MIPv6 환경에서 VoIP 서비스를 위한 통합 보안 메커니즘 제시와 요구사항 분석

* 서종운 °, * 안태선, * 김지수, * 강현국
* 고려대학교
*{terryortony °, cokein, jissung, kahng}@korea.ac.kr

Scenario Proposal and Requirements analysis of Integrated Secure mechanism for VoIP Services in MIPv6

* Jong-Wun Seo°, * Tae-Sun Ahn, * Ji-Soo Kim, * Hyun-Kook Kahng
* Korea University

요 약

현재 인터넷 서비스의 근간을 형성하고 있는 IPv4 의 가용 주소 공간의 고갈, 보안성의 결여, 그리고 멀티미디어 서비스를 위한 QoS(Quility of Service)의 필요성과 같은 요구사항을 바탕으로 차세대 인터넷 프로토콜(IPv6)로의 전환이 요구되고 있다. 본 연구 목적은 이러한 네트워크상의 이동 인터넷 환경에다 실시간 서비스를 제공할 수 있도록 SIP(Session Initiation Protocol)를 적용하여 통합 된 환경이 이전 보다 안전한 인터넷 정보 서비스를 제공할 수 있도록 보안 메커니즘을 적용 하였다. 네트워크 계층과 응용 계층의 이동성 관리 모델의 통합은 전체적인 시그널링 부하를 줄이고 지속적인 통신을 위한 빠른 핸드오프를 제공한다. 즉, 본 연구는 현재 Mobile IPv6 에서 보안상 취약점으로 나타나는 문제점 및 SIP 보안 고려사항 및 이동성을 해결하기 위해 제안되는 해결방안들을 분석하고 적합한 보안 메커니즘 적용 방안을 제안 하였다.

I. 서론

차세대 정보통신망이 All-IP 망으로 발전하면서 기존의 인터넷 망을 이용한 새로운 서비스에 대한 관심이 높아지고 있으며 최근에는 멀티미디어 실시간 전송이 중요한 이슈로 떠오르고 있다. SIP 는 이러한 멀티미디어 서비스의 일환으로 차세 대 인터넷 서비스 분야에 매우 두각을 나타내고 있으며 VoIP(Voice Over IP)는 특히 SIP 기술의 발전에 의해 그 활용과 응용이 다양해지면서 더욱 주목을 받고 있다.

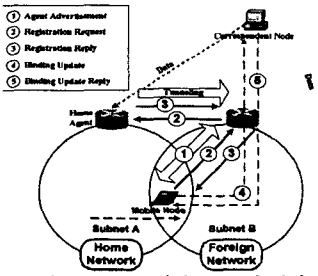
SIP 를 기반으로한 VoIP 는 실시간 서비스를 제공한다. 차세대 통신망으로 발전함으로 인해 이러한 실시간 서비스는 유선망 뿐만 아니라 무선망에서도 필요로 하게 될 것이다. SIP 에 이동성을 부여하는 접근방식은 크게 두 가지가 있는데, 그 하나는 기존의 SIP 를 확장하여 이동성을 부여하는 것이고, 또 하나는 Moblie IP 에 기반하는 방식이 있다. 이 두 접근방식에 근거하여[1] 단말 이동성 제공을 위한 통합 구조를 제안하였으며, 가까운 미래에서는 IPv6 가 도입될 것으로 예상 되므로 네트워크 자체에서 이동성을 제공하는 Mobile IPv6 를 기반으로 접근하는 방식이 합리적일 것이다. 그러나 무선 네트워크에서의 시그널 전송은 어느 누구나 신호를 감지할 수 있기 때문에 안전한 데이터를 전송하는데 어려움이 있다. 이러한 문제 때문에 Mobile IPv6 구조에서 보안은 매우 중요한 요소이다. 현재 IETF 에서는 Mobile IPv6 에 대한 표준화 작업에서 보안 문제를 주요 이슈로 다루고 있다.

