MIPv6에서 보안성을 향상시킨 효율적인 핸드오버 메커니즘

정윤수° 우성희 이상호
충북대학교
bukmunro@netsec.cbnu.ac.kr°, shwoo@cnu.ac.kr, shlee@chungbuk.ac.kr

AN Efficient Handover Mechanism Enhanced Security in MIPv6

Yoonsu Jeong°. Sunghee Woo. Sangho Lee
Chungbuk National University

요 약

무선으로 인터넷에 접속하는 사용자와 서비스의 급격한 증가로 인하여 차세대 인터넷 주소 체계인 IPv6가 제안되었다. 현재 IPv6의 기능들을 사용하면서 효과적으로 이동성을 제공하기 위한 해결책으로 Mobile IPv6(MIPv6)가 제안되고 있다. 하지만 MIPv6는 핸드오프와 관련된 동작을 하는 동안, 일정 시간 동안 통신이 불가능해짐으로 인해, 끊김 없는 통신 서비스를 제공하지 못하는 단점이 있다. 이 논문에서는 기존의 MIPv6 문제점을 해결하기 위해 context와 쿠키 정보를 이용하여 이동노드의 시그널 재초기화 과정을 없애고 패킷 손실 및 지연을 줄인 효율적이고 안전한 핸드오버 메커니즘을 제안한다.

1. 서 론

이동 통신망 기술이 발전함에 따라 이동 호스트(MN) 사용에 대한 요구가 증가하고 있으며, 호스트의 이동에 상관없이 통신이 가능하도록 하는 기법에 대한 관심이 높아지고 있다. 이를 위해, IETF에서는 핸드오프 시에도 이동 호스트의 위치를 관리하여 끊임없는 통신을 제공하는 Mobile IPv6 프로토콜을 제안하였다[2,3,5].

MIPv6[1]는 IPv6의 기능들을 그대로 이용하면서 이동성을 제공하고자하기 때문에 MIPv6보다 효과적으로 이동성을 지원할 수 있으며 탁월한 규모 확장성을 지니고 있다. 하지만 이러한 MIPv6는 MN(Mobile Node)이 핸드오프를 수행할 때 지연 시간이 발생하게 되며, 이는 통신 서비스를 수행중인 MN의 경우 데이터 손실이 초래된다. 따라서 이러한 지연 시간을 줄이는 연구가 많이 진행되고 있다.

이 논문에서는 MIPv6의 단점을 개선하기 위해 효율적이고 안전한 핸드오프 메커니즘을 제안한다. 제안 메커니즘에서는 효율적이고 안전한 핸드오프 처리를 제공하기 위해 context 정보를 이용하여 이동노드의 시그널 재초기화 과정을 없애고 패킷 손실 및 지연을 줄였다. 또한 FMIPv6 핸드오프 과정을 선 처리하여 핸드오프 지연을 줄였다.

이 논문의 구성은 다음과 같다. 2장에서는 핸드오프 시간과 MIPv6 프로토콜에 대해 살펴보고, 3장에서 context와 쿠키정보를 이용한 MIPv6 핸드오프 메커니즘을 제안한다. 4장에서는 제안 프로토콜의 성능을 평가하고, 5장에서 결론을 맺도록 한다.

2. 관련연구

2.1 MIPv6

MIPv6는 IPv6의 기능을 그대로 이용하면서 이동성을 제공하고자 하기 때문에 MIPv4보다 효과적으로 이동성을 지원할 수 있으며 탁월한 확장성도 지니고 있다. Neighbor Discovery와 Address Autoconfiguration 기능을 이용하여 이동 단말이 이동하였을 때 자도응로 자신의 위치 정보를 구성할 수 있도록 하였으며, 자신이 이동한 위치 정보를 필요한 노드들에게 알릴 수 있도록 Destination 옵션을 추가함으로써, IPv4에서는 필요했던 일부 시그널 메시지들과 에이전트를 제거하였다. 또한 Route Optimization을 위한 프로토콜이 기본 기능으로 제공되고 있다. MIPv6는 홈 에이전트(HA), 홈 네트워크, Correspond Node(CN), CoA(Care Of Address)드의 MIPv4의 기본개념을 그대로 수용하고 있다. MN은 이동하면서 방문 링크로부터 CoA를 획득하고 HA에게 이동 서비스를 요청하는 객체이다. 홈 네트워크를 떠나면 MN은 먼저 Neighbor Discovery 메커니즘을 통해 이동을 감지하고, 로컬 라우터에서는 ICMPv6 Router Advertisement 메시지를 주기적으로 보낸다. MN은 Stateless나 Stateful Address Autoconfiguration을 통해 새로운 CoA를 획득한다. 그리고 MN은 Binding Update(BU) 메커니즘을 통해 HA에 새로운 CoA를 등록한다. MN은 BU 메시지를 Binding ACK(BA) 메시지가 되돌아 올 때까지 HA에 보내고, 이 후 MN의 홈 어드레스와 CoA가 Binding 되고 HA의 캐쉬에 등록된다. HA라는 홈 네트워크 상의 라우터는 등록된 CoA의 Binding Cache를 유지한다. 등록 후 HA는 MN에게 오는 패킷을 터널링하여 MN에 보낸다. MN은 소스 어드레스처럼 CoA를 사용하여 패킷을 CN에게 직접 전달 할 수 있고, CN이 패킷의 근원지를 식별할 수 있도록 MN은 Destination Options안에 홈 어드레스를 실어 보낸다.

