ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

CR-SeMMS : NEMO환경에서 SIP에 기반한 비용절감의 안전한 이동성관리 기법

CR-SeMMS: Cost-Reduced Secure Mobility Management Scheme Based on SIP in NEMO Environments

조 철 희* 정 종 필**
Chul-Hee Cho Jong-Pil Jong

요 약

IETF(Internet Engineering Task Force)의 MVPN(Mobile Virtual Private Network) 은 NEMO(NEtwork MObility)를 지원하도록 설계되어 있지 않기 때문에 실시간 응용에 적합하지 않다. 따라서 안전한 NEMO에서 VPN을 지원하는 아키텍처와 프로토콜이 필요하다. 본 논문에서는 VPN 환경에서 실시간 응용을 위해 설계된, SIP(Session Initiation Protocol)에 기반한 CR-SeMMS(Cost-Reduced Secure Mobility Management Scheme) 시스템을 제안한다. 제안하는 기법은 NEMO에서의 MVPN을 지원하는 방법을 제안하여 전체 네트워크가 이동하는 경우, 지속적으로 세션을 유지하도록 한다. 또한, 핸드오프의 경우 지연 시간 요소로 고려되는 인증 시간을 단축하기 위하여 HOTP(HMAC based One Time Password) 기반의 인증방식을 이용한 핸드오프 방식을 제안하여 세션을 유지하기 위해 지속적으로 발생하는 시그널링 처리시간을 개선하였다. 마지막으로, 제안한 방식과 기존 방식을 시뮬레이션하여 핸드오프 수행의 평균 시간이 개선되는 것을 확인한다.

ABSTRACT

The mobile Virtual Private Network (MVPN) of Internet Engineering Task Force (IETF) is not designed to support NEwork MObility (NEMO) and is not suitable for real-time applications. Therefore, an architecture and protocol which supports VPN in NEMO are needed. In this paper, we proposed the cost-reduced secure mobility management scheme (CR-SeMMS) which is designed for real-time applications in conjunction with VPN and also which is based on the session initiation protocol (SIP). Our scheme is to support MVPN in NEMO, so that the session is well maintained while the entire network is moved. Further, in order to reduce the authentication delay time which considers as a delaying factor in hands-off operations, the signaling time which occurs to maintain the session is shortened through proposing the hands-off scheme adopting an authentication method based on HMAC based One Time Password (HOTP). Finally, our simulation results show the improvement of the average hands-off performance time between our proposed scheme and the existing schemes.

☞ keyword : 네트워크 이동성, 모바일 네트워크, HOTP SIP 인증, 노드 핸드오프, 네트워크 핸드오프

1. 서 론

무선랜 서비스 지역이 점차 확대되면서 노트북을 이용하여 언제 어디서나 인터넷을 사용하고자 하는 사용자들의 요구도 증가하고 있다. 이러한 변화를 수용하기 위해 기차, 버스, 배 등의 이동수단에서 인터넷 서비스를 제공할 수 있는 기술이 주목 받고 있다. 이러한 기술 중 하나가 IP 네트워크 이동성 기술인 NEMO(NEtwork MObility)이다[1-3]. NEMO는 네트워크 내의 모든 노드들이 이동을 인식하지 않고 인터넷 연결서비스를 MR(Mobile Router)에서 제공해 주는 기술로 IETF에서 IPv6를 기반으로 표준화가 진행되고 있다. NEMO에서는 다른 네트워크를 거치지 않고 인터넷 망에 직접 연결하여 이동성 서비스를 제공한다. 따라서 다양한 이동수단 뿐 아니라 텔레매틱스, PAN, Ad-hoc 네트워크 등에도 적용될 수 있다.

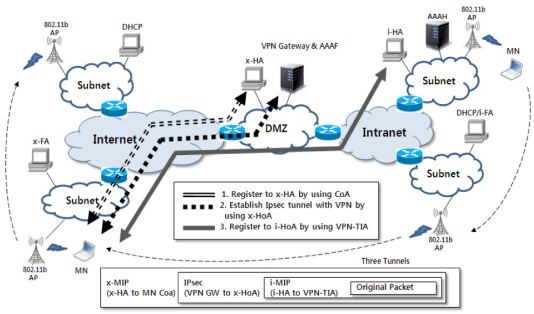
보안은 오늘날 인터넷에서 중요한 문제가 되고 있으며, VPN(Virtual Private Network)은 인터넷과 인트라넷 사이에서 안정된 사용자 통신을 확보하기 위해 개발되었다. NEMO에서의 VPN서비스는 다양한 응용에서 사용될 수 있다. 따라서 모바일 네트워크는 안정된 방법으로 그

* 정 회 원 : 성균관대학교 정보통신대학원 정보보호학과
chuli77@skku.edu
** 정 회 원 : 성균관대학교 정보통신공학부 (공학박사)
jpjeong@skku.edu (교신저자)
[2012/01/03 투고 - 2012/01/10 심사(2012/05/08 2차) - 2012/06/08 심사완료]

것의 인트라넷에 접근할 수 있다. 예를 들어, NEMO VPN은, 경찰 순찰차에서의 무선 장치가 범죄자 데이터베이스, 운전 면허증과 차량 등록 데이터베이스에 액세스할 수 있는 것같이 공공안전을 위하여 사용될 수 있다. 그러나, VPN 서비스를 제공하는 방법은 IETF의 NEMO 워킹그룹에서 아직 해결되지 않았다. IETF가 이동성를 지원하는 VPN 아키텍처를 제안했지만, 이 솔루션은 모바일 장비 그룹의 이동성을 고려하지 않았고, 단지 단일 노드를 위한 것이며 실시간 응용에 적합하지 않은 MIP(Mobile IP)을 기반으로 한다. IETF의 MVPN(Mobile VPN)은 하나의 IPSec[4] 터널과 두 개의 MIP 터널을 사용한다. 세 개의 터널은 실시간 패킷을 전송 중에 상당한 오버헤드의 원인이 된다. 따라서 안전한 NEMO에서 MVPN을 지원하는 새로운 아키텍처와 프로토콜이 요구된다. 또한 인증 절차의 복잡성과 모바일 장비그룹의 이동으로 각각의 노드에서 발생할 수 있는 다수의 시그널링 메시지는 상당한 오버헤드의 원인이 된다.

본 논문에서는 MVPN상에서 실시간 응용에 적합하며, 시그널링 시간의 단축을 위해 SIP(Session Initiation Protocol)에 기반한 비용절감의 안전한 이동성관리 기법(CR-SeMMS)을 제안한다. 이것은 전체 네트워크가 이동하며 지속적으로 세션을 유지하도록 함으로써 실시간 응용에 적합하도록 설계되었으며 SIP 기반의 MVPN과 NEMO를 통합하여 보안성과 실시간 서비스를 위한 효율적인 그룹 이동성을 제공한다. 또한, 모든 SIP 클라이언트들은 MIP에서의 HA(Home Agent)와 같은 이동 에이전트를 통하지 않고도 서로 간에 직접적인 통신을 할 수 있다. 따라서 경로가 최적화된다. 이것은 IP기반의 음성통신(VoIP)과 비디오 스트리밍과 같은 실시간 응용에 유용할 뿐만 아니라 IPSec 터널이나 MIP 터널을 요구하지 않는다. 따라서 모바일 네트워크가 그것의 연결위치 주소를 변경할 때, 주소등록 요청은 하나의 NEMO VPN 게이트웨이가 전체 모바일 네트워크를 대표할 수 있으며 이것은 시그널링 오버헤드를 상당히 줄일 수 있다. 그리고 CN들의 모든 연결주소를 URL 목록에 결합후 하나의 INVITE 메시지에 결합하여 전송함에 따라 시그널링 수를 단축하였다. 또한 핸드오프할 때 지연 시간 요소로 고려되는 인증 시간을 단축하기 위하여 HOTP(HMAC based One Time Password) 기반의 인증방식[5]을 채택하여 세션을 유지하기 위해 지속적으로 발생하는 시그널링 시간을 향상하였다. 그리고 모바일 네트워크 내부에 있는 다수 노드의 발생신호를 통합하여 시그널링 시간을 단축한다.

본 논문은 다음과 같이 구성되었다. 2장에서는 기존에



(그림 1) IETF에서 제안한 MVPN

IETF에서 제안한 MVPN을 위한 아키텍처의 문제점과 SIP기반 MVPN의 필요성에 대해 알아본다. 3장에서는 제안한 SIP기반 비용절감의 안전한 이동성관리 기법을 기술하고, 4장에서는 제안 기법의 성능을 평가하는 분석 모델과 성능평가를 수행한다. 마지막으로 5장에서 본 논문의 결론을 맺는다.

2. 관련 연구

IETF는 MVPN[6]을 위한 아키텍처와 프로토콜을 정의해왔다. (그림 1)은 IETF MVPN을 보여준다. 여기에는 인트라넷과 인터넷에 위치하는 내부 HA(i-HA) 와 외부 HA(x-HA) 그리고 두 개의 HA가 있다.

MN가 인트라넷 외부로 이동할 때, 우선 DHCP (dynamic host configuration protocol) 서버 또는 FA(Foreign Agent)로부터 새로운 CoA(Care-of Address)를 획득한다. 그리고 CoA를 x-HA에 등록한다. 그다음 MN은 그것의 외부 홈 주소(x-HoA)를 사용하여 VPN 게이트웨이와 IPSec 터널을 생성한다. IPSec 터널은 IKE(Internet Key Exchange)[7]을 사용하여 생성된다. 세 개의 터널(x-MIP, IPSec, i-MIP)은 (그림 1)에 보여진다.

(그림 2)는 IETF MVPN의 시그널링 메시지 흐름을 보여준다. IETF MVPN은 모바일 장비 그룹의 이동성을 고려하지 않기 때문에 NEMO에 적용될 수 없고, 긴 핸드오프 지연과 단대단(End-to-End) 지연[8,9]을 발생시킬 것이다. 이 터널들은 패킷의 길이와 처리 시간 관점에서 상당한 오버헤드를 증가시킨다. 이것은 실시간 응용의 성능을 저하시킬 수 있으며 SIP기반 MVPN이 제안되었지만 단일 노드의 이동만을 고려하였다[10,11].

