Diameter Mobile IP 환경에서 안전하고 빠른 세션키 분배 메커니즘

송지은*, 조기환*
*전북대학교 컴퓨터정보학과
jeusong, ghcho@chonbuk.ac.kr

A Secure and Fast Session Key Distribution Mechanism in Diameter Mobile IP Environment

Ji-Eun Song*, Gi-Hwan Cho*
*Dept of Computer Information Statistics, Chonbuk University

요 약

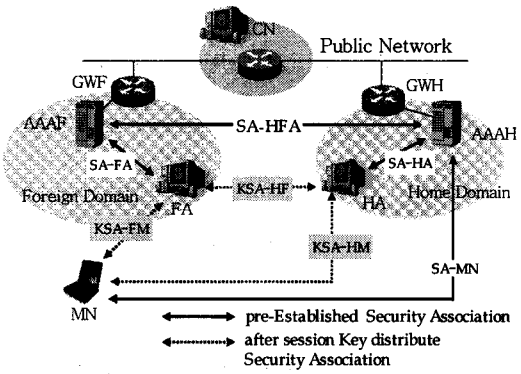
Diameter-MIPv4 프로토콜은 기존 Mobile IP(MIP)의 취약한 키 분배 문제를 해결하고 이동노드에 대해 인증 및 권한 검증, 과금 서비스 등을 지원함으로써 보다 개선된 보안 메커니즘을 제안하고 있다. 그러나 홈 망의 Diameter 서버에 의해 인증 및 등록이 수행된 후 공중망을 통해서 이동노드에게 세션키를 분배하는 것은 많은 보안상 공격에 노출될 수 있으며 원격지 도메인간의 빈번한 등록 메시지 교환은 통신 지연을 야기 시킬 수 있다. 본 논문에서는 안전한 세션키 분배를 위해서, 이동 노드의 등록 수행 과정 중 홈 망과 방문 망 사이에 IPsec(IP security) 터널을 구축함으로써 공중망에서의 세션키 유출 위협을 감소시켰다. 또한 네트워크의 계층성과 Micro-Mobility MIP 메커니즘을 이용하여 동일 도메인 내에서의 핸드오프 시 이동 노드의 인증 및 등록, 세션키 분배를 지역화 함으로써 통신 지연 문제를 효율적으로 개선하였다.

1. 서론

Mobile IP는 사용자가 이동하면서도 서비스 단절 없이 세션을 유지할 수 있도록 하는 기술로서 현재 3GPP/3GPP2 IMT-2000망과 WLAN망 등을 기반으로 여러 WISP(Wireless Internet Service Provider)들에 의해 활발히 개발되고 있다. 그러나 Mobile IP가 이와 같은 IP 기반의 개방형 네트워크 패러다임을 수용하기 위해서는 이질적인 관리 망에서 이동성을 지원하기 위한 핸드오프 기술의 확장 및 보안 기술의 개선이 필요하다. 특히 보안상 이슈에 대해 IETF AAA WG에서는 도메인간에 이동 노드를 동적으로 인증(authentication)하고 액세스 권한(authorization)을 검증하며 과금(accounting) 할 수 있는 프로토콜을 제안하고 있으며 현재 Diameter 에 대한 표준화를 진행하고 있다. RADIUS나 TACACS+와 같은 PPP 기반의 AAA 프로토콜과 달리 Diameter는 도메인간에 이동성 지원, 강화된 보안 솔루션 제공, 보안 및 신뢰성을 기반으로 하는 하부 프로토콜 수용, 추가적인 서비스를 위한 확장성 등을 보장하고 있다. 특히 Diameter-MIPv4 응용에서는 홈 AAA 서버의 KDC(Key Distribution Center) 기능을 통해 기존 Mobile IP의 동적인 키 분배 메커니즘의 부재로 인한 통신 개체간의 안전한 상호 인증의 어려움과 낮은 확장성 문제를 해결하였으며 AAA 서비스 제공 및 인증된 이동노드에 대해 HA(Home Agent) 혹은 홈 주소를 할당하는 기능을 제공한다.