2.2. 핸드오프 지연시간

핸드오프 지연 시간이란 MN이 현재 네트워크에서 다른 네트워크로 이동하는 동안 통신을 할 수 없게 되는 기간을 말한다. MIPv6에서 이 핸드오프 지연 시간은 크게 L2 핸드오프 지연 시간과 L3 핸드오프 지연 시간으로 나뉜다.

L2 핸드오프 지연 시간은 MN이 실제로 현재 AR과 연

결을 끊고 핸드오프해 간 AR과 연결을 맺는데 걸리는 시간으로, IEEE 801.11 WLAN에서는 probe 지연 시간, 인증(authentication) 지연 시간, 협력(association) 지연 시간으로 나뉜다. 먼저, MN은 핸드오프 할 적절한 Access Point(AP)를 찾기 위해 채널을 검색하게 되는데, 존재하는 모든 채널을 검색한다. MN이 적절한 AP를 찾게 되면, 그 AP와 authentication에 관련된 정보를 주고 받고, 실제로 연결을 맺게 된다. [1]에서 살펴볼 수 있듯이 L2 핸드오프 지연 시간 중 채널 검색을 위한 probe 지연 시간이 가장 길다는 것을 알 수 있다.

L3 핸드오프 지연 시간은 이동 탐지(Movement Detection) 지연시간, 복사주소 탐지(Duplicate Address Detection(DAD) 지연 시간, 바인딩 업데이트(Binding Update) 지연 시간으로 나뉜다. MD 지연 시간은 MN이 IPv6 Router Discovery 기법을 사용하여 핸드오프한 사실을 알게 되기까지 걸리는 시간이다. 그리고 나서, MN은 새로운 주소(NCoA)를 생성하는데 이 주소를 검증하는데 걸리는 시간이 DAD 지연 시간이다. 검증된 주소는 HA에게 등록되어야 하는데, 이 때 걸리는 시간이 BU 지연 시간이다.

3. context와 쿠키 정보를 이용한 MIPv6 핸드오프 메커니즘

이 절에서는 ConText 정보와 쿠기 정보를 이용하여 FMIPv6의 기능을 통합한 제안 방식의 기본 모델을 설명한다. 제안된 모델은 HO가 발생한 후 바로 NewCoA의 CN에게 정보를 알린다. CN과 MN 사이의 최적 라우트를 빠르게 찾기 위해서 라우트 서브넷의 라우팅 알고리즘을 사용한다. 또한, OldAR에서 NewAR로 패킷을 포워딩 하였을 때 야기되는 패킷 지연을 최소화한다.

3.1 가정

제안된 MIPv6 기본 모델의 핸드 오버 처리 메커니즘의 가정은 아래와 같다.

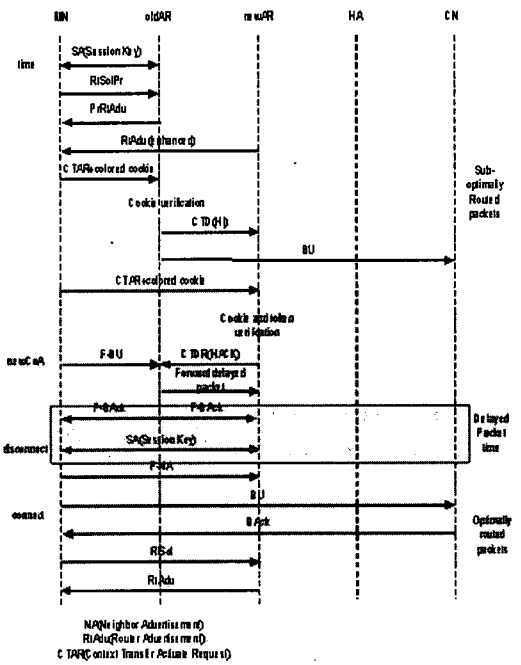
① L2는 핸드오버 이벤트가 발생할 경우에 미리 L3을 시그널 할 수 있다.
② L2는 AR(Access Router)들이 서로 연결될 수 있도록 IPv6 주소의 액세스 포인트 인식자와 매핑할 수 있는 정보를 제공한다.
③ MN는 주어진 특정 시간에 액세스 포인트의 액티브 L2 링크을 가지는데 단일 링크를 사용된다.