본 논문에서는 VoIP 서비스를 위한 단말기의 이동성을 지원하기 위해 Mobile IPv6 기반의 HA 와 SIP 기반의 Registrar 를 통합한 이동 에이전트(MA)와 통합 환경에서의 안전한 서비스 제공을 위한 효율적인 인증 메커니즘을 제시 하고자 한다.

II. 관련 연구

2.1 Mobile IPv6 이동 메커니즘

이동 노드가 새로운 링크로 이동할 때마다 IP 주소를 변경 할 수는 있지만 IP 변경이 일어날 때 마다 TCP 와 같은 상위 프로토콜 계층에서의 연결은 유지될 수 없다. MIPv6 는 상위 프로토콜에 투명성을 가지면서 이동성을 지원하기 위해 설계 되었으며 Home Address Destination 옵션을 정의함으로써 IPv6 노드는 터널링을 사용하지

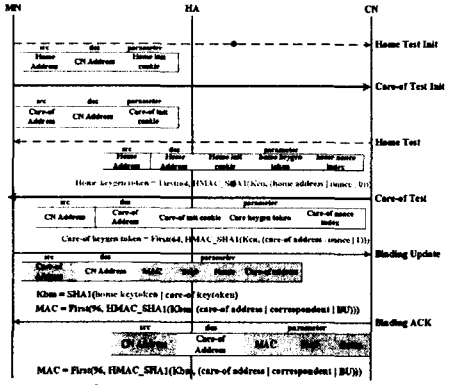


<그림 1. MIPv6 기본 구조 및 절차 >

않으면서 TCP 연결과 같은 상위 계층에서 세션을 유지시킬 수 있다. 그림 1 에서는 MIPv6 의 기본 구조와 절차를 기술한다.

2.2 Mobile IPv6 보안 메커니즘

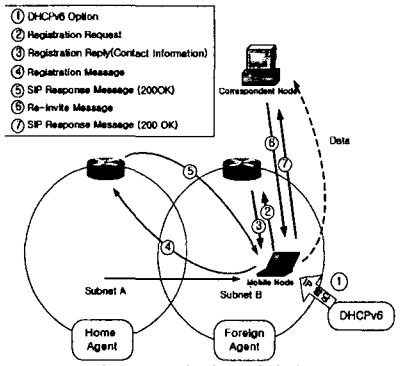
Mipv6 는 특정한 이동 노드의 주소가 자주 변경될 수 있기 때문에 이를 이용하여 해당 노드의 주소를 다르게 알려 줌으로써 해당 노드로의 패킷이 다른 호스트로 전달되게 할 수도 있으며 이동 서비스를 제공 받지 못하도록 할 수 있다. 이러한 Mobile IPv6 가 가지고 있는 전형적인 보안 문제점을 요약해 보자면 크게 3 가지 이슈가 있다. 첫 번째 이슈는 이동환경에서 Home Address Option 을 이용한 공격이고, 두 번째 이슈는 라우팅 헤더를 이용한 공격, 마지막으로 바인딩 갱신(Binding Update)을 수행할 때 발생할 수 있는 공격이 있다. 현재 MIPv6 표준화 진행과정에서 중요히 여겨지는 이슈는 바인딩 갱신에서의 인증 문제가 주를 이루고 있다. 바인딩 갱신은 MN 와 HA 사이, MN 와 CN 사이에서 발생한다. 먼저 MN 와 HA 사이의 바인딩은 IPsec ESP (Encapsulating Security Payload) 프로토콜이 제안되어지며, 두 번째로 MN 와 CN 사이는 RR(Return Routability)가 제안 되어진다.
그림 2 는 MN 가 CN 사이의 RR(Return Routerbility) 과정을 보여준다.