다음 [그림 1]은 MIP와 AAA 프로토콜의 상호 연계 아키텍처를 보여주고 있다. SA-FHA, SA-FA, SA-HA와 같이 각 도메인의 통신 개체들과 AAA 서버 사이에 미리 협정된 보안 연계(SA : Security Association)를 기반으로 하여 홈 AAA 서버는 MN-AAA 비밀키를 이용하여 이동 노드에 대한 인증을 수행한다. 만일, 인증이 성공적으로 수행되면 홈 AAA 서버는 MN(Mobile Node)와 FA(Foreign Agent) 그리고 HA 사이에 보안 세션키를 생성하여

분배함으로써 새로운 보안 관계를 구축할 수 있게 된다. 그러나 인증이 불확실하고 안정성이 확보되지 않은 라우터들로 구성된 공중망을 통해 전송되는 세션키는 보안상 공격에 노출되기 쉽다. 게다가 MN가 빈번하게 이동할 때마다 원격지에 있는 홈 Diameter AAA 서버에까지 인증 및 등록을 요청하고 세션키를 할당받는 것은 통신 지연의 요인이 될 수 있다. 그러므로 Diameter-MIPv4 프로토콜에서 안정적이고 끊김 없는(seamless) 통신 서비스를 보장하기 위해 보다 안전하고 빠른 세션키 분배 메커니즘이 고려되어야 한다. 따라서 본 논문에서는 IPsec[1] 구축을 통해 공중망의 위험 요소로부터 세션키를 보호하고 Micro Mobility[2]의 특성을 이용하여 신속하게 세션키를 분배할 수 있는 방안을 제안한다.

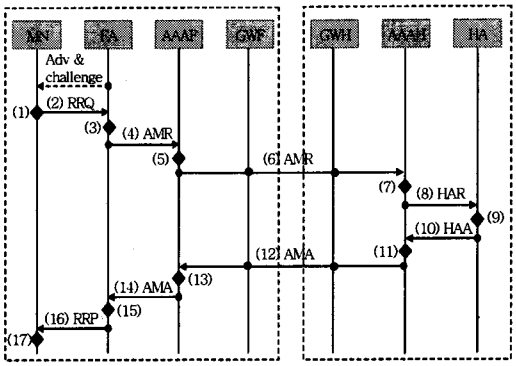


[그림 1] MIP & AAA 상호 연계 아키텍쳐

논문의 구성은 다음과 같다. 다음 2장에서는 현재 IETF에 의해 제안된 Diameter-MIPv4 프로토콜의 인증 및 등록 메커니즘에 대해 살펴보고 이어 3장에서는 본 논문에서 제안하는 세션키 분배 방법에 대해 살펴본다. 마지막으로 4장에서는 결론 및 향후 연구과제를 기술한다.

2. Diameter-MIPv4 인증 및 등록 메커니즘 [3]

MIP-AAA 메커니즘을 지원하는 방문 도메인에서 MN이 등록 요청을 하는 경우 등록 절차는 다음 [그림 2]와 같다. (1) MN는 Foreign 도메인으로의 이동을 감지하고 Adv.(Advertisement) 메시지를 통해 CoA(Care of Address)를 획득한다. (2) MN는 MN-AAA 인증 확장을 등록 요청 메시지인 RRQ (MIP Registration ReQuest)에 추가하여 FA에게 전송한다. (3)(4) FA는 MN으로부터 받은 MIP RRQ