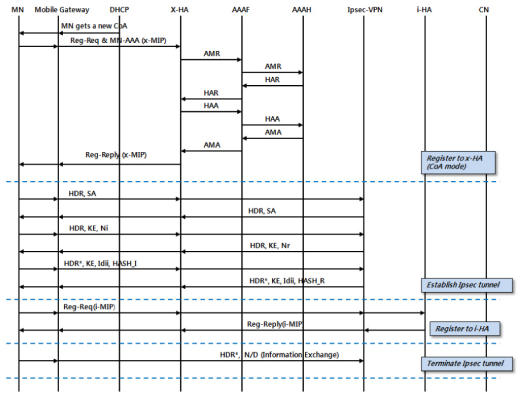
SIP은 호스트 이동성 및 세션 지속성을 제공하기 위한 SIP기반의 NEMO에서 쉽게 배포되고, 데이터 전송지연

(표 1) 사용 용어 정리

단축어	설 명
ALG	Application Level Gateway
AVP	Attribute Value Pair
CN	Correspondent Node
CoA	Care of Address
CR-SeMMS	Cost-Reduced Secure Mobility Management Scheme
HA	Home Agent
HMAC	Hash-based Message Authentication Code
HOTP	HMAC based One Time Password
IKE	Internet Key Exchange
i-HA	Internal HA
i-MIP	Internal MIP
MAA	Multimedia-Auth-Answer
MAR	Multimedia-Auth-Request
MIDCOM	Middlebox Communication
MIKEY	Multimedia Internet Keying
MIP	Mobile IP
MN	Mobile Node
MR	Mobile Router
NEMO	Network Mobility
OTP	One Time Passwords
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SA	Security Association
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP-NVG	SIP NEMO VPN Gateway
SRTP	Secure Real-time Transport Protocol
TEK	Traffic Encryption Key
TGK	TEK Generation Key
UAA	User-Authorization-Answer
UAR	User-Authorization-Request
VPN	Virtual Private Network
VPN-TIA	VPN Tunnel Inner Address
X-HA	external HA
X-MIP	external MIP

을 줄일 수 있는 것으로 제안된다[12,13].

그러나 NEMO에 SIP을 적용할 경우, 진행중인 세션들 중에서 많은 re-INVITE 메시지를 전송하기 때문에 핸드오프 동안의 시그널링 비용을 증가시킬 수 있다. 사용자 인증을 위하여 SIP에 기본적으로 구현된 인증은 HTTP 다이제스트이다. 이것은 비밀 키를 사용한 인증으로 Challenge-Response 패러다임을 기반으로 한다. 인터넷 응용에서 대부분의 프로토콜은 서비스를 제공하기 전에 클



(그림 2) IETF MVPN의 시그널링 흐름.

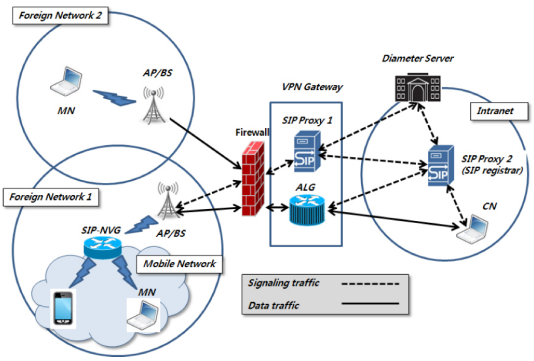
라이언트를 인증하기 위해 이 메커니즘을 사용한다. 그러나, 이 방법은 프로토콜 설계관점에서 시그널링 교환을 증가시킨다. 이 방식을 사용하는 SIP 인증은 두 번의 핸드쉐이크가 필요하다. 이러한 인증절차를 간소화하기 위해 본 논문에서는 HOTP 기반의 인증을 채택하였다. 따라서 많은 시그널링 비용 발생의 원인 중의 하나인 인증처리시간을 단축하였다. 본 논문은 NEMO에서의 MVPN을 지원하는 방법을 고려하였으며, 인증시간 및 모바일 네트워크의 시그널링 시간을 단축하기 위한 방법을 고려하였기 때문에 실시간 응용에 적합하다.

3. SIP기반 비용절감의 안전한 이동성관리

3.1 기본 구조

제안하는 SIP기반 비용절감의 안전한 이동성관리 기법(CR-SeMMS)은 SIP, SRTP(Secure Real-time Transport Protocol)[14], MIKEY(Multimedia Internet KEYing)[15], 그리고 NEMO에서 VPN 서비스를 제공하는 Diameter[16]로 구성되어 있다. (그림 3)는 제안한 CR-SeMMS의 아키텍처를 나타낸다.

(그림 3)은 외부 네트워크에 있는 모바일 네트워크가 홈 네트워크에 있는 CN(Correspondent Node)으로 연결하는 것을 보여준다. Foreign Network 1에 있는 모바일 네트워크에서 보이는 SIP-NVG(SIP NEMO VPN Gateway)는 다른 네트워크들로 가기 위한 모바일 네트워크의 게이트웨이이다. 그것은 SIP 표준을 따르고, 모바일 네트워크와 외부 간의 트래픽을 관리한다. VPN 게이트웨이는 SIP Proxy 1과 ALG(Application Level Gateway)로 구성되어 있



(그림 3) 제안 시스템의 아키텍처

다. 인터넷과 인트라넷 사이에는 외부 사용자가 인트라넷에 직접 접속하는 것을 방지하기 위해 방화벽이 있다. 그리고 SIP Proxy 1은 들어오는 SIP 메시지를 Diameter 서버를 통해 인증하는 SIP Proxy 서버이며, SIP Proxy 2(SIP Registrar)로 메시지를 라우팅 한다. 한편, MIKEY는 모든 데이터 트래픽을 감독하는 ALG를 위한 보안키를 제공하기 위해, 키 관리 프로토콜로 사용된다.

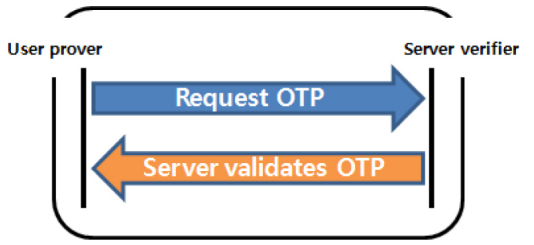
CR-SeMMS에서 SIP은 MN, SIP-NVG, SIP Proxy 1, SIP Proxy 2, 그리고 CN간의 세션을 관리하는 주요한 프로토콜이다. ALG에서의 자원 할당이 MIDCOM(Middlebox Communication) [18]을 사용하여 획득되는 동안, Diameter 기반 프로토콜[16]을 기반으로 하는 Diameter SIP 응용[17]은 Diameter 서버에서 사용자를 인증・인가하기 위해 사용된다. 또한, 보안 정보를 전달하기 위하여 MIKEY 메시지가 Diameter 기반 프로토콜과 SDP(Session Description Protocol)[19] 메시지에 포함되어 있다. SIP는 응용계층 시그널링 프로토콜로, 제안한 CR-SeMMS에서 세션을 생성, 수정, 종료하는데 사용된다. 또한, SIP는 그 자체의 보안과 인증 스키마를 정의하고 있다. 제안한 CR-SeMMS에서 우리는 모바일 사용자를 인증하고 식별하는 데 SIP을 사용한다. SIP는 또한 사용자와 단말기의 이동성을 지원한다 [12,20]. 단말기 이동성은 최초의 세션에서의 것과 동일한 Call ID를 사용하여 CN에게 새로운 INVITE (re-INVITE) 명령을 보냄으로써 이루어진다. 새로운 INVITE 명령은 MN이 새로운 위치에서 획득한 새로운 연결 주소가 포함된다. re-INVITE 명령을 받은 후, CN은 이후의 트래픽을 MN의 신규 위치로 리디렉트(redirect)한다.

SRTP는 RTP(실시간 전송 프로토콜)[21]과 RTCP(RTP 제어 프로토콜)[21] 스트림에 대하여 암호화 및 무결성을 제공하기 위한 프레임워크를 정의한다. MIKEY는 RTP/SRTP를 통해 실행되는 멀티미디어 실시간 응용을 위해 개발된 키 관리 프로토콜이다. IKE는 유니캐스트를 위한 키 관리 프로토콜로 널리 사용되는 반면, MIKEY는 점대점(P2P) 또는 소규모 대화형 그룹을 위해 설계되었다. 또한 MIKEY는 다른 환경의 요구 사항을 수용할 수 있다. 예를 들어, SDP 메시지 내에 MIKEY 메시지가 내포될 수 있으며, MIKEY 메시지를 전달하기 위해 SDP에 새로운 타입 K가 정의되어 있다. MIKEY의 주요 목적은 TGK (TEK2 Generation Key) 그리고 보안 전송 프로토콜에서 사용되는 정책 및 다른 관련된 보안 매개변수를 전송하는 것이다.

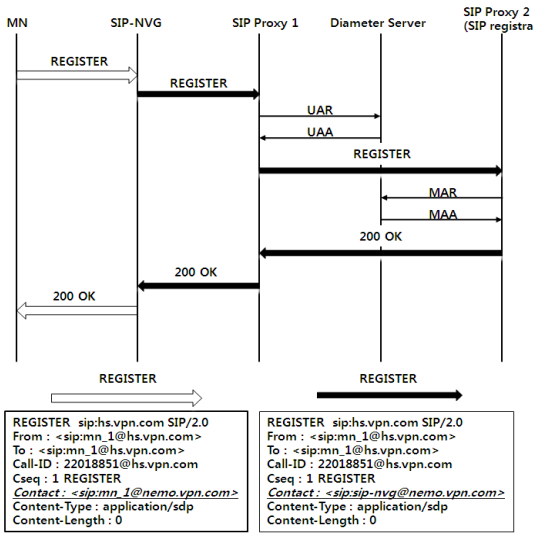
Diameter 기반 프로토콜을 기반으로 하는 Diameter SIP 응용은 SIP 서버의 클라이언트가 Diameter 서버에 의해 인증 및 인가받도록 허용한다. Diameter SIP 응용에는 여섯 개의 Diameter 명령들이 있으며, 제안한 CR-SeMMS에서 SIP REGISTER와 INVITE 메시지를 처리하기 위해, UAR (User-Authorization Request)/UAA(User-Authorization Answer), MAR(Multimedia-Auth Request)/MAA(Multimedia-Auth Answer) 명령을 사용한다.

인증은 Diameter 서버에 의해 수행되며, 핸드오프할 때 지연 시간 요소로 고려되는 인증 시간을 단축하기 위하여 제안한 CR-SeMMS에서 HOTP 기반의 인증방식을 채택한다. HOTP는 이벤트 동기화 방식의 OTP 생성 알고리즘으로써 클라이언트와 인증 서버가 비밀키 K를 공유하고 있으며, 증가하는 카운터 값인 C와 HMAC-SHA-1 해쉬 알고리즘을 이용하여 패스워드를 생성한다. 그리고 다음 인증 시에는 증가된 카운터 값(C+1)을 이용해 새로운 패스워드(6자리)를 만든다. OTP 메카니즘은 세 개의 매개변수(해시 알고리즘, 비밀키, Challenge/Counter)를 기반으로 단일 사용자 패스워드를 생성한다. HOTP는 인증 서버와 사용자 간에 기억하고 있는 인증 횟수(Counter)를 OTP의 입력값으로 하여 패스워드를 생성하며, 카운터 값이 일치해야 인증이 수행된다. "counter"매개변수는 동기화 OTP의 특성이 있으며(그림 4), 클라이언트는 인증 서버로부터 미리 항목을 받지 않고 새로운 패스워드를 생성한다.

