해를 최소화 한다. MAP으로부터 확인(Ack) 메시지를 받은 MN은 HA에게 위치 등록 메시지를 전송하고, 확인(Ack) 메시지를 받는다. 이때 HA는 확인 메시지와 함께 MN의 근처의 정당한 MAP의 주소 리스트를 같이 전송한다. 이 링크는 보안이 이미 체결된 안전한 링크이므로 MAP 주소 리스트는 안전하게 MN에게 전달된다. 이후 MN은 임시 위치 등록의 유효시간이 만료되기 전에 다시 한 번 MAP에게 위치등록을 하게 된다. 기존의 Inter-MAP간의 이동일 때 위치 등록하는 횟수로 보면 제안하는 시스템이 1번 더 위치 등록 절차를 갖지만, 임시 위치 등록 서비스가 정당한 것이라면, 기존의 방법보다 더 빠르게 서비스를 받을 수 있는 장점이 있다.

4. 성능 분석

4.1 이동성 모델

본 논문의 네트워크 모델은 hexagonal cellular 네트워크 모델을 사용하였다. 각 MAP 도메인은 동일한 수(R개)의 range ring으로 구성되었다고 가정한다. 각 range ring r($r \geq 0$)은 6r 셀들로 구성된다. 가장 중앙의 셀을 "0"이라고 하고, 이 셀을 감싸는 6개의 셀은 "1"이라고 한다. 같은 방식으로 하면, 그림 7 같이 된다.

본 논문에서는 MN의 이동성 모델링을 위해 Random-Walk Mobility 모델을 사용하였다. Rando m-Walk Mobility 모델은 이동 속도가 느린 보행자 같은 이동체

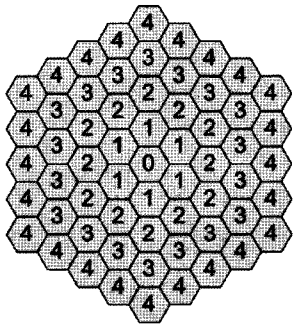

그림 7 hexagonal cellular 네트워크 모델

에 적합한 모델이다[4].

본 논문에서는 Random-Walk Mobility 모델의 2차원 Markov Chain 모델을 사용하여 단말의 이동성을 모델링 하였다[5]. 이 모델에서는 MN의 다음 위치는 이전 위치에 임의의 값을 더한 것이 된다. 여기서 임의의 값은 임의의 분포에서 독립적으로 선택된 값이다. 또한 MN이 네트워크에 머무를 확률을 q라고 할 때 다른 네트워크로 이동할 확률은 1-q이다. 그림 7에서, MN이 range ring r(r > 0)번째 셀에 있다면, 외부로 나갈 경우(r값이 증가), 내부로 들어갈 경우(r값이 감소)의 확률은 각각 다음과 같다[10].

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

본 논문에서는 Markov chain의 상태 r은 MN의 현재 위치와 중앙 셀 사이의 거리로 정의하고[5], 이 값은 현재의 MN의 위치를 나타내는 인덱스로 사용한다. 결과적으로, MN이 상태 r이라는 것은 MN이 현재 range ring r에 있다는 것을 의미한다.

다음의 식에서 상태 천이 확률 $\alpha_{r,r+1}$와 $\beta_{r,r-1}$은 MN이 중앙 셀부터 떨어진 거리를 나타내는 확률을 각각 나타낸다.

$$\alpha_{r,r+1}=\begin{cases}(1-q) & \text{if } r = 0\\ (1-q)p^{+}(r) & \text{if } 1 \le r \le R\end{cases} \quad (2)$$

$$\beta_{r,r-1}=(1-q)p^{-}(r) \qquad \text{if } 1 \le r \le R \quad (3)$$

여기서 q는 앞서 말했듯이 MN이 네트워크에 그대로 머무를 확률을 나타낸다.

MAP 도메인의 크기가 range ring R 내에서 상태가 r인 steady-state 확률을 $P_{r,R}$이라고 가정하면, 식 (2), (3)과 steady state 확률 $P_{0,R}$에 의해 $P_{r,R}$은 다음과 같다[4,10].

$$P_{r,R}=P_{0,R}\prod_{i=0}^{r-1}\frac{\alpha_{i,i+1}}{\beta_{i+1,i}} \qquad \text{for } 1 \le r \le R \quad (4)$$

여기서 $P_{0,R}$은 $\sum_{r=0}^{R}p_{r,R}=1$ 이므로 다음과 같다.

$$P_{0,R}=\frac{1}{1+\sum_{r=1}^{R}\prod_{i=0}^{r-1}\frac{\alpha_{i,i+1}}{\beta_{i+1,i}}} \quad (5)$$

4.2 비용 함수

제안하는 시스템의 비용을 비교 분석하기위해 본 논문에서는 다음 그림과 같은 시스템 모델을 가정한다.