[그림 2] Diameter-MIPv4의 등록 메커니즘

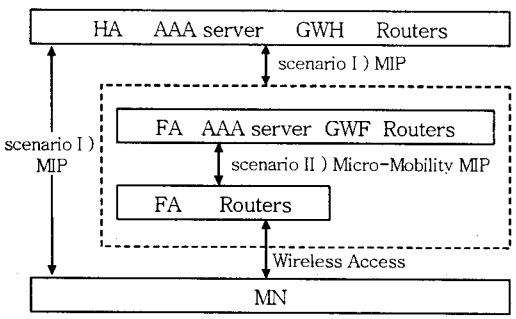
메시지의 파라미터를 체크해 MN의 홈 주소, HA 주소, MN의 NAI(Network Access Identity) 등의 정보를 추출하여 각각 해당 AVP로 인코딩하여 AMR(AA-Mobile-Node-Request) 메시지를 생성한다. 이어 AMR 메시지를 로컬 Diameter 서버인 AAAF(AAA-Foreign)에게 전달하여 MN에 대한 인증 및 권한 검증을 요청한다. (5)AAAF는 수신한 AMR 메시지의 User-Name AVP를 식별하여 [4]에 따라 로컬에서 처리하거나 자신이 직접 인증 할 수 없을 경우 (6)과 같이 AAAH(AAA-Home)에게 전달한다. (7)(8) AAAH는 SA-HFA 보안관계를 통해 MN를 인증하고 사용자 프로파일에 따라 서비스 권한 검증을 수행한다. MN에 대한 인증이 성공적으로 이루어지면 [그림 1]에서와 같은 세 가지 세션키 즉, FM, HF, HM 키를 생성하고 이를 포함하여 HAR(Home-Agent-MIP-Request) 메시지를 생성하여 HA에게 전달한다. (9)(10) HAR메시지를 받은 HA는 MIP 등록을 수행하고 세션키를 포함하여 HAA(Home-Agent-MIP-Answer)를 생성하고 AAAH에게 전송한다. (11) HA로부터 HAA를 받으면 AAAH는 MN에 대한 AAA 정보를 업데이트하고 과금 세션을 시작할 수 있다. (12)(13) AAAH에게 전송된 AMA 메시지에 따라 AAAF 또한 AAA 정보를 업데이트하고 과금 세션을 시작한다. 과금 정보는 방문 망과 홈 망에 걸쳐 실시간으로 관리 및 전달된다. (14)(15) FA는 전송 받은 AMA 메시지내의 RRP(MIP Registration RePly) 메시지를 디캡슐레이션 시키고 MIP 등록절차를 완료한다. (16)(17)과 같이 RRP 메시지가 MN에게 전송되고 나면 MN는 FM, HM 과 같은 세션키를 획득하여 MIP 서비스를 받을 수 있게 된다.

이와 같은 절차로 AAA 프로토콜을 이용한 MN의 인증 및 키 분배, MIP 등록이 이루어진다. 그런

데 위 메커니즘에서 유의하여 고려되어야 할 몇 가지 사항이 있다. 이미 살펴본 바와 같이 성공적인 인증 후 생성된 AMA 메시지는 AAAH으로부터 분배되는 중요한 보안 세션키들을 포함하고 있다. 따라서 AMA 메시지가 안전하게 방문 도메인에 전달되도록 하는 것은 중요한 일이다. 게다가 원격지인 홈 망과 MN이 속한 방문 망 사이의 컨트롤 메시지 교환을 최소화하는 것은 인증/등록 및 키 분배로 인한 통신 지연을 합리적으로 감소시키는 대안이 될 수 있다. 따라서 다음 장에서는 이에 대한 해결책으로 본 논문에서 제안하는 세션키 보호 및 빠른 세션키 분배 메커니즘에 대해 구체적으로 기술한다.

3. 제안한 세션키 분배 메커니즘

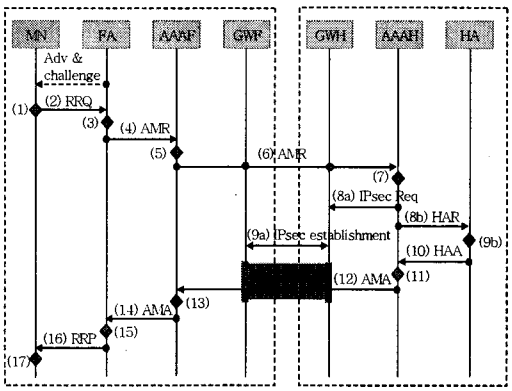
본 장에서는 [그림 3]과 같이 MN의 이동 형태에 따라 두 가지 시나리오로 나누어 제안 메커니즘을 설명하도록 하겠다. 다른 도메인간의 이동시 공중망을 통해 메시지가 교환될 때는 MIP 프로토콜이 적용된다. 또한 한 도메인 내의 이동은 Micro-mobility .MIP 프로토콜 방식을 따른다. 또한 제안하는 메커니즘은 다음 사항을 기본 가정으로 하고 있다. 첫째, 각 도메인의 Agent와 라우팅들은 네트워크 구조상 계층적으로 최상위에 GW(GateWay)를 갖는다. GW는 도메인 내에서의 모든 이동에 관한 사항을 관리한다. 둘째로 각 도메인 내부는 VPN(Virtual Private Network)에 의해 안전하게 보호된다는 것을 기본 가정으로 한다.