SIP-NVG는 다른 네트워크로 이동하기 위한 모바일 네트워크의 게이트웨이이다. SIP-NVG는 모바일 네트워크가 서로 다른 IP 서브넷 사이를 로밍할 때, 진행중인 세션이 끊어지지 않도록 유지할 뿐만 아니라 안전한 방법으로 데이터를 전송한다. SIP-NVG에는 두 종류의 Egress (외부)와 Ingress(내부) 인터페이스가 있다. SIP-NVG는 Egress 인터페이스를 통해 인터넷에 연결한다. 모바일 네



(그림 4) 동기화방식의 OTP



(그림 5) 모바일 네트워크가 외부 네트워크에 있을 때 REGISTER명령어 전송흐름

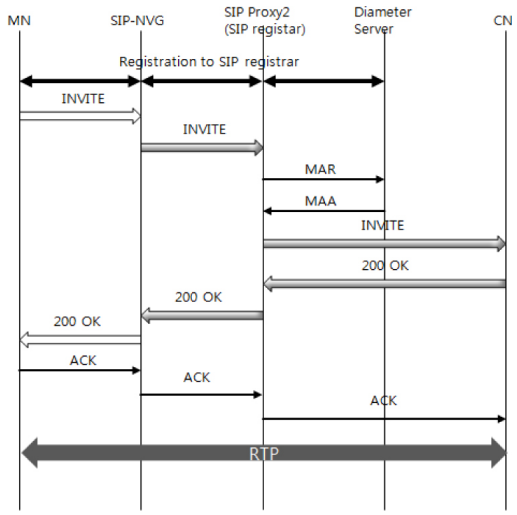
트워크가 새로운 IP 서브넷으로 이동할 때, SIP-NVG의 Egress 인터페이스는 새로운 IP 주소를 할당받는다. 한편, MN이 모바일 네트워크에 접속하려 할 때, 그것은 SIP-NVG의 Ingress 인터페이스에 연결한다. 제안한 CR-SeMMS에서 각각의 모바일 네트워크는 기본적으로 SIP 기능이 있는 MR인 한 개의 SIP-NVG를 가지고 있다. 제안한 CR-SeMMS에서 SIP-NVG는 해당하는 헤더를 이용하여 Egress와 Ingress 인터페이스 간의 SIP 메시지와 데이터 트래픽을 라우팅할 수 있다.

(그림 5)는 모바일 네트워크가 외부 네트워크에 있을 때의 등록 흐름을 보여준다. MN이 모바일 네트워크에 들어가면 새로운 IP 주소를 할당받고, SIP-NVG에 새로운 IP 주소를 등록한다. (그림 5)는 MN이 새로 얻은 연결 주소와 함께 REGISTER 명령을 전송하여, 홈 네트워크에 있는 SIP registrar에 자신의 현재 위치를 업데이트하는 것을 보여준다. 이 예제에서 모바일 네트워크가 외부 네트워크에 있고, MN에 할당된 신규 주소가 mn-1@nemo.vpn.com이라고 가정한다. 제안한 CR-SeMMS에서, SIP Proxy 2는 시그널링 메시지를 처리할 뿐만 아니라 SIP registrar 역할을 한다. (그림 5)와 같이, SIP-NVG는 REGISTER 명령의 Contact 필드를 MN의 주소(mn-1@nemo.vpn.com)로부터 SIP-NVG의 URI 주소(sip-nvg@hs.vpn.com)로 변환한다. 게다가, SIP-NVG는 MN에 대한 등록 정보를 기록하기 위해 매핑 테이블을 설정한다. 따라서 이후 MN으로 향하는 각각의 요청은 SIP-NVG로 리디렉트되며, SIP-NVG는 매핑 테이블에 따라 요청을 MN에게 전달한다.

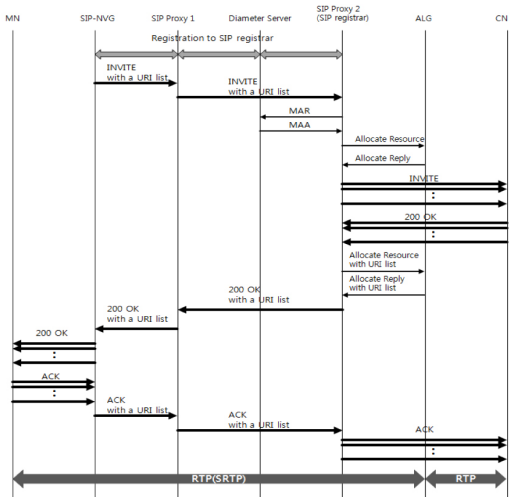
(그림 3)에 보이는 바와 같이, 제안한 CR-SeMMS는 MIDCOM 아키텍처를 따르는 ALG를 채택한다. 여기에서 ALG는 단지 SIP Proxy 2로부터 명령을 받아서 해당 명령에 대한 응답을 제공한다. ALG는 홈 네트워크로부터 MN으로 들어오는 RTP 스트림을 받을 때, 전체 IP/UDP/RTP 헤더를 새로운 것으로 교체한다, 그리고 그 새로운 RTP 패킷을 SRTP 포맷으로 변환하며, SRTP 스트림을 목적지로 전달한다. 그리고 반대 방향에서 ALG는 인터넷으로부터 SRTP 스트림을 받는다. 이후, ALG는 그것을 해독하고 SRTP 패킷의 유효성 여부를 확인한다. 그 SRTP 패킷이 복호화되고 성공적으로 확인된 경우에는 RTP 페이로드는 새로운 RTP 헤더에 의해 전달된다. 이후, 새로운 RTP 패킷은 홈 네트워크로 전송된다. ALG에서 각 세션은 충분한 내부 및 외부 자원을 필요로 한다. 예를 들어, 외부 자원은 외부 수신 주소, 외부 수신 포트, 외부 목적지 주소, 및 외부 목적지 포트를 포함하며, 목적지 주소와 포트는 SIP Proxy 2에서 제공한다. 한편, 내부 자원은 내부 수신 주소, 내부 수신 포트, 내부 목적지 주소, 내부 목적지 포트를 포함한다. 모든 리소스가 준비될 때, ALG에서 세션이 시작되며, 내부 또는 외부 리소스 모두 성공적으로 예약될 때, ALG는 예약된 수신 주소와 포트를 SIP Proxy 2에 회신한다.

3.2 동작

(그림 3)의 제안한 CR-SeMMS에서 전체 모바일 네트워크는 IP 서브넷에서 다른 곳으로 한꺼번에 이동할 수 있다. 이것을 네트워크 핸드오프라고 하며, MN이 모바일 네트워크 내부 또는 모바일 네트워크 외부의 이동이 가능한데, 이것을 노드 핸드오프라고 한다. (그림 6)은 노드 핸드오프의 예로서 MN이 외부 네트워크에 위치한 모바



(그림 6) MN이 홈 네트워크 내부에 위치한 모바일 네트워크로 이동시 INVITE명령의 전송흐름



(그림 7) 모바일 네트워크가 홈 네트워크에서 외부 네트워크로 이동시 메시지흐름

일 네트워크로 이동할 때의 흐름을 보여준다. 우선 MN는 SIP-NVG와 SIP registrar에 등록한다. 등록 후에 그들 사이에 활성 세션이 있다면, MN는 CN에 re-INVITE할 필요가 있다. INVITE 요청에 대하여, SIP-NVG는 Contact 필드를 MN의 주소에서 SIP-NVG의 URI 주소로 변환하며, SIP-NVG의 URI 주소가 들어있는 RECORD-ROUTE 필드를 추가한다. 따라서 기존 세션의 후속 메시지는 SIP-NVG에 의해 라우팅이 수행된다. 이 경우에 시그널링 메시지는 SIP Proxy Server 2에 도착하기 전에 SIP Proxy Server 1을 통과하고, Diameter 서버에 의해 인증이 필요하다.

모바일 네트워크와 CN 모두가 동일한 영역 내에 위치할 때, 즉 동일한 인트라넷 또는 인터넷에서 동일한 네트워크 도메인에 위치할 때, 모바일 네트워크에 연결한 MN과 CN사이의 데이터 트래픽은 ALG를 통과할 필요가 없다. 데이터 트래픽은 모바일 네트워크와 CN간에 직접 전송된다. 또한, CN이 인트라넷 내부에 있고, 모바일 네트워크가 인트라넷과 인터넷 사이를 이동한다고 가정한다. 이에 대한 예제로서, 모바일 네트워크가 홈 네트워크로부터 Foreign Network 1로, Foreign Network 1로부터 Foreign Network 2로, 그 다음 Foreign Network 2로부터 다시 홈 네트워크로 이동하는 경우를 고려한다.

(그림 7)은 모바일 네트워크가 인트라넷에서 인터넷으로 이동할 때 흐름을 보여준다. SIP-NVG가 외부 네트워크로 이동할 때, 그것은 새로운 IP 주소를 SIP registrar에

```
v = 0
c = IN IP4 sip-nvg@hs.vpn.com
a= URI list : <sip : cn_1@hs.vpn.com> port = 6600
    ID = 132387 src = sip : mn_1@hs.vpn.com
a = URI list : <sip : cn_2@hs.vpn.com> port = 6868
    ID = 327623 src = sip : mn_2@hs.vpn.com
```

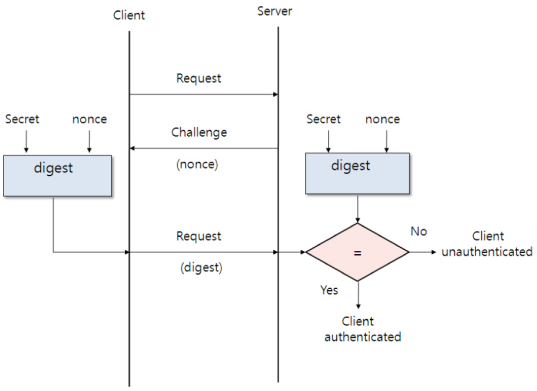
(그림 8) SDP에서 2개의 CN을 포함한 URI 목록의 예.