<그림 2. Return Routability Process >

2.3 SIP 이동 메커니즘

비록 SIP 프로토콜과 응용의 설계 목적이 종단 노드들에게 이동성을 부여하지 않았을지라도 현재 SIP 프로토콜에 이동성 지원을 부여하기 위해 연구가 활발히 진행중이다. 그림 3 에서는 종단 이동 성에 관한 SIP 의 기본 아키텍처 및 절차를 기술하였다.
이동노드가 Home 망을 벗어나 새로운 망으로 이동할 때,



<그림 3. SIP 의 이동 메카니즘 >

MN 은 새로운 주소(CoA)를 DHCP 서버로부터 할당 받게 된다[5]. 새로운 IP 를 할당받은 MN 은 이동한 망에 있는 proxy 서버와의 인증절차를 거치게 되며 이때 인증절차는 HTTP 인증절차를 따른다. 이러한 인증과정 이후에 MN 은 이동한 망의 Registrar 로부터 Contact 정보를 Registration 메시지를 통해 전해 받게 된다. MN 은 망 이동을 통해 얻은 새로운 정보(CoA, Contact URI)를 포함한 Registration 메시지를 홈 레지스트라에게 보내고, 진행중인 세션의 CN 에게는 세션 재설정 메시지를 보내게 된다. 이때 홈 레지스트라에서 등록 메시지를 통해 갱신된 정보는 다음 의 새로운 세션이 정확한 새로운 주소로 변경이 되어지도록 홈 레지스트라에게 등록되며, CN 에게 보낸 세션 재설정 메시지는 다음 홉에게 패킷을 전달하기 위한 MN 의 새로운 IP 주소를 포함한다.

2.4 SIP 보안 메커니즘

SIP 에서의 신호에 대한 보안은 크게 End-to-End 보안과 Hop-by-Hop 신호 보안으로 구분 할 수 있다. End-to-End 보안 메커니즘으로는 Digest, Hop-by-Hop 보안 메커니즘으로는 IPSec, TLS 가 사용 되어진다.

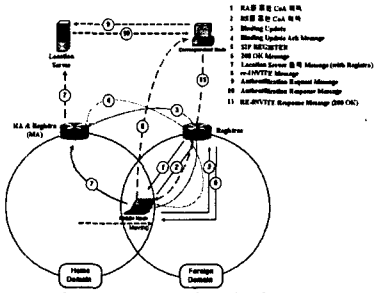
SIP 보안에서는 기본적으로 메시지에 대한 기밀성과 무결성을 지원하여 메시지 변조와 같은 공격으로부터 보호하고, 메시지에 대한 인증을 통해 공격을 차단 해야 한다. 이를 위한 SIP 메시지 전체에 대한 암호화는 메시지에 대한 기밀성을 보장하여 네트워크 상의 정보 누출을 방지하지만 Proxy 서버에서 SIP 메시지의 헤더에 있는 라우팅 정보를 확인 할 수 없어 메시지의 정확한 전달에 문제가 발생한다. 따라서 Proxy 서버와 SIP UA(User Agent)간 상호 신뢰하기 위한 방법으로 IPSec 이나 TLS 와 같은 네트워크나 트랜스포트 레이어 보안 프로토콜을 적용하여 홉간의 메시지 기밀성과 무결성을 지원한다.

End-to-End 암호화 방법으로는 프락시에서 SIP 메시지를 변경하거나 분석 할 수 있도록 라우팅 관련 헤더부분을 제외한 부분을 S/MIME 을 사용하여 암호화 하여 전송한다. S/MIME 은 End-to-End 간의 메시지에 대한 기밀성과 무결성을 지원한다.

SIP 에서는 메시지 변조를 통한 서비스 방해나 Replay 공격을 방지하기 위해 메시지에 대한 인증 메커니즘을 지원하고 있으며 이를 위해 HTTP 에서 사용하는 인증 방법인 Digest 인증 방법을 적용하고 있다.