[그림 3] Diameter-MIPv4 핸드오프 시나리오

3.1 Scenario I) MIP : inter-domain 핸드오프

서로 다른 관리 도메인간에 이동하는 inter-domain 핸드오프 프로시저는 [그림 4]와 같으며 2장에서 설명하였던 것과 같이 FA에 전달된 MN의 RRQ 메시지는 AMR 메시지에 인코딩되어 AAAF를 거쳐 AAAH에 전송된다. (7) AAAH는 MN의 인증을 수행하고 (8a)와 같이 인증이 성공할 경우 GWH(Gate Way-Home)에게 GWF(GateWay-Foreign)와 IPsec 보안 터널링을 구축하도록 IPsec Req. 메시지를 전달한다. 또한 (8b)(9b)와 같이 HA는 전달된 HAR 메시지에 의해 MN의 등록을 수행하고 세션키들을 포함한 HAA 메시지가 생성된다. 이때 동시에 (9a)와 같이 GWF와 GWH 간에 IPsec IKE(Internet Key Exchange) 과정이 진행되고 이 협상이 완료되면 강한 인증 및 무결성, 기밀성 등을 보장하는 IPsec 터널이 구축되게 된다. 따라서 (12)와 같이 AAAH에 의해 생성된 AMA 메시지는 IPsec 터널 경로를 통해 공중망을 가로질러 방문 망에 도달함으로써 AAAF에게 세션키들을 안전하게 분배할 수 있다.



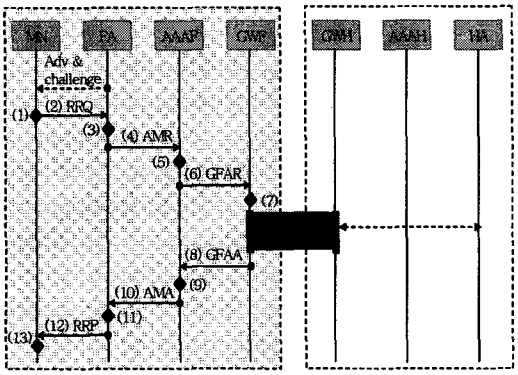
[그림 4] inter-domain 핸드오프 : 안전한 세션키 분배 메커니즘

AAAH에 의해 수행된 인증 결과에 따라 IPsec 터널을 구축하여 세션키를 분배하는 것은 인증 결과에 무관하게 인증 전에 IPSec을 구축함으로써 야기될 수 있는 불필요한 IKE 오버헤드를 감소시킬 수 있다. 또한 HA에 대한 등록 수행과 동시에 GW간의 IPsec 구축을 병행하여 수행함으로써 IPsec 터널 생성 시간의 경제성도 획득 할 수 있다. 이와 같이 보안상 공격에 노출되기 쉬운 공중망에서 IPsec encryption 터널을 구축함으로써 GWF와 GWH 간을 end-to-end security로 안전하게 세션키를 전송할 수 있다.

3.2 Scenario II) Micro Mobility MIP : intra-domain 핸드오프

MN이 같은 방문 도메인 내를 이동하는 경우 게이트웨이인 GWF가 도메인 내의 MN의 이동성에 관한 사항을 관리한다. 다시 말해서 GWF가 방문 도메인

내에서 HA와 같은 역할을 하는 것이다. 그러므로 MN이 동일한 도메인 내에서 이동하는 한, 홈 망과 이동 망 사이에서 어떠한 MIP 등록에 관한 메시지도 교환될 필요가 없다. 따라서 intra-domain 핸드오프에서는 새로운 세션키의 정의가 필요하다. MN-FA, FA-GWF, MN-GWF간의 세션키로 각각 MF, FGW, MGW 키가 AAAF에 의해 생성 및 분배되어야 한다.