등록해야 한다.

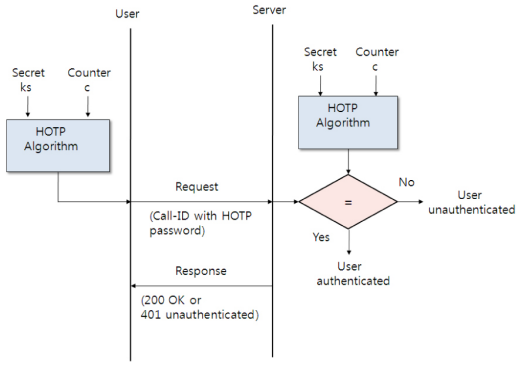
이후에 SIP-NVG는 세션 테이블에 따라서 모바일 네트워크 내에 있는 MN의 활성화 여부를 체크한다. SIP-NVG는 모든 진행중인 세션을 복구하기 위해 모든 CN을 re-INVITE해야 한다. 그러나 이 과정은 무선 링크에 상당한 시그널링 메시지의 원인이 될 수 있다. SIP-NVG는 시그널링 오버헤드를 줄이기 위해, CN들의 모든 연결주소를 URI 목록에 결합한다. 이후 URI 목록은 하나의 INVITE 메시지에 임베디드된 SDP에 의해 전송된다.

(그림 8)는 SDP에서 URI 목록의 예를 보여준다. re-INVITE 메시지는 SIP-NVG의 새 연결 주소를 포함하고 있다. 그것은 SIP Proxy 1로 보내진다. 이후 SIP Proxy 1은 진행중인 세션의 확인 책임이 있는 SIP Proxy 2로 메시지를 라우팅한다.

URI 목록이 포함된 INVITE 메시지를 전달 받은 SIP registrar는 모든 CN들에게 각각 INVITE 메시지를 전송한



(그림 9) HTTP 다이제스트 인증



(그림 10) HOTP SIP 인증

다. CN들은 활성 세션이 있는 경우에 SIP registrar에게 응답 메시지(200 OK)를 전송한다. 이 과정 또한 무선 링크에서 상당한 시그널링 메시지의 원인이 될 수 있으며, 이 시그널링 오버헤드를 줄이기 위해 다수의 응답 메시지를 받은 SIP registrar는 CN들의 모든 접속 주소를 URI 목록에 추가하여 저장한다. 이후 URI 목록은 하나의 Allocate Resource 명령에 포함되어 ALG에 전달된다. Allocate Resource 명령을 받은 ALG는 URI 목록에 의하여 외부 리소스를 허용한 뒤 SIP registrar에게 Allocate Reply 응답 메시지를 전송한다. 그 다음, SIP registrar는 SDP에 URI 목록이 포함된 하나의 응답 메시지를 SIP Proxy 1로 전송한다.

제안한 CR-SeMMS는 각각의 활성 세션을 인증하기 위해, (그림 10)과 같은 HOTP SIP 인증 방식을 채택한다. HOTP는 이벤트 동기화 방식의 OTP생성 알고리즘으로써 한 번의 핸드쉐이크로 클라이언트 인증을 수행한다. 클라이언트와 인증 서버 간에 동기화된 시간 값과 동일한

```
INVITE sip : mn_2@hs.vpn.com SIP/2.0
From : <sip : mn_1@hs.vpn.com>
To : <sip : mn_2@hs.vpn.com>
Call-ID : 238730@hs.vpn.com
Cseq : 43 INVITE
Content-Type : application/sip
Content-Length : 0
```

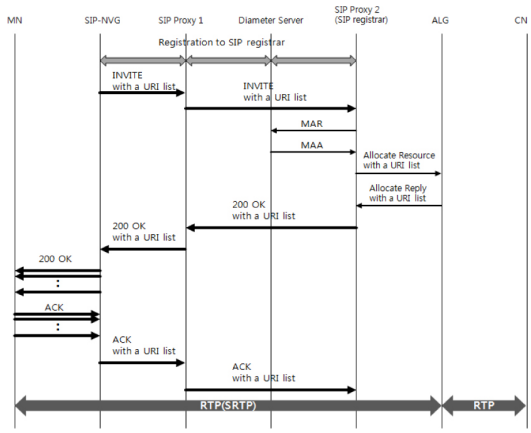
(그림 11) HOTP 콜 ID(Call-Id)를 포함한 SIP 메시지의 예

인증 횟수를 기준으로 OTP를 생성한다.

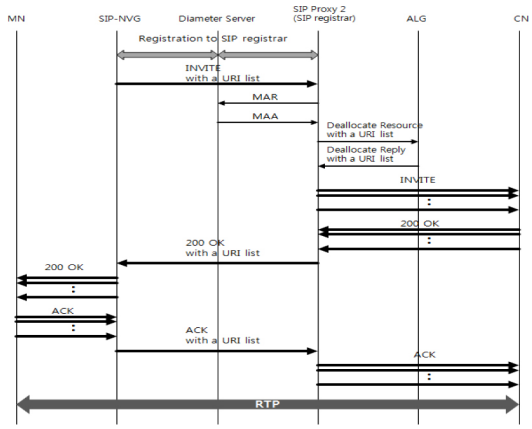
한편 HTTP 다이제스트 인증인 경우는 비동기화 인증으로 임의의 난수를 암호 알고리즘의 입력 값으로 사용해서 일회용 패스워드를 생성하는 방식이기 때문에 인증 서버가 임의의 난수 값을 생성해서 사용자에게 보내면(challenge) 사용자는 이 난수 값을 사용하여 해쉬값을 생성한다. 여기서 나오는 출력 값을 일회용 패스워드로 응답하여 사용자 인증이 수행된다. 이것은 인증을 위해 두 번의 핸드쉐이크를 필요로 한다. 따라서 더 많은 시그널링 비용이 발생할 것이다. MN이 모바일 네트워크에 연결될 때 SIP-NVG는 MN을 나타내는 인증에 필요한 보안 정보를 함께 저장한다. (그림 11)는 SIP 메시지 헤더의 Call-ID 필드에 HOTP 알고리즘[5]에 의해 생성된 패스워드의 예를 보여준다.

Diameter SIP 응용에서의 Diameter 명령(MAR/MAA)은 인증 메시지를 처리하는데 사용한다. 시그널링 오버헤드를 줄이기 위해 각 세션에 대한 보안 정보는 하나의 MAR/MAA 메시지에 집합된다. 이것은 처리를 요구하는 여러 개의 세션이 있다는 것을 알리기 위하여, MAR/MAA의 Diameter 헤더 내에 있는 Command 플래그에 예약된 비트 "M"을 설정함으로 가능하다. 따라서, 먼저 SIP Proxy 2는 Diameter 서버가 세션을 인증하고 승인하도록 요청할 MAR를 보낸다. 이후 Diameter 서버는 Call-Id 에 포함된 패스워드와 계산된 패스워드를 비교하여 사용자 에이전트를 인증한다. 두 값이 같은 경우, Diameter 서버는 한 번의 핸드쉐이크로 사용자 인증절차를 완료한다. Diameter 서버는 인증 데이터를 확인하고 SIP Proxy 2에게 각 세션의 인증 결과를 알려준다. 세션이 성공적으로 확인되면 Diameter 서버는 이 세션에 대한 TGK와 MIKEY 한 쌍을 생성한다. 이후 MAA는 각 세션에 대한 모든 확인 결과 코드를 보유하게 된다.

SIP-NVG는 인트라넷에 접근이 허용되면, SIP Proxy 2는 세션의 보호를 위해 충분한 자원을 할당해야 한다. 우선, SIP Proxy 2는 ALG에게 각 진행중인 세션에 대하여



(그림 12) 모바일 네트워크가 외부 네트워크에서 다른 외부 네트워크로 이동시 메시지흐름



(그림 13) 모바일 네트워크가 외부 네트워크로부터 홈 네트워크로 돌아올시 메시지흐름

내부 수신 주소, 내부 수신 포트를 예약하도록 명령한다. SIP Proxy 2로부터의 명령은 Data SA, SRTP 보호를 위한 TGK, 그리고 CN의 원래 수신주소와 수신포트를 포함할 수 있다. ALG는 예약된 주소와 포트로 응답한다. SIP Proxy 2는 URI 목록에 기초한 INVITE 요청을 다시하기 위해 SDP에 수신 주소와 수신 포트를 추가한다. 이후 그들을 각 CN으로 라우팅을 수행한다. 각 CN은 re-INVITE의 SDP에 동의하는 경우 OK로 응답한다. 각 CN로부터 OK를 수신한 후, SIP Proxy 2는 다시 ALG에게 외부 수신 주소와 수신 포트를 예약하도록 명령한다. ALG는 또한 예약된 외부 수신 주소와 수신 포트로 응답한다. 할당된 모든 리소스가 준비되면, SIP Proxy 2는 각 200 OK의 SDP에 수신 주소와 수신 포트를 대체한다. 또한, TGK를 전송하기 위해 SDP에 MIKEY 초기화 메시지를 추가한다. 수정이 완료되면 SIP Proxy 2는 새로운 SDP가 포함된 각 OK를 SIP-NVG에게 전송한다. SIP-NVG가 각 OK를 수신하면, 그것은 MN에게 메시지를 전달한다. ALG는 내부 및 외부 양쪽 자원이 획득되었을 때 작동하기 시작한다. 모바일 네트워크에 연결된 각 MN가 MIKEY 초기화 메시지가 포함된 OK를 받았을때, 그것은 MIKEY 초기화 메시지를 처리하고 공유 TGK을 추출해야 한다. 이후 MN는 MIKEY 응답 메시지를 포함하는 SDP와 함께 ACK 메시지를 보낸다. MN는 ACK 메시지를 전송한 후에 모든 전송 세션을 시작한다.

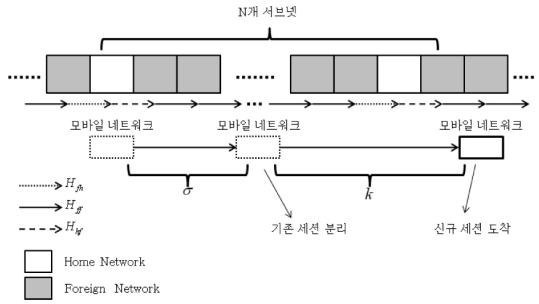
(그림 12)은 모바일 네트워크가 다시 다른 외부 네트워크로 이동할 때의 흐름을 보여준다. SIP-NVG는 또한 Registrar에 그것의 새로운 위치를 업데이트하고, 활성 세션을 가진 CN들에게 re-INVITE를 보낼 필요가 있다. 그러나 SIP Proxy 2는 CN들을 대신하여 OK로 응답할 것이다. SIP Proxy 2는 단지 ALG에게 외부 수신 주소와 포트를 수정하라고 명령한다. 흐름의 나머지 부분은 (그림 7)과 유사하다.