3. 통합 MIP-SIP 구조 와 위치관리 서버 제안

제안된 통합 SIP-MIP 이동성 관리 방식의 네트워크 구조는 그림 4 에 나타나 있다.
이 구조는 위치관리를 돕기 위한 SIP 네트워크 서버, 통합



< 그림 4. 제안된 통합보안 메커니즘 >

된 Home 에이전트와 SIP 레지스트라(MA), 인증 및 MN 의 위치 관리를 위한 Location 서버를 사용하였다. 통합된 HA 와 SIP 레지스트라는 SIP 와 MIP, 두 프로토콜 모두를 위한 위치등록, 위치 갱신 그리고 위치질의를 담당한다. 우리는 통합된 HA 와 SIP 레지스트라를 간단히 MA(Mobile Agent)로 간주한다.

MIPv6 에서의 등록과정은 이동노드의 새로운 IP 주소를 알리고 MN 의 홈 주소와 현재의 CoA 사이의 바인딩 정보를 갱신하기 위함이다. 이것은 TCP 연결과 비 SIP UDP 스트림이 이동후에 유지되도록 한다. 반면, SIP 세션 재설정의 목적은 CN 에게 SIP 세션의 설정과 MN 의 새로운 현재 IP 주소를 알리는 것이다. 이것은 CN 들이 설정된 미디어 스트림과 시그날링 세션들을 MN 의 현재 IP 주소에 직접적으로 재경로 설정을 하도록 한다. 우리의 제안된 이동 에이전트는 이동 VoIP 서비스를 위한 두 접근방법의 이점을 얻기 위해 MIPv6 의 홈 에이전트와 SIP 레지스트라의 기능을 통합하였다. 우리의 방법은 이동성 관리 지원을 위한 주소 바인딩 메커니즘에 중점을 두었으며, 통합된 MA 는 두가지 타입의 바인딩을 유지한다. SIP 레지스트라에서의 바인딩과 유사한 " 사용자 주소 바인딩" 은 사용자 수준의 SIP 식별자들과 노드의 임시 IP 주소를 매핑한다. MIP Home 에이전트에서의 매핑과 유사한 " IP 주소 바인딩" 은 노드를 식별하는 영구적인 IP 주소와 임시 보조 주소 사이의 바인딩이다. 이동 사용자는 음성과 다른 TCP 기반, 비 SIP 설정 서비스들(예, 텍스트 메시지, WWW 접속등)을 모두 접속하기를 원하기 때문에 이동성 에이전트는 이러한 두가지 바인딩 메커니즘을 동시에 지원하여야만 한다. 그림 5 는 우리의 통합된 이동성 에이전트에서의 이동성 바인딩 테이블을 설명하고 있다. 이 테이블의 목적은 이동노드의 영구적 IP 주소(홈 IP)와 현재 할당된 이동 IP 주소(현재 위치 또는 연결된 보조주소)를 매핑하고 이에 따라 패킷을 전달하는 것이다. 또한, 이 테이블은 이동사용자의 영구적인 주소(Contact URI)와 현재의 할당된 이동 IP 주소(현재위치)사이의 바인딩을 지원하기 위해 사용된다. 전자는 IP 주소 (현재위치) 사이의 바인딩을 지원하기 위해 사용된다. 전자는 IP 주소 바인딩을 위해 디자인 된 것이고, 후자는 사용자 주소 바인딩을 위해 정의된 것이다.