[그림 5] intra-domain 핸드오프 : 빠른 세션키 분배 메커니즘

[그림 5]는 intra-domain 내에서의 핸드오프 시 MIP 등록 메커니즘에 대해 보여주고 있다. (2)와 같이 MN에 의해 전송된 RRQ 메시지로부터 FA는 AMR 메시지를 생성하여 AAAF에게로 전송한다. (5)에서 AAAF는 AMR 메시지에 포함된 MN의 홈 주소, HA 주소, MN의 NAI(Network Access Identity)에 관한 각 AVP로부터 해당 MN을 식별하고 이 MN이 AAAH로부터 인증 받은 레코딩이 있는지 검색한다. AAAF는 이전에 자신을 통해 전달된 AMR 메시지에 대한 응답, 즉 인증 결과와 세션키가 담긴 AMA 메시지 정보를 보유하고 있으며 MN에 대한 인증 정보와 과금 정보를 유지하고 있다. 따라서 만일 AAAF는 MN이 일정 시간 안에 AAAH로부터 인증되었던 노드로 확인 될 경우 자체적으로 도메인 내에서 사용될 세션키인 MF, FGW, MGW 키를 생성한다. 그리고 이어 생성한 세션 키들을 등록을 요청하는 MIP-Reg-Request AVP와 함께 인코딩하여 GFAR 메시지를 생성한 후 (6)과 같이 GWF에 전송한다. (7)(8) GWF는 인증이 이루어진 MN에 대한 등록을 수행하고 MIP-Reg-Reply AVP와 세션키 정보를 포함하여 GFAA 메시지를 AAAF에게 전송한다. (9) 등록 응답 메시지인 GFAA를 받은 AAAF는 MN의 AAA 정보를 갱신하고 과금 세션을 계속해서 유지하도록 한다. (10)(11) AAAF는 AMA 메시지를 생성하여 FA에게 전달하고 이를 받은 FA는 지역적 등록 수행을 완료하고 RRP 메시지를 생성한다. (12)(13) 마침내 MN에게 등록 응답 메시지가 전송됨으로써 성공적으로 MN에게 MIP 서비스를 제공할 수 있게 된다.

[그림5]에서 보는 바와 같이 MN이 이전에 인증받아 접속했던 도메인과 동일한 도메인 내에서 이동할 경우 어떤 MIP 등록 메시지도 공중망을 거쳐 홈 망의 통신 개체와 교환되지 않는 것을 볼 수 있다. 한편, GWF와 GWH사이에는 MN이 최초로 방문 망에 접속하였을 때, 시나리오 1에서 살펴본 바와 같은 절차에 의해 구축된 IPsec 터널이 존재하며 이 터널을 통해 방문 망과 홈 망 사이에 유효한 보안/인증 관계가 유지되고 있다. 이와 같은 네트워크의 계층성과 Micro-Mobility MIP 이동성의 특징을 고려한 메커니즘에 의해 동일 도메인 내에서의 MN 인증 및 등록, 세션키 생성 및 분배에 대한 요구가 빠르게 처리될 수 있다.

4. 결론

Diameter-MIPv4 서비스가 제공되는 이동 통신 환경에서 안전하면서도 끊김 없는 좋은 품질의 무선 인터넷 서비스를 위해서는 MIP 인증/등록 과정에서 생성된 세션키를 안전하고 신속하게 분배할 수 있어야 한다. 이에 대해 본 논문에서 제안한 IPsec 터널링을 통한 세션키 분배 보안과 Micro-Mobility 메커니즘을 이용한 지역적 세션키 분배 방안은 좋은 해결 방안이 될 수 있다. 이 외에도 Diameter-MIPv4 기반에서 패킷 분실을 최소화하기 위한 방안 및 세션키의 안정성을 높이기 위한 효율적인 세션키 갱신 메커니즘 등도 좋은 연구 분야가 될 수 있다.

참고문헌

[1] J. Zao, et al., "Use of IPSec in Mobile IP," *IETF Draft*, draft-ietf-mobileip-ipsec-use-00.txt, Nov. 1997

[2] Y. xu, et al., "Mobile IP Based Micro Mobility Management Protocol in the Third Generation Wireless Network," *IETF Draft*, draft-ietf-mobileip-3gwireless-ext-06.txt, Nov. 2001

[3] P. R. Calhoun, et al., "Diameter Mobile IPv4 Application," *IETF Draft*, draft-ietf-aaa-diameter-mobileip-13.txt, Oct. 2002

[4] P. R. Calhoun, et al., "Diameter Base Protocol," *IETF Draft*, draft-ietf-aaa-diameter-17.txt, Dec. 2002