위와 같은 가정에서, MN이 MIPv6 서비스의 두 공급자 사이의 경계를 이동하려 할 때 공급자는 이웃의 액세스 정보와 관련된 매핑 정보를 서로 제공할 것이다.

3.2 제안 메커니즘

[5]에서 제안된 기법을 기반으로 CT의 주요 이슈들을 해결하기 위한 방안으로 CT와 FMIPv6을 통합하였으며, 통합된 모델은 [그림 1]과 같다. 제안 모델과 FMIPv6 모델의 주된 차이점은 데이터 링크(L2)로부터 HO-warning 후에 곧바로 oldAR에서 CN로 BU를 보낸다. 비록 패킷이 oldAR에서 newAR로 터널되더라도 MIPv6 모델과 비교하여 많은 차이점이 없다. 패킷들이 지연될 동안의 총 시간은 FMIPv6 모델[4]과 비교할 때 보다 더 짧다.
제안 모델의 목표는 HOgn에 곧바로 newCoA의 CN에게 정보를 알리는 것이다. 이것은 MN을 통해 BUs를 보내는 AR을 통해 수행된다. MN의 BU 리스트는 AR에서 복사된다. 이 복사는 초기 MN의 관리와 동일한 방법으로 AR-proxy에 의해 관리되어야 한다. 이 복사는 주기적으로 초기와 동기화한다.
HO-event가 탐지되고 newCoA가 AR에 의해 생성되자마자 BU 리스트의 복사는 모든 액티브 CN을 NewCoA에게 알리는데 사용된다.
MN이 핸드오버 처리를 초기화하기 전에, MN은 세션 키를 공유한 oldAR과 SA를 가진다고 가정하고 MN은 권한 정보를 얻기위해 colored cookie를 부여한다.
효율적이고 안전한 핸드오버 처리를 연구하기 위해 제안된 [그림 1]의 핸드오버 처리는 다음과 같은 이점을 준다.

① CT의 목적은 지연, 패킷 손실을 줄이는 것이고, 이동 노드로부터 노드의 시그널 재설정 과정을 피하는 것이다.
② FMIPv6는 불필요한 링크 스위치 지연과 비교하여 가능한 작게 IP 프로토콜 동작에 의해 발생되는 핸드오버 지연을 줄이는 것이 목적이다.



[그림 1] 제안 핸드오버 처리 기법

제안된 모델의 각각이 처리 과정은 다음과 같다.

· 단계 1 : MN은 RtSolPr 메시지를 보내거나 NewAR로부터 향상된 advertisement를 수신한다. 향상된 advertisement의 정보를 기반으로 핸드오버 결정을 한다.

· 단계 2 : MN은 세션키로 암호화된 CTAR과 clored 쿠키(cookie)를 OldAR에게 메시지를 보낸다. OldAR은 colored 쿠키를 검증한다. 만일 검증이 통과되면 OldAR은 MN을 인증하고 MN의 QoS 요청이 성공적으로 권한을 부여받는다. 그 후 NewAR에게 CTD를 보낸다. 이 메시지는 FMIPv6의 HI처럼 간주될 수 있다. CTD는 세션키등을 포함한 colored 쿠키와 권한 토큰을 검증하기 위해 NewAR에 대한 파라미터를 얻는다.

· 단계 3 : MN은 평문으로 전송되는 CTAR과 colored 쿠키를 포함하여 NewAR에게 메시지를 보낸다. NewAR은 colored 쿠키와 권한 토큰을 검증한다. 만일 검증이 성공적이라면 NewAR은 MN 자신의 context라는 것을 보증한다. 그 때 NewAR은 OldAR에게 FMIPv6의 HACK로 간주되는 CTDR을 보낸다. 그 후 NewAR과 MN은 세션키를 공유함으로써 SA을 설정한다.