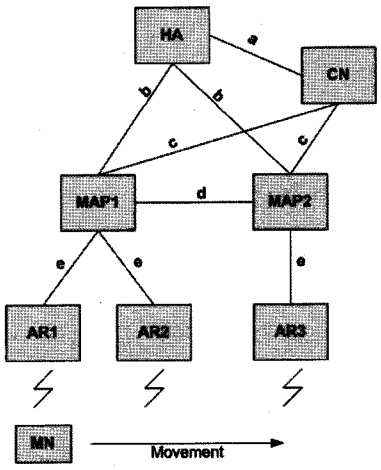

그림 8 HMIPv6의 시스템 모델

그림에서 소문자 알파벳은 구성 노드간의 전송 비용을 의미한다.

HMIPv6 시스템에서 네트워크를 이동할 때의 비용은 위치 등록 비용($C_{location}$), 패킷 전달 비용(C_{packet}), SA 체결 비용($C_{SA\#}$)으로 나누어진다. 그러므로 총 핸드오프 비용, C_{total}은 다음과 같다.

$$C_{total}=C_{SA\#}+C_{location}+C_{packet} \quad (6)$$

4.2.1 위치 등록 비용

C_g와 C_l은 각각 글로벌 위치등록 비용, 지역 위치 등록 비용을 의미한다고 할 때, 전통적인 IP 네트워크에서는 두 노드간의 거리에 비례해서 시그널링 비용이 증가한다는 것에 의해 C_g와 C_l는 다음 식과 같다.

$$C_g=2\cdot(\kappa\cdot f+\tau\cdot(b+e))+PC_{HA}+C_l \quad (7)$$

$$C_l=2\cdot(\kappa\cdot f+\tau\cdot e)+PC_{MAP} \quad (8)$$

위식에서 τ 는 유선에서 전송 비용, κ 는 무선에서 전송비용을 나타낸다. 그리고 b, e, f는 노드간의 거리, 즉 전송 비용을 의미한다. PC_{HA}와 PC_{MAP}는 각각 HA

와 MAP에서의 처리 비용을 의미한다. Random Walk Mobility 모델에 의해, MN이 MAP 사이(Inter-MAP handoff)의 이동을 할 확률은 $p_{R,R} \cdot \alpha_{r,r+1}$와 같다. 만약 MN이 range ring R 내에 있고, MAP 도메인의 범위가 R이라고 가정할 때, range ring R이 range ring R+1이 되는 이동은 MN이 MAP간의 이동을 한다는 것을 의미한다. 그 외의 경우는 MN은 MAP 도메인 내에서 이동하는 경우이다. 이때는 지역 위치 등록만 수행하면 된다. 위의 내용을 고려하면 위치 등록 비용, $C_{location}$은 아래의 식과 같다.

$$C_{location} = \frac{p_{R,R} \cdot \alpha_{R,R+1} \cdot C_g + (1 - p_{R,R} \cdot \alpha_{R,R+1}) \cdot C_l}{T} \quad (9)$$

T는 MN이 셀에 머무는 평균 시간을 의미한다.

4.2.2 패킷 전송 비용

C_{MAP}과 C_{HA}을 각각 MAP과 HA의 패킷 전송을 위한 처리 비용 이라고 할 때, 패킷 전송 비용은 다음과 같다.

$$C_{packet} = C_{MAP} + C_{HA} \quad (10)$$

HMIPv6 시스템에서는 MAP은 RCoA를 LCoA로 또는 LCoA를 RCoA로 변경하는 매핑 테이블을 관리한다. 이 매핑 테이블은 HA가 가진 Bind Cache와 비슷한 역할을 한다. MAP에서의 처리 비용을 계산할 때, 매핑 테이블에서 값을 찾는 시간이 고려 되어야한다. 또한 변경된 주소로 라우팅하는 비용도 고려되어야 한다. 그러므로 C_{MAP}은 매핑 테이블에서 값을 찾는 시간, C_{lookup}과 라우팅 비용, $C_{routing}$의 합으로 계산 된다. 이때 C_{lookup}은 매핑 테이블의 크기에 비례해서 커지게 될 것이며, 매핑 테이블이 크다는 것은 MAP 도메인 내에 관리하는 MN의 수가 많다는 것과 같은 의미이다. 그래서 MAP 도메인 내의 AR의 평균 개수를 N_{AR}, 하나의 AR 내의 평균 MN의 개수를 K이라고 하면, MAP 도메인 내의 MN의 개수는 N_{MN}이 된다고 할 때 다음과 같은 식이 된다.

$$N_{MN} = N_{AR} \times K \quad (11)$$

또한 $C_{routing}$은 MAP도메인 내의 AR의 개수에 대해 로가리즘(logarithm)하게 증가하게 된다[4].