(그림 13)는 모바일 네트워크가 홈 네트워크로 이동할 때의 흐름을 보여준다. 인트라넷 내부에서는 데이터 트래픽이 안전하기 때문에 ALG는 모든 내부 및 외부의 자원할당을 취소하도록 요청한다.

제안한 CR-SeMMS는 SIP를 기반으로 하기 때문에 MIP로부터 상속받는 문제(세 터널에 의한 오버헤드) 및 긴 단대단(End-to-End) 지연은 제안한 아키텍처에서는 문제가 되지 않는다.

4. 성능 분석

제안한 CR-SeMMS에서는 핸드오프 동안 세션 연속성을 지속적으로 유지하기 위해 시그널링 메시지가 보내진다. 제안한 CR-SeMMS의 성능을 평가하기 위하여 시그널링 비용을 수치화하는 것이 중요하다. [21-24]와 유사하게, 시그널링 비용 함수는 전송 비용과 처리 비용으로 구성된다. 전송 비용은 두 개의 네트워크 노드사이의 거리에 비례하며, 처리 비용은 메시지를 처리하는 또는 메시지를 확인하는 비용이 포함된다. 제안한 CR-SeMMS에서 모바일 네트워크의 상호 영역 로밍(Inter-Realm Roaming)은 아래와 같이 세 가지 유형의 핸드오프로 구성된다.



(그림 14) 분석을 위한 네트워크 토폴로지

(표 2) 분석시 사용된 파라미터 정의

변수	설 명
N	모바일 네트워크가 인트라넷으로 돌아가기전 방문하는 네트워크 수
λ	모바일 네트워크에 대한 세션 도착율
$1/\mu$	평균 세션 서비스 시간
$1/\gamma$	평균 네트워크 거주시간
c	모바일 네트워크에서의 진행중인 세션 최대수
δ_σ	σ에 대한 확률 밀도 함수

1) 홈 네트워크로 부터 외부 네트워크로 이동시 핸드오프
2) 외부 네트워크로 부터 또다른 외부 네트워크로 이동시 핸드오프
3) 외부 네트워크로 부터 홈 네트워크로 이동시 핸드오프

그것들은 각각 H_{hf}, H_{ff}, 그리고 H_{fh},로 표현된다. 네트워크 토폴로지는 (그림 14)와 같이 모바일 네트워크가 $N-1$개의 외부 네트워크들을 통과하여 이동한 후에 인트라넷(home network)으로 돌아오는 경우로 가정한다. 따라서, N이 보다 더 큰 경우, 모바일 네트워크는 홈 네트워크로 돌아오기 전에, 그 홈 네트워크로 부터 더 멀리 여행한다. 예를 들어, 핸드오프 순서는 $H_{hf}H_{ff}H_{ff}$ ... $H_{ff}H_{fh}$로 나타날 수도 있다. (표 2)에는 분석에 사용되는 매개 변수가 나열되어 있다.

모바일 네트워크에 대하여 서브넷에서 네트워크 체류시간 t_M에 대한 pdf(확률밀도함수)를 $f_m(t)$으로 하고, $E[t_M]=1/\gamma$ 으로 하면 그것의 라플라스 변환은 다음과 같다.

$$f_m^*(s)=\int_{t=0}^{\infty} e^{-st} f_m(t)\,dt.$$

모바일 네트워크로 SIP 세션의 도착은 도착율 λ인 포아송 과정(Poisson process)을 따른다고 가정한다. 세션의 서비스 시간은 평균이 $1/\mu$인 지수분포를 따른다. (그림 14)를 참고하여 모바일 네트워크에 i개의 진행중인 세션이 있는 상태에서 모바일 네트워크가 두 이벤트 사이에서 k개의 서브넷을 통과할 확률을 $a(k)$로 정의한다. 여기서 이벤트는 새로운 세션이 도착하는 것이나 진행중인 세션이 모바일 네트워크로부터 벗어나는 것을 의미한다. 두 개의 연속된 이벤트 사이의 간격을 t_{s_i}으로 나타낸다. t_{s_i}동안 모바일 네트워크에는 i개의 진행중인 세션이 있다. 두개의 독립적인 포아송 과정의 자산의 합에 기반하여, t_{s_i}는 새로운 포아송 과정의 중간 도착 시간이라고 생각할 수 있다. 따라서

$$E\left[t_{s_i}\right]=\frac{1}{\pi_i}=\begin{cases}\dfrac{1}{\lambda+i\mu}, 0\le i\le c\\ \dfrac{1}{i\mu}, i=c,\end{cases} \quad (1)$$

여기에서, c는 모바일 네트워크에서 허용되는 진행중인 세션의 최대수이다. 위의 가정에 따라서 다음을 얻을 수 있다.

$$a_i(k)=\begin{cases}1-\dfrac{\left(1-f_m^*(\pi_i)\right)\gamma}{\pi_i}, k=0,\\ \dfrac{\gamma}{\pi_i}\left[1-f_m^*(\pi_i)\right]^2\left[f_m^*(\pi_i)\right]^{k-1}, k>0.\end{cases} \quad (2)$$

간략화하기 위해, 논문의 나머지에서는 $g_i=f_m^*(\pi_i)$으로 표현한다. 여기에서 $k=jN+q$ 그리고 $0\le q<N$ 으로 하면,

$$a_i(jN+q)=\frac{\gamma(1-g_i)^2}{\pi_i g_i}\left(g_i{}^N\right)^j g_i{}^q=yz^jx^q, \quad (3)$$

여기서

$$y = \frac{\gamma(1-g_i)^2}{\pi_i g_i}, z = g_i^N, x = g_i.$$

수치적 증명을 위해, 네트워크 거주 시간이 감마분포를 따른다고 가정한다. 감마확률변수의 라플라스 변환은 다음과 같이 표현된다.

$$f_m^*(s) = \left(\frac{\gamma\beta}{s+\gamma\beta}\right)^\beta \quad (4)$$

이에 따라서, 다음을 얻을 수 있다.

$$g_i = f_m^*(\pi_i) = \left(\frac{\gamma\beta}{\pi_i+\gamma\beta}\right)^\beta \quad (5)$$

제안한 CR-SeMMS에서 모바일 네트워크는 여러 개의 네트워크을 통과하여 이동할 때, 그것의 위치를 업데이트하기 위하여 SIP registrar에 등록을 수행할 필요가 있다. 또한 모바일 네트워크내에 여러 개의 MN과의 진행중인 세션이 있다면 여러 개의 CN으로 re-INVITE 메시지를 보낼 필요가 있다. 따라서 비용은 SIP-NVG를 위한 등록비용과 세션을 지속적으로 유지하기 위한 re-INVITE 비용으로 구성된다. 등록 비용은 SIP-NVG가 전체 모바일 네트워크 대신에 SIP registrar에 등록할 수 있기 때문에, 모바일 네트워크에 있는 진행중인 세션의 수와 관계가 없다. 반면에, re-INVITE 비용은 모바일 네트워크에 있는 진행중인 세션의 수에 따라 달라진다. 진행중인 세션의 수가 증가하면 비용도 증가한다. 그러나, URI 목록이 하나의 re-INVITE 메시지에 포함되도록 설계하기 때문에, 실제로 각각의 CN으로 re-INVITE 메시지를 보내기 전의 re-INVITE 비용은 모바일 네트워크에 얼마나 많은 진행중인 세션이 있는가에 상관없이 거의 일정하다. 또한, REGISTER 또는 INVITE 요청시 HOTP기반의 인증방식을 사용함으로써 한번의 핸드쉐이크로 클라이언트 인증을 수행한다. 이것은 시그널링 메시지를 처리할 때 Request/Response 횟수를 줄여줌으로 시그널링 처리 비용을 상당히 줄여준다. 그것은 (그림 7), (그림 12) 그리고 (그림 13)에서 볼 수 있다. 그리고 각 시그널링 비용에 대한 매개변수를 (표 3)과 같이 정의한다.

따라서, 핸드오프에 대한 시그널링 비용을 다음과 같이 나타낼 수 있다.

$$\begin{aligned} S_{hf}^i &= R_f + L_{hf} + iI_{hf}, \\ S_{ff}^i &= R_f + L_{ff} + iI_{ff}, \\ S_{fh}^i &= R_h + L_{fh} + iI_{fh} \end{aligned} \quad (6)$$

(표 3) 핸드오프 시그널링 비용 매개변수 정의

변수	설 명
S_{hf}^i	i 개의 진행중인 세션을 가진 모바일 네트워크가 홈 네트워크에서 외부 네트워크로 이동시 평균 핸드오프비용.
S_{ff}^i	i 개의 진행중인 세션을 가진 모바일 네트워크가 외부 네트워크에서 또다른 외부 네트워크로 이동시 평균 핸드오프비용.
S_{fh}^i	i 개의 진행중인 세션을 가진 모바일 네트워크가 외부 네트워크에서 홈 네트워크로 이동시 평균 핸드오프비용.
R_h	모바일 네트워크가 그것의 홈 네트워크로 들어갈 때 모바일 네트워크의 평균 등록 비용.
R_f	모바일 네트워크가 외부 네트워크로 들어갈 때 모바일 네트워크의 평균 등록 비용.
L_{hf}	모바일 네트워크가 그것의 홈 네트워크로 부터 외부 네트워크로 이동시 첫번째 re-INVITE에 대한 평균 비용.
L_{ff}	모바일 네트워크가 외부 네트워크로 부터 또다른 외부 네트워크로 이동시 첫번째 re-INVITE에 대한 평균 비용.
L_{fh}	모바일 네트워크가 외부 네트워크로 부터 그것의 홈 네트워크로 이동시 첫번째 re-INVITE에 대한 평균 비용.
I_{hf}	모바일 네트워크가 그것의 홈 네트워크로 부터 외부 네트워크로 이동시 두번째 re-INVITE에 대한 평균 비용.
I_{ff}	모바일 네트워크가 외부 네트워크로 부터 또다른 외부 네트워크로 이동시 두번째 re-INVITE에 대한 평균 비용.
I_{fh}	모바일 네트워크가 외부 네트워크로 부터 그것의 홈 네트워크로 이동시 두번째 re-INVITE에 대한 평균 비용.

(그림 14)에서 처럼, 모바일 네트워크가 t_{s_i}동안 k개의 서브넷을 통과 한다고 가정한다. 그리고 모바일 네트워크가 인트라넷을 방문한 시간부터 마지막의 이벤트가 발생하는 시간까지 그것이 통과하는 서브넷의 수를 σ로 나타낸다.