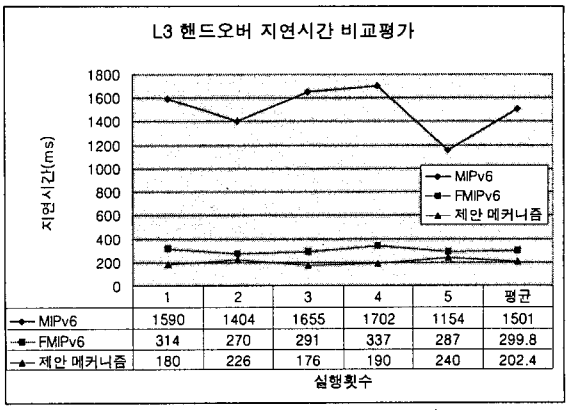
· 단계 4 : MN이 OldAR과 연결이 제대로 이루어지지 않을지라도 OldAR은 패킷 손실의 정도가 크지 않게 NewAR에 패킷을 포워드 한다. 그때 NewAR은 CASP-QoS 클라이언트나 RSVP 프로토콜과 같은 것으로 BU나 QoS 설립 과정을 초기화 한다.

· 단계 5 : 처리가 성공적이었을때, NewAR은 NewCoA을 사용하여 MN을 인식하고 새로운 colored 쿠키를 MN에게 부여한다. NewAR은 MN에게 패킷을 전달하기 시작한다.

4. 평가

이 장에서는 이 논문에서 제안된 메커니즘과 기존의 MIPv6, FMIPv6의 성능을 헬싱키 대학에서 개발한 MIPL MIPv6을 기반으로 비교 분석함으로써, 제안된 프로토콜의 성능이 우수함을 보이고 있다[6].

[그림 2]는 실험의 신뢰성을 높이기 위해 MIPv6, FMIPv6 그리고 제안된 메커니즘의 핸드오프 지연 시간(L3)을 5번 반복 실험하여 실험 결과의 평균치를 구하였다. [그림 2]의 결과에서 볼 수 있듯이 제안 메커니즘은 FMIPv6보다 L3 핸드오버 지연시간이 적다는 것을 쉽게 알 수 있다. 또한 제안 메커니즘의 경우 OldAR의 터널링 서비스를 효율적으로 이용하여 MIPv6와 FMIPv6보다 데이터 지연 시간 및 손실을 13% 줄임으로써, 핸드오버 성능 향상을 꾀하고 있다. 또한, 제안 프로토콜은 FMIPv6에서 지원하지 않는 보안부분을 지원하고 있기 때문에 안전성 측면에서도 기존 메커니즘 보다 우수하다.



	1	2	3	4	5	평균
MIPv6	1590	1404	1655	1702	1154	1501
FMIPv6	314	270	291	337	287	299.8
제안 메커니즘	180	226	176	190	240	202.4

실행횟수

[그림 2] L3 핸드오버 지연시간 비교평가

5. 결 론

이 논문에서는 MN의 핸드오프 속도를 빠르게 하고, 무선네트워크 상에서 교환되는 위치 등록, 시그널링 메시지 수를 context를 이용하여 줄이는 메커니즘을 제시하였다. 제시된 메커니즘은 MIPv6가 차세대 셀룰러 네트워크 기반 기술로 발전함에 따라 신뢰성 있고 빠른 이동성 관리 기술을 제공할 것으로 기대한다.

향후 연구에서는 MIPv6망에서 핸드오프 속도 개선 및 보안 성능 강화뿐만 아니라 QoS보장을 위한 기법에 대해서도연구가 필요하고 제안된 기법에 대해 시뮬레이션을 통하여 실제적으로 어떠한 성능 효과를 나타내는지에 대한 연구가 필요하다.

참고문헌

[1] Johnson. D, and Perkins, C. E., "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-18.txt, IETF, Work In Progress.

[2] Perkins. C.E. (ed.), "IP Mobility Support", RFC 2002, IETF, October 1996.

[3] Thomas. M, "Analysis of Mobile IP and RSVP Interactions", October 2002.

[4] Koodli R., "Fast Handovers for Mobile IPv6", Internet Draft, draft-ietf-mipshop-fast-mipv6-01.txt, January 2004.

[5] Song, L., Kotz, D., Jain, R., He, X., "Evaluating location predictors with extensive Wi-Fi mobility data", Proceedings of the 23rd Joint Conference of the IEEE Comp. and Comm. Societies (INFOCOM). Volume 2. (2004) 1414-1424.

[6] A. J. Tuominen and H. Petander, et al., MIPL Mobile IPv6 for Linux in HUT Laboratory, available from http://www.mobile-ipv6.org