위의 내용을 고려하여 C_{MAP}을 계산 하면 식 (12)와 같이 되며, λs는 패킷 도착률을, S는 패킷의 평균 크기를 나타낸다. 또한 α 와 β 는 weighting factor이다.

$$\begin{aligned} C_{MAP} &= \lambda_s \cdot S \cdot (C_{lookup} + C_{routing}) \\ &= \lambda_s \cdot S \cdot (\alpha N_{MN} + \beta \log(N_{AR})) \end{aligned} \quad (12)$$

한편, CHA는 다음과 같다.

$$C_{HA} = \lambda_s \cdot \theta_{HA} \quad (13)$$

기존의 MIPv6 시스템에서는 경로 최적화 (route optimization)을 사용하므로, 첫 번째 패킷만이 HA를 통해 전송되고 나머지는 모두 MN에게 직접 전송되므로 위와 같이 계산된다. 여기에서 G_{HA}는 HA에서 패킷 처리 비용이다.

4.2.3 SA 체결 비용

제안하는 시스템의 성능을 비교 분석 하기위해 기존에 제안된 3가지 시스템과 본 논문에서 제안하는 시스템의 C_{SA}를 계산하였다. $C_{SA\#}$에서 #은 본 논문에 나타나는 순서를 의미한다. 예를 들어 C_{SA2}는 "CGA와 CBI을 이용하여 MN과 MAP간의 SA를 체결하는 방법"의 SA 체결 비용을 의미한다. SA를 협상하는 확률은 MN이 이동하는 확률과 관계가 있으므로 다음과 같이 계산된다.

$$C_{SA\#} = \frac{p_{R,R} \cdot \alpha_{R,R+1} \cdot C_{SA\#\_g} + (1 - p_{R,R} \cdot \alpha_{R,R+1}) \cdot C_{SA\#\_l}}{T} \quad (14)$$

$C_{SA\#_g}$은 MN이 MAP간 이동할 때의 SA 체결 비용을, $C_{SA\#_l}$은 MAP내에서 이동할 때의 비용을 의미하고 다음과 같이 각각 계산된다.

$$\begin{aligned} C_{SA1\_g} &= 2 \cdot 2 \cdot (\kappa \cdot f + \tau \cdot e) + 5 \cdot PC_{SA} \\ &\quad + 2 \cdot (\kappa \cdot f + \tau \cdot (b + e)) + 3 \cdot PC_{SA} \end{aligned} \quad (15)$$

$$C_{SA1\_l} = 2 \cdot (\kappa \cdot f + \tau \cdot e) + 3 \cdot PC_{SA} \quad (16)$$

$$\begin{aligned} C_{SA2\_g} &= 2 \cdot (\kappa \cdot f + \tau \cdot (b + e)) \\ &\quad + 3 \cdot PC_{SA} + C_{SA2\_l} \end{aligned} \quad (17)$$

$$\begin{aligned} C_{SA2\_l} &= 4 \cdot PC_{SA} + 2 \cdot (\kappa \cdot f + \tau \cdot e) \\ &\quad + 2 \cdot (\kappa \cdot f + \tau \cdot e) + 3 \cdot PC_{SA} \end{aligned} \quad (18)$$

$$\begin{aligned} C_{SA3\_g} &= 4 \cdot 2 \cdot (\kappa \cdot f + \tau \cdot e) + 9 \cdot PC_{SA} \\ &\quad + 2 \cdot (\kappa \cdot f + \tau \cdot (b + e)) + 3 \cdot PC_{SA} \end{aligned} \quad (19)$$

$$C_{SA3\_l} = 2 \cdot 2(\kappa \cdot f + \tau \cdot e) + 5 \cdot PC_{SA} \quad (20)$$

$$\begin{aligned} C_{SA4\_g} &= 2 \cdot (\kappa \cdot f + \tau \cdot e) + 2 \cdot (\kappa \cdot f + \tau \cdot (b + e)) \\ &\quad + 3 \cdot PC_{SA} \end{aligned} \quad (21)$$

$$C_{SA4\_l} = 2 \cdot (\kappa \cdot f + \tau \cdot e) + PC_{SA} \quad (22)$$

5. 성능 평가 결과

이 장에서는 앞에서 설명한 식을 바탕으로 제안한 시스템과 기존의 시스템의 성능을 비교 분석하였다. 표 1은 성능 분석을 위해 필요한 파라미터 값이며, [4,6,7]을 참조하였다. ***a, b, c, d, e, f*** 는 각 노드 사이의 홉 수를 고려한 전송 비용을 의미하며, 표 1처럼 가정하였다.