$0<\sigma<N$ 일때, t_{s_i}동안의 모바일 네트워크에서의 총 시그널링 비용은 다음과 같다.

$$\begin{aligned} & C_i(N,\pi_i,\gamma,\sigma) \\ &= \sum_{k=0}^{\infty}\left\{S_{hf}^i\left[\frac{k+\sigma-1}{N}\right]+S_{fh}^i\left[\frac{k+\sigma}{N}\right]\right. \\ &= S_{ff}^i\frac{\gamma}{\pi_i}+\frac{\left(S_{hf}^i g_i-S_{ff}^i g_i+S_{fh}^i-S_{ff}^i\right)\left(1-g_i\right)g_i^{N-1}\gamma}{\left(1-g_i^{N}\right)g_i^{\sigma}\pi_i} \end{aligned} \tag{7}$$

만약 σ이 지수분포를 따른다면, σ에 대한 p.d.f 는 다음과 같다.

$$\delta_\sigma=\begin{cases} e^{-\sigma}\left(\dfrac{1-2e^{-(N+1)/2}+e^{-1}}{1-e^{-1}}\right), 0\le\sigma\le\dfrac{N-1}{2} \\ e^{-(N-\sigma)}\left(\dfrac{1-2e^{-(N+1)/2}+e^{-1}}{1-e^{-1}}\right), \dfrac{N-1}{2}<\sigma\le N-1 \end{cases} \tag{8}$$

따라서,

$$\begin{aligned} & C_{i\_exponential}(N,\pi_i,\gamma) \\ &= \sum_{\sigma=0}^{N-1}\delta_\sigma C_i(N,\pi_i,\gamma,\sigma)=S_{ff}^i\frac{\gamma}{\pi_i}+\frac{\gamma\left(1-g_i\right)}{\pi_i\left(1-g_i^{N}\right)} \\ &\left\{\frac{\left(1-e^{-1}\right)\left(S_{hf}^i-S_{ff}^i+\left(S_{fh}^i-S_{ff}^i\right)g_i^{N-1}\right)}{1-2e^{-(N+1)/2}+e^{-1}}\right. \\ &+\frac{\left(1-e^{-1}\right)\left(S_{hf}^i g_i-S_{ff}^i g_i+S_{fh}^i-S_{ff}^i\right)g_i^{N-1}}{1-2e^{-(N+1)/2}+e^{-1}} \\ &\left.\left(\sum_{\sigma=1}^{(N-1)/2}\frac{e^{-\sigma}}{g_i^{\sigma}}+\sum_{\sigma=(N+1)/2}^{N-1}\frac{e^{-(N-\sigma)}}{g_i^{\sigma}}\right)\right. \end{aligned} \tag{9}$$

위에 언급된 내용처럼, 모바일 네트워크로의 세션의 도착은 포아송 과정(Poisson process)을 따른다. 그리고 세션 서비스 시간은 지수분포를 따른다. 뿐만 아니라, 모바일 네트워크에서 허용되는 진행중인 세션의 최대 수는 c 값으로 제한되어있다. 따라서, 모바일 네트워크에서의 진행중인 세션의 수를 M/M/c/c 큐잉 시스템(queuing system)으로 모델링 할 수 있다. 모바일 네트워크에 i개의 진행중인 세션이 있는 안정상태확률(steady state probability)은 다음 수식에 의해 얻어진다. [22]

$$P_i=\frac{\lambda^i}{i!\mu!}\left(\sum_{x=0}^{c}\frac{\lambda^x}{x!\mu^x}\right)^{-1} \tag{10}$$

결과적으로, 단위 시간 당 평균 핸드오프-시그널링 비용은 다음과 같다.

$$\sum_{i=0}^{c}C_{i\_exponential}P_i\pi_i \tag{11}$$

위 수식에서 π_i와 p_i값은 (1) 과 (10)에서 얻을 수 있다.

또한, 우리는 이동패턴의 변화에 따른 영향을 고려하여, 평균 체류 시간이 감마분포(gamma distributed [23], [24])를 따른다고 가정한다. 따라서, 그 변화는 다음과 같다.

$$Var=\frac{1}{\beta\gamma^2} \tag{12}$$

제안한 CR-SeMMS의 성능을 평가하기 위해, (표 4)와 같은 매개 변수들을 정의한다.

(표 4) CR-SeMMS 시그널링 비용 매개변수 정의

변수	설 명
a_x	노드 x에서 SIP registration에 대한 처리비용.
b_x	노드 x에서 SIP INVITE 메시지에 대한 처리비용.
$A_{x,y}$	노드 x와 노드 y사이에 SIP registration 전송비용.
$B_{x,y}$	노드 x와 노드 y사이에 SIP INVITE 메시지에 대한 전송비용.
U	SIP Proxy 1이 UAR/UAA 메시지를 처리하고 Diameter 서버로 전송하기 위한 전체비용.
M	SIP Proxy 2가 MAR/MAA 메시지를 처리하고 Diameter 서버로 전송하기 위한 전체비용.

(표 4)에서 x, y는 각각 MN, SIP-NVG, SIP Proxy 1, SIP Proxy 2 (SIP Registrar), ALG, 그리고 CN을 표시하는 mn, nvg, pro, reg, alg 또는 cn이 될 수 있다. 3 장에서 설명한 시그널링 메시지 흐름에 따라서, 위의 비용은 다음과 같이 계산된다.

$$R_h = a_{nvg} + a_{reg} + 2A_{nvg,reg} + M,$$

$$R_f = a_{nvg} + 2a_{pro} + a_{reg} + 2A_{nvg,pro} + 2A_{pro,reg} + U + M,$$

$$L_{hf} = 2b_{nvg} + 3b_{pro} + 4b_{reg} + 2b_{alg} + 3B_{nvg,pro} + 3B_{pro,reg} + 4B_{reg,alg} + B_{reg,cn} + M,$$

$$L_{ff} = 2b_{nvg} + 3b_{pro} + 2b_{reg} + b_{alg} + 3B_{nvg,pro} + 3B_{pro,reg} + 2B_{reg,alg} + M,$$

$$L_{fh} = 2b_{nvg} + 3b_{reg} + b_{alg} + 3B_{nvg,reg} + 2B_{reg,alg} + B_{reg,cn} + M,$$

$$I_{hf} = b_{mn} + b_{nvg} + b_{reg} + b_{cn} + 2B_{mn,nvg} + 2B_{reg,cn},$$

$$I_{ff} = b_{mn} + b_{nvg} + 2B_{mn,nvg},$$

$$I_{fh} = b_{mn} + b_{nvg} + 2B_{mn,nvg} + b_{reg} + b_{cn} + 2B_{reg,cn};$$

IETF MVPN에서의 시그널링 비용과 비교하기 위해, 우리는 Diameter MIPv4 Application [25]가 x-MIP을 인증하는 데 사용된다고 가정한다. 또한, 우리는 MN이 공유 모드(colocated mode)에 있다고 가정한다. FA mode의 분석은 거의 같은 결과를 가지고 있기 때문에 제시되지 않는다. 아래첨자 mn, mg, vpn, xha 그리고 iha는 각각 MN, Mobile Gateway, IPsec-based VPN gateway, x-HA 그리고 i-HA를 나타낸다. 그리고 (표 5)와 같이 매개 변수를 정의한다.

(그림 2)에 보여지는 시그널링 메시지 흐름에 따라. 위의 비용은 다음과 같이 계산된다.

$$M_x = 2d_{mg} + 2d_{xha} + 2W_{mn,mg} + 2W_{mg,xha} + 2H,$$

$$M_{i-o} = 2d_{mg} + 2d_{xha} + 2d_{vpn} + d_{iha} + 2W_{mn,mg} + 2W_{mg,xha},$$

$$M_{i-i} = d_{iha} + 2W_{mn,mg} + 2W_{mg,iha},$$

$$T_{est} = 2e_{mn} + 6e_{mg} + 6e_{xha} + 3e_{vpn} + 6Z_{mn,mg} + 6Z_{mg,xha} + 6Z_{xha,vpn},$$

$$T_{ter} = Z_{mn,mg} + Z_{mg,vpn} + e_{vpn}.$$

모바일 네트워크가 다른 네트워크 사이를 이동할 때 IETF MVPN의 핸드오프 비용은 다음과 같이 얻어진다.

(표 5) IETF MVPN 시그널링 비용 매개변수 정의

변수	설 명
M_x	x-MIP 등록 비용
M_{i-o}	MN이 인트라넷 외부에 위치할 때 i-MIP 등록 비용
M_{i-i}	MN이 인트라넷 내부에 위치할 때 i-MIP 등록 비용
T_{est}	IPsec 터널의 설정 비용
T_{ter}	IPsec 터널의 해지 비용
d_x	노드 x에서 MIP 등록에 대한 처리비용
e_x	노드 x에서 IPsec 메시지에 대한 처리비용
$W_{x,y}$	노드 x와 노드 y사이에 MIP 등록에 대한 전송 비용
$Z_{x,y}$	노드 x와 노드 y사이에 IPsec 메시지에 대한 전송 비용
H	x-HA가 HAR/HAA와 AMR/AMA 메시지를 처리하고 AAAF와 AAAH로 전송하기 위한 전체 비용

$$D_{hf} = M_x + M_{i-o} + T_{est},$$

$$D_{ff} = M_x,$$

$$D_{fh} = M_{i-i} + T_{ter}.$$

제안한 아키텍처에서, SIP-NVG는 전체 모바일 네트워크에 대한 이동성을 관리한다. 그러므로, 모바일 네트워크가 새로운 서브넷으로 이동하면, SIP-NVG은 전체 모바일 네트워크를 위해 SIP Registrar에 등록할수 있다. 한편 SIP-NVG가 없으면, 같은 모바일 네트워크에서 모든 MN은 개별적으로 그것의 위치를 업데이트할 필요가 있다. 따라서, 더 많은 시그널링 비용이 발생된다. 우리는 SIP-NVG이 없을때의 비용을 다음과 같이 재정의(6) 할 수 있다.

$$S^i_{hf} = mR_f + iL_{hf} + iI_{hf},$$

$$S^i_{ff} = mR_f + iL_{fh} + iI_{ff},$$

$$S^i_{fh} = mR_h + iL_{hh} + iI_{fh}.$$

위 수식에서 m은 모바일 네트워크에 연결하는 MN의 갯수라고 가정한다. 또한, 제안한 아키텍처에서 사용하는 HOTP(An HMAC based One-Time Password) 인증방식은 이벤트 동기화 방식으로, 한번의 핸드쉐이크로 클라이언트 인증을 수행한다. 반면에 많은 보안프로토콜에서 채