User URI	Contact URI	Home Address	Current Location (CoLocated CoA)	CoA	Lifetime

<그림 5. 홈에이전트의 이동성 바인딩 테이블>

이동노드가 Home 망을 벗어나 새로운 망으로 이동할 때, MN 은 Router Advertisement 또는 Router Solicitate 를 이용 이동한 망의 정보(prefix)를 얻는다. 이 정보를 바탕으로 임시 IPv6 주소(CCoA)를 생성하고 MA 에 Binding Update 메시지를 보낸다. Binding Update 메시지를 수신한 MA 는 Binding ACK 를 MN 에게 보내고 이를 수신한 MN 은 외부망의 Registrar 에게 Registration 메시지를 보내 Contact 정보를 획득한다. 이때 MN 은 새로운 SIP 세션이 이동한 위치로 전달되도록 MA 에 등록하기 위하여 Registration 메시지를 통해 보내게 되고 CN 에게는 Re-Invite 메시지를 보내어 이전 세션을 재설정을 위한 요청을 하게 된다. Registration 메시지를 받은 MA 는 MN 에 위치정보를 등록하고 이를 Location 서버에 저장한다. MN 으로부터 Re-Invite 메시지를 받은 CN 은 Re-Invite 메시지를 보낸 CN 이 이전 세션과 동일한 세션의 INVITE 메시지인지를 판단하고(Re-Invite 메시지인지를 판단) 동일한 세션에 대한 Invite 메시지인 경우 Location 서버에게 CN 에 대한 인증을 요청한다. Location 서버로부터 인증확인 메시지를 받은 CN 은 진행중인 세션을 새로운 MN 의 위치로 갱신시킨다.

이러한 접근방법을 통해, 우리는 MIP 의 빠른 CoA 바인딩을 연구하고 설정된 미디어 스트림을 재 지정하기 위한 SIP 의 능력을 연구함으로서 이동 노드측의 계속되는 터널링 데이터 패킷들을 회피하여 가능한 가장 빠른 SIP 기반의 VoIP 세션의 핸드오프를 구현한다. 새로운 SIP 호가 가입자의 사용자 주소에 위치할 때, SIP INVITE 메시지는 이 주소를 제공하는 도메인의 프록시 서버로 지시되어 진다. 프록시 서버는 레지스트라의 홈 에이전트를 참고하고, 거의 현재 장치 주소(Contact URI)와 현재장치의 위치(현재 위치 또는 CoA)를 얻는다. 그리고 프록시 서버는 INVITE 메시지를 장치에 직접 전송한다. 일단 호가 설정되면, 미디어는 시그날링 경로와는 독립적으로 호의 종단 사이에서 직접적으로 흐르게 된다.

통합된 모델의 보안메커니즘은 홉간의 기밀성과 무결성을 보장하기 위하여 통합모델의 MIPv6 패킷에는 IPSec 을 SIP 메시지에는 TLS 를 사용한다. End-to-End 보안으로는 S/MIME 을 사용한다.

4. 결론 및 향후 계획

본 논문에서 우리는 이동망에서 이전보다 안전한 실시간 서비스를 제공하기 위한 효율적인 통합 메커니즘을 제안하였다. 제안된 메커니즘은 각각의 프로토콜을 분석하여 각 프로토콜의 이동성의 결점들을 상호 보완하여 패킷손실과 핸드오프 지연을 줄일 수 있다. 그리고 통합된 환경에 적합한 보안 메커니즘을 적용함으로써 효율적인 정보보호 서비스를 제공할 수 있으며 네트워크 계층과 응용 계층의 시그널링 부하를 줄이고 지속적인 통신을 위한 빠른 핸드오프를 제공할 수 있다는 결론을 내리게 되었다.

본 연구의 향후 과제로는 안정된 정보보호 서비스망을 구축할 수 있도록 세부적인 프로토콜 메커니즘을 연구해야 하며 시뮬레이션 및 구현을 통하여 성능을 측정할 예정이다.

References

1. Jin-Woo Jung, Doug Montgomery, Jung-Hoon Cheon, Hyun-Kook Kahng, "Mobility Agent with SIP registrar for VoIP Services", LNCS2713, June 2003

2. David B. Johnson and Charles Perkins, "Mobility Support in IPv6," IETF Internet Draft, draft-ietf-mobileip-ipv6-24.txt, June 2003

3. J. Rosenberg, H. Schulzrinne, E. Schooler, M. Handley, G. Camarillo, A. Johnston, J. peterson, R. Sparks, " Session Initiation Protocol" , RFC 3261 in IETF, June 2002

4. J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC2617 in IETF, June 1999

5. H. Schulzrinne, B. Volz, Ericsson, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers", RFC3319 in IETF, July 2003