τ 는 유선에서 전송 비용, κ 는 무선에서 전송비용을 의미하며, 무선 네트워크는 일반적으로 유선 네트워크보다 전송 에러가 많으므로 표 1처럼 가정하였다. PC_{HA}, PC_{MAP} 는 각각 HA와 MAP에서의 처리 비용을 의미하고, PC_{SA} 는 노드에서 보안을 위해 계산하는 비용을 의미한다. MAP은 HA보다 관리하는 MN의 개수가 작으므로 표 1처럼 가정하였으며, 보안을 위한 계산량 또한 많은 자원을 사용하므로 표 1처럼 가정하였다.

표 1 성능 평가를 위한 파라미터 값

Parameter	Value	Parameter	value
α	0.1	c	4
β	0.2	d	1
γ	0.05	e	2
θ_{HA}	20	f	1
τ	1	PC_{HA}	24
κ	2	PC_{MAP}	12
a	6	PC_{SA}	24
b	6		

그림 9는 Random-Walk Mobility 모델에서 MN이 네트워크에 머무르는 시간에 따라 전체 핸드오프 비용(Total Cost)의 변화를 그래프로 나타낸다. 모든 시스템에서 전반적으로 전제 핸드오프 비용은 네트워크에 머무르는 시간이 길면 길수록 낮아지는 것을 알 수 있다. 네트워크에 머무르는 시간은 곧 MN이 이동하는 횟수가 적다는 것으로 생각하면 결과를 쉽게 이해할 수 있다.

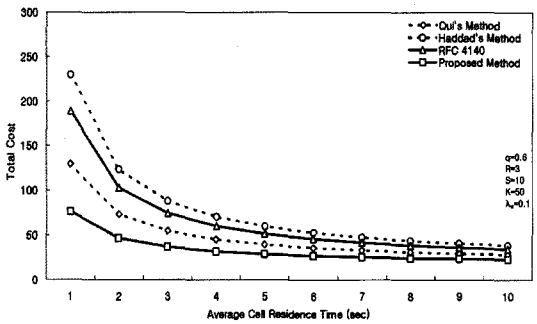

그림 9 MN의 네트워크에 머무르는 시간(T)에 따른 전체 핸드오프 비용 (q=0.6, R=3)

식 (23)은 제안하는 시스템과 기존 시스템의 성능을 비교하기 위한 것이다.

$$\text{성능향상}(\%) = 1 - \frac{\text{제안시스템의 } C_{total}}{\text{기존시스템의 } C_{total}} \quad (23)$$

식 (23)을 사용하여 분석하면, 제안하는 시스템은 Qui의 방법과 비교할 때에 최대 41%에서 최소 20%까지, Haddad의 방법과 비교할 때에 최대 67%에서 최소 42%까지, RFC4140의 방법과 비교할 때에 최대 60%에서 최소 35%까지 전체 핸드오프 비용을 줄일 수 있는 것을 알 수 있다.

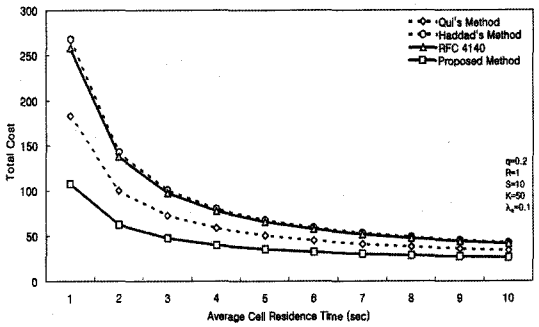

그림 10 MN의 네트워크에 머무르는 시간(T)에 따른 전체 핸드오프 비용 (q=0.2, R=1)

그림 10은 q 와 R 값을 제외하고 그림 9의 실험과 동일한 파라미터를 사용한 결과 이다. q 값이 작은 것은 MN이 자주 이동한 한다는 것을 의미하고, R 값이 작은 것은 MAP 도메인의 크기가 작아진 것을 의미한다.

MN이 자주 이동하면서 MAP 도메인의 크기가 작을 경우는 Inter-MAP 이동이 자주 발생하게 된다. Qui의 방법과 RFC4140의 방법은 거의 동일한 성능을 나타낸다.