택하고 있는 HTTP 다이제스트 인증방식은 Challenge-Response 패러다임을 기반으로 한다. 따라서, SIP 서버의 클라이언트가 SIP REGISTER와 INVITE 메시지 발송시 SIP Registrar는 사용자의 인증 및 인가를 위하여 Diameter 서버에 UAR/UAA, MAR/MAA 명령을 사용하여 인증을 수행하는데, 이 과정에서 SIP 서버의 클라이언트와 Diameter 서버간에 두번의 핸드쉐이크가 발생한다. 따라서 HTTP 다이제스트 인증방식 사용시의 비용은 다음과 같이 계산된다.

$$
\begin{aligned}
R_h &= 2a_{mg} + 2a_{reg} + 4A_{mg,reg} + 2M,\\
R_f &= 2a_{mg} + 4a_{pro} + 2a_{reg} + 4A_{reg,pro} + 4A_{pro,reg} + 2U + 2M,\\
L_{hf} &= 3b_{mg} + 5b_{pro} + 5b_{reg} + 2b_{alg} + 5B_{reg,pro} + 5B_{pro,reg}\\
&\quad + 4B_{reg,alg} + B_{reg,cn} + 2M,\\
L_{ff} &= 3b_{mg} + 5b_{pro} + 3b_{reg} + b_{alg} + 5B_{reg,pro} + 5B_{pro,reg}\\
&\quad + 2B_{reg,alg} + 2M,\\
L_{fh} &= 3b_{mg} + 4b_{reg} + b_{alg} + 5B_{mg,reg} + 2B_{reg,alg} + B_{reg,cn} + 2M,\\
I_{hf} &= b_{mn} + b_{mg} + b_{reg} + b_{cn} + 2B_{mn,mg} + 2B_{reg,cn},\\
I_{ff} &= b_{mn} + b_{mg} + 2B_{mn,mg},\\
I_{fh} &= b_{mn} + b_{mg} + 2B_{mn,mg} + b_{reg} + b_{cn} + 2B_{reg,cn};
\end{aligned}
$$

5. 수치적 결과

이번 장에서는 4장에서 제시한 분석에 대한 수치적 결과를 제공한다. 4장에서 설명한 바와 같이, 시그널링 비용 함수는 전송 비용과 처리 비용으로 구성된다. 우리는 전송비용이 발신지와 목적지 노드 사이의 거리에 비례한다고 가정하고, 처리비용은 SIP 메시지[26], [27], [28], [29]를 처리하는 것과 확인하는 것을 포함한다고 가정한다. 성능을 설명하기 위해, 합리적으로 선택된 매개변수 값이 (표 6)에 나열되어 있다.

그리고, IETF MVPN의 시그널링 비용과 비교하기 위해, 우리는 x-HA이 VPN gateway 그리고 AAAF와 함께 위치한다고 가정하고, i-HA는 SIP Proxy 2/ Registrar와 같은 지점에 위치한다고 가정한다. 그리고, IETF MVPN에서의 AAAH는 CR-SeMMS에서의 Diameter 서버와 같은 지점에 위치한다. 제안된 CR-SeMMS에서, 주요한 목적중의 하나는 VPN을 지원하면서 핸드오브에 대한 시그널링 비용을 감소시키는 것이다.

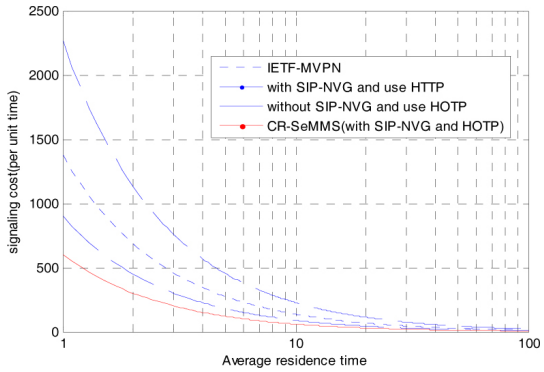
(그림 15)는, SIP-NVG가 있는, SIP-NVG가 없는, 그리

(표 6) 성능평가를 위한 변수 값

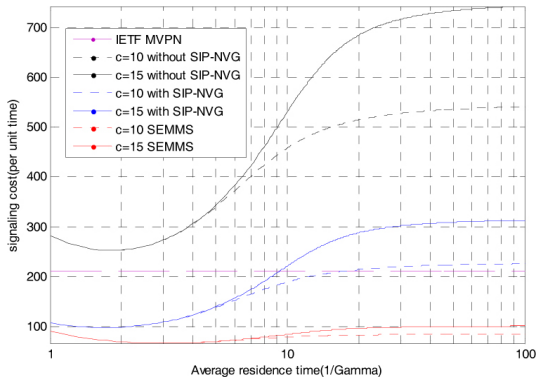
변수	값		변수	값
a_{mg}	25.0		$A_{nvg,reg}$	5.0
a_{pro}	5.0		$A_{nvg,pro}$	10.0
a_{reg}	25.0		$A_{pro,reg}$	0.1
b_{mn}	5.0		$B_{mn,nvg}$	1.0
b_{nvg}	25.0		$B_{nvg,reg}$	5.0
b_{pro}	5.0		$B_{nvg,pro}$	10.0
b_{reg}	40.0		$B_{pro,reg}$	0.1
b_{alg}	50.0		$B_{reg,alg}$	0.1
b_{cn}	10.0		$B_{reg,cn}$	0.5
U	30.0		M	40.0
d_{mg}	10.0		$W_{mn,mg}$	1.0
d_{xha}	25.0		$W_{mg,xha}$	10.0
d_{vpn}	40.0		$W_{xha,vpn}$	1.0
d_{iha}	25.0		$W_{vpn,iha}$	0.1
H	80.0		$W_{mg,iha}$	5.0
e_{mn}	5.0		$Z_{mn,mg}$	1.0
e_{mg}	10.0		$Z_{mg,xha}$	10.0
e_{xha}	25.0		$Z_{xha,vpn}$	1.0
e_{vpn}	40.0		$Z_{mg,vpn}$	11.0

고 HTTP 인증 방식을 사용하는 상태에서의 평균 시그널링 비용이 IETF MVPN과 비교된것을 보여

준다. 위에서 정의한 것과 같이, m은 모바일 네트워크에 연결하는 MN의 갯수이다. 그리고, 우리는 $N=7$, $m=5$, $c=10$ 그리고 $\rho=\lambda/\mu=5$라고 가정한다. SIP 기반 프로토콜에서, SIP re-INVITE 명령과 SIP 등록 명령은 각각의 핸드오프 동안 수행될 필요가 있다. 따라서, SIP 기반 프로토콜에 대한 시그널링 비용은 MIP에서의 비용보다 더 높을 것이다. 그러나, (그림 15)는 SIP-NVG를 가진 CR-SeMMS가 IETF MVPN보다 핸드오프에 대하여 더 적은 시그널링 비용을 갖는다는 것을 보여준다. 이것은 IETF MVPN가 세 개의 터널을 설정하기 위해서 특정한 시간을 필요로 하기 때문이다. 뿐만 아니라, IETF MVPN은 단일 노드의 이동성을 위해 설계되었기 때문이다. SIP-NVG가 없는 모바일 네트워크와 비교하면, 예상대로, 제안된 CR-SeMMS가 핸드오프 시그널링 비용을 상당히 줄여준다. 이것은 모바일 네트워크가 새로운 서



(그림 15) 다른 체류시간(residence time) 에서의 시그널링 비용 비교



(그림 16) IETF, without SIP-NVG, with SIP-NVG, SEMMS에서의 시그널링 비용 비교

브넷으로 이동하는 경우, SIP-NVG은 전체 모바일 네트워크를 대표하여 SIP Registrar에 등록할 수 있다. 그러나 SIP-NVG가 없으면, 같은 모바일 네트워크에서 모든 MN은 개별적으로 그것의 위치를 업데이트 해야하기 때문이다. 또한, HTTP 다이제스트 인증방식을 사용하는 모바일 네트워크와 비교하면, HOTP 인증방식 사용시 더 적은 시그널링 비용을 갖는다는 것을 보여준다. 이것은 SIP 서버의 클라이언트가 SIP REGISTER와 INVITE 메시지를 처리시 Diameter 서버간에 두번의 핸드쉐이크를 필요로 하기 때문이다. 우리는 또한 평균 네트워크 체류시간이 증가할 때, 즉 모바일 네트워크가 상대적으로 낮은 이동성을 가지고 있을 때, 핸드오프에 대한 시그널링 비용이 감소하는 것을 볼 수 있다.

(그림 16)은 ρ대비 핸드오프에 대한 평균 시그널링 비용을 보여준다. 여기에서 매개 변수는 $\gamma=0.1$인 경우를 제외하고는 (그림 15)에서의 것과 동일한 값을 사용한다. (그림 15)와 마찬가지로, 제안한 CR-SeMMS는 SIP-NVG가 없는 것, 그리고 HTTP 인증방식을 사용하는 것 보다 핸드오프에 대하여 더 적은 시그널링 비용을 가지고 있다. 한편, IETF MVPN는 ρ에 따라 CR-SeMMS보다 더 높은 또는 더 낮은 시그널링 비용을 갖을 수 있다. 이것은 MIP에서 핸드오프에 대한 시그널링 비용이 세션 갯수에 독립적이기 때문이다. MIP는 단지 IP 계층에서 이동성을 관리한다. 따라서, 핸드오프에 대한 시그널링 비용은 세션 용량, 그리고 모바일 네트워크에서 세션의 갯수를 나타내는 ρ에 관계없이 일정하게 유지된다. (그림 16)에서, MN이 x-HA와 i-HA로 보내는 정기적인 위치 업데이트 비용은 고려되지 않았다. 또한, 우리는 x-HA가 최적의 위치에 놓인다고 가정한다. 이러한 요소들이 포함될 경우, IETF MVPN에 대한 비용은 훨씬 더 높게 나타날 것이다. (그림 16)은 CR-SeMMS에서의 시그널링 비용이 IETF MVPN에서의 비용보다 더 높을 수 있다는 것을 보여주지만, CR-SeMMS에서의 패킷 전송 비용은 IETF MVPN에서의 비용보다 매우 낮은것을 보여준다. 이것은 CR-SeMMS에서는, 삼각 라우팅 그리고 세 개의 터널과 같은 사안이 없기 때문이다. 우리는 또한 ρ가 증가할 때, SIP 기반 솔루션(SIP-based solutions)에 대한 평균 비용 역시 증가하는 것을 볼수있다. 그 이유는, 진행중인 세션이 많을수록, 세션 연속성을 유지하기 위해 더 많은 re-INVITE 메시지가 필요하기 때문이다. 게다가, ρ가 20보다 더 큰 경우에는, (그림 16)에 표현된 모든 기법의 비용은 거의 일정하게 유지된다. 이것은 ρ가 20에 근접할 때, 각 기법에서 진행중인 세션의 숫자가 모바일 네트워크에서 허용되는 최대 개수에 도달하기 때문이다. SIP 기반 기법(SIP-based techniques)에서 $c=10$ 그리고 $c=15$인 경우와 비교하면, $c=15$인 경우에 모바일 네트워크상에 더 많은 세션이 존재한다. 따라서, re-INVITE 메시지에 대하여 더 많은 시그널링 비용이 발생한다. 그리고, 홈 네트워크로부터 외부 네트워크로의 이동은 다른 유형의 핸드오프보다 더 높은 시그널링 비용의 원인이 되기 때문에, 홈 네트워크를 빈번하게 방문하는 것은 더 많은 시그널링 비용의 결과를 가져온다.