전체적으로 Inter-MAP 이동이 잦아지게 되면 시스템의 성능은 전반적으로 낮아지게 된다. 그림 9와 그림 10을 비교하면, Haddad의 방법, 제안하는 방법은 Inter-MAP 이동이 잦아져도 성능에 미치는 영향이 적은 반면, RFC4140의 방법, Qui의 방법은 크게 성능이 저하되었다.

6. 결 론

현재 MIPv6에서 이동 성능을 향상시키기 위한 많은 방법이 연구, 제안되고 있다. 그중 HMIPv6는 MN의 이동성 관리를 지역에 MAP이라는 노드를 배치하여 이동 성능을 향상 시킨 시스템이다. 하지만 MN과 MAP 사이의 보안이 취약 할 경우 여러 가지 보안 문제가 발생하게 된다. 본 논문에서는 이미 제안된 보안 기법을 분석하여 새로운 보안 시스템을 제안하였다. 제안 시스템을 기존의 시스템과 비교 분석하기위해 수학적으로 시스템을 모델링하고, Random-Walk Mobility 모델을 기

반으로 이동성을 모델링하였다. 실험 결과, 제안한 시스템은 기존의 시스템과 비교하여 최대 58%, 최소 22%의 전체 핸드오프 비용을 줄일 수 있음을 수학적으로 성능 분석하였다.

참 고 문 헌

[1] D. B. Johnson and C. E. Perkins, "Mobility support in IPv6," IETF RFC 3775, June, 2004.

[2] H. Soliman, C. Castelluccia, K. El Malki, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," RFC 4140, Aug. 2005.

[3] Kent, S. and R. Atkinson, "IP Authentication Header," RFC 2402, Nov. 1998.

[4] Sangheon Pack and Yanghee Choi, "A study on performance of hierarchical mobile IPv6 in IP-based cellular networks," IEICE Transactions on Communications, vol. E87-B no. 3 pp.462-469, Mar. 2004.

[5] I.F. Akyildiz and W. Wang, "A dynamic location management scheme for next -generation multitier PCS systems," IEEE Trans. Wireless Commun., vol.1, no.1, pp.178-189, Jan. 2002.

[6] M. Woo, "Performance analysis of mobile IP regional registration," IEICE Trans. Commun., vol.E86-B, no.2, pp.472-478, Feb. 2003.

[7] X. Zhang, J.G. Castellanos, and A.T. Capbell, "P-MIP: Paging extensions for mobile IP," ACM Mobile Networks and Applications, vol.7, no.2, pp.127-141, 2002.

[8] Jose Caldera, Dionísio de Niz, and Junichi Nakagawa "Performance Analysis of IPsec and IKE For Mobile IP on Wireless Environments," http://www-2.cs.cmu.edu/~dionisio/personal-publications.html

[9] D. Harkins and D. Carrel, "The Internet Key Exchange," IETF RFC 2409, November, 1998.

[10] Jonghyoun choi and Youngsong Mun, "An Efficient Handoff Mechanism with Web Proxy MAP in Hierarchical Mobile IPv6," ICCSA2005, LNCS 3480, pp.271-280, May 2005.

[11] Feng Bao, Robert Deng, Ying Qiu and Jianying Zhou, "A Scheme for the Security between Mobile Node and Mobility Anchor Point in Hierarchical Mobile IPv6," IETF Internet draft, draft-qiu-mipshop-mn-map-security-00.txt (work in progress), Oct. 2005.

[12] W. Haddad and S. Krishnan, "Combining Cryptographically Generated Address and Crypto -Based Identifiers to Secure HMIPv6," IETF Internet draft, draft-haddad-mipshop-hmipv6-security-01 (work in progress), Oct. 2005.

[13] J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)," IETF RFC 3971, March, 2005.

최 종 현

2001년 숭실대학교 컴퓨터학부 학사. 2003년 숭실대학교 컴퓨터학부 석사. 2003년~현재 숭실대학교 컴퓨터학부 컴퓨터통신 박사과정. 관심분야는 IPv6, Mobile IPv6, Grid, 네트워크 보안, 광 네트워크

문 영 성

1983년 연세대학교 전자공학 학사. 1986년 캐나다 Univ. of Alberta 전자공학 석사. 1993년 Univ. of Texas, Arlington 컴퓨터공학 박사, 1992년 미국 Supercomputing 학술대회 최우수 학생 논문상 수상. 1994년~현재 숭실대학교 컴퓨터학부 부교수. Journal of Supercomputing 편집위원. 관심분야는 Mobile IPv6, IPv6, GRID networking