6. 결 론

IETF는 모바일 VPN 아키텍처를 제안했지만, 그것은 시그널링 노드의 움직임을 위해 설계되었다. 게다가 IETF MVPN은 하나의 IPSec 터널과 두 개의 MIP터널이

필요하기 때문에 실시간 패킷을 전송하기 위한 대형 오버헤드를 가지고 있다. 다른 한편으로는, NEMO가 네트워크 이동성을 지원하지만, NEMO에서 모바일 VPN을 지원하기 위한 효율적인 방법은 없다.

이 논문은 NEMO에서의 MVPN을 지원하는 방법을 제안하여 전체 네트워크가 이동시, 지속적으로 세션을 유지하도록 하였으며, HOTP 기반의 인증방식을 제안하여 세션을 유지하기 위해 지속적으로 발생하는 시그널링 처리시간을 단축하도록 설계 하였다. 또한 NEMO와 VPN을 통합하여 보안성을 높였으며 HOTP 인증방식을 사용하여 시그널링 비용을 감축한 CR-SeMMS에 대한 설계와 성능분석을 하였다. 제안한 CR-SeMMS는 특히 실시간 서비스에 적합하도록 만들어진 SIP을 기반으로 한다. 그러나 SIP기반의 이동성 관리가 라우팅 최적화를 지원하기 쉬울지라도, NEMO에서 SIP를 채택함으로 인하여, 진행중인 세션을 유지하기 위해 많은 시그널링 메시지를 전송하기 때문에 핸드 오프 동안 시그널링 비용이 증가될 수 있다. 제안한 CR-SeMMS에서 URI 목록은 각각의 노드에 개별적으로 시그널링 메시지를 전송하는것 대신에 SIP Proxy 서버를 알리는데 이용된다. 따라서 시그널링 비용은 감소한다. 또한, 기존 HTTP 다이제스트 인증방식에 따른 사용자 인증시는 여러 번의 핸드쉐이크를 필요로 하여 많은 시그널링 비용이 발생하였으나, 제안한 CR-SeMMS는 인증시 HOTP에 기반한 인증방식을 사용함으로 인하여 인증서버와의 핸드쉐이크 횟수를 상당히 단축하였다. 따라서 시그널링 비용은 감소한다. SIP Proxy 서버와 Diameter 서버는 인증과 권한부여에 대한 책임이 있다. 그리고, ALG는 MIDCOM 아키텍처에 따라서, 데이터 전송을 위한 보안정보 처리를 위해 SIP Proxy 서버로 부터의 명령을 받아들인다. ALG는 보호된 그리고 보호되지 않은 데이터를 전환 그리고 중계할 책임이 있다. 따라서, 비 인가된 데이터는 인터넷에서 ALG를 통과할 수 없다. 본 논문에서는 모바일 VPN과 NEMO를 통합함으로써 실시간 서비스를 위한 효율적인 그룹 이동성 관리 그리고 비용 절감 방법에 대해 살펴보았다. NEMO는 현재 연구 초기단계로 다양한 기술 및 정책들이 융합되어 실현될 것으로 생각되며, 효율적인 서비스를 위해 경로 최적화 방법, 멀티호밍 기술, 포괄 이동 네트워크에서 서비스 방법 등이 앞으로 연구되어야 할 분야이다. 또한 상용 서비스를 하기 위해서는 빠른 이동 감지 기술에 대한 연구도 필요하다.

ACKNOWLEDGMENT

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

참 고 문 헌

[1] V. Schena and G. Losquadro, “FIFTH Project Solutions Demonstrating New Satellite Broadband Communication System for High Speed Train,” Proc. IEEE Vehicular Technology Conf., pp. 2831-2835, May 2004.

[2] “WirelessCabin Project,” http://www.wirelesscabin.com, 2011.

[3] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert,“Network Mobility (NEMO) Basic Support Protocol,” IETF RFC 3963, Jan. 2005.

[4] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” IETF RFC 2401, Nov. 1998.

[5] D. M’Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen,”HOTP: An HMAC-Based One-Time Password Algorithm”,RFC 4226, December 2005.

[6] S. Vaarala and E. Klovning, “Mobile IPv4 Traversal Across IPsec-Based VPN Gateways,” IETF RFC 5265, June 2008.

[7] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),”IETF RFC 2409, Nov. 1998.

[8] J.-C. Chen, Y.-W. Liu, and L.-W. Lin, “Mobile Virtual Private Networks with Dynamic MIP Home Agent Assignment,” Wireless Comm. and Mobile Computing, vol. 6, no. 5, pp. 601-616, Aug. 2006.

[9] J.-C. Chen, J.-C. Liang, S.-T. Wang, S.-Y. Pan, Y.-S. Chen, and Y.-Y. Chen, “Fast Handoff in Mobile Virtual Private Networks,” Proc. IEEE Int’l Symp. World of Wireless Mobile and Multimedia Networks (WoWMoM ’06), pp. 548-552, June 2006.

[10] S.-C. Huang, Z.-H. Liu, and J.-C. Chen, “SIP-Based Mobile VPN for Real-Time Applications,” Proc. IEEE Wireless Comm. And Networking Conf. (WCNC ’05), pp. 2318-2323, Mar. 2005.

[11] Z.-H. Liu, J.-C. Chen, and T.-C. Chen, “Design and Analysis of SIP-Based Mobile VPN for Real-Time Applications,” IEEE Trans. Wireless Comm., vol. 8, no. 11, pp. 5650-5661, Nov. 2009.

[12] A. Dutta, F. Vakil, J.-C. Chen, M. Tauil, S. Baba, N. Nakajima, and H. Schulzrinne, “Application Layer Mobility Management Scheme for Wireless Internet,” Proc. IEEE Int’l Conf. Third Generation Wireless and beyond (3G Wireless), pp. 379-385, May 2001.

[13] D. Vali, S. Paskalis, A. Kaloxylos, and L. Merakos, “An Efficient Micro-Mobility Solution for SIP Networks,” Proc. IEEE GLOBECOM, pp. 3088-3092, Dec. 2003.

[14] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, “The Secure Real-Time Transport Protocol (SRTP),”IETF RFC 3711, Mar. 2004.

[15] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, “MIKEY: Multimedia Internet KEYing,” IETF RFC 3830, Aug. 2004.

[16] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko,“Diameter Base Protocol,” IETF RFC 3588, Sept. 2003.

[17] M. Garcia-Martin, M. Belinchon, M. Pallares-Lopez, C. Canales, and K. Tammi, “Diameter 세션 Initiation Protocol (SIP) Application,” IETF RFC 4740, Nov. 2006.

[18] P. Srisuresh, J. Kuthan, J. Rosenberg, A. Molitor, and A. Rayhan, “Middlebox Communication Architecture and Framework,” IETF RFC 3303, Aug. 2002.

[19] M. Handley and V. Jacobson, “SDP: 세션 Description Protocol,” IETF RFC 2327, Apr. 1998.

[20] J.-C. Chen and T. Zhang, IP-Based Next-Generation Wireless Networks. John Wiley and Sons, Jan. 2004.

[21] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” IETF RFC 3550, July 2003.

[22] D. Gross and C.M. Harris, Fundmentals of Queueing Theory. John Wiley and Sons, 1998.

[23] M.M. Zonoozi and P. Dassanayake, “User Mobility Modeling and Characterization of Mobility Patterns,” IEEE J. Selected Areas Comm., vol. 15, no. 7, pp. 1239-1252, Sept. 1997.

[24] Y. Fang and I. Chlamtac, “Teletraffic Analysis and Mobility Modeling of PCS Networks,” IEEE Trans. Comm., vol. 47, no. 7, pp. 1062-1072, July 1999.

[25] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, and P. McCann, “Diameter Mobile IPv4 Application,” RFC 4004, Aug. 2005.

[26] J. Xie and I.F. Akyildiz, “A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP,” IEEE Trans. Mobile Computing, vol. 1, no. 3, pp. 163-175, July-Sep. 2002.

[27] W. Ma and Y. Fang, “Dynamic Hierarchical Mobility Management Strategy for Mobile IP Networks,” IEEE J. Selected Areas Comm., vol. 22, no. 4, pp. 664-676, May 2004.

[28] R. Rummler, Y.W. Chung, and A.H. Aghvami, “Modeling and Analysis of an Efficient Multicast Mechanism for UMTS,” IEEE Trans. Vehicular Technology, vol. 54, no. 1, pp. 350-365, Jan. 2005.

[29] S. Fu, M. Atiquzzaman, L. Ma, and Y.-J. Lee, “Signaling Cost and Performance of SIGMA: A Seamless Handover Scheme for Data Networks,” Wireless Communications and Mobile Computing, vol. 5, no. 7, pp. 825-845, Nov. 2005.

◐ 저 자 소 개 ◑

조 철 희 (Chul-Hee Cho)

2011년 성균관대학교 정보통신대학원 정보보호학과(공학석사)
관심분야 : 네트워크 보안, 무선이동 네트워크, 암호학 etc.
E-mail : chuli77@skku.edu

정 종 필 (Jong-Pil Jong)

1997년 성균관대학교 정보통신공학과(공학사)
2003년 성균관대학교 대학원 정보통신공학과(공학석사)
2008년 성균관대학교 대학원 정보통신공학과(공학박사)
2008년~현재 성균관대학교 정보통신공학과 교수
관심분야 : 모바일컴퓨팅, 센서이동성, 차량모바일네트워크, 스마트기기보안, 네트워크보안, IT융합, 인터렉션사이언스 etc.
E-mail : jpjeong@skku.edu