韓國컴퓨터情報學會 論文誌
第14卷 第12號, 2009. 12.

2009-14-12-3-7

SIP기반 홈네트워킹 보안 기술에 관한 연구

함 영 옥*, 신 용 태**

A study with respect to the home networking security Technology based on SIP

Yoeng-ock Ham*, Young-tae Shin**

요 약

홈 네트워크는 유무선 네트워크를 기반으로 언제, 어디서나 정보가전 및 기기제어와 양방향 멀티미디어 서비스를 이용할 수 있는 주거환경을 일컫는다. 홈 네트워크가 점차 활성화되고 있는 현시점에서 댁내망은 PC 뿐만 아니라 홈오토메이션, 백색가전 등 다양한 기기들로 구축되기 때문에 외부의 공격 형태 및 피해 양상 역시 다양하게 나타날 수 있다. 그래서 본 논문에서 홈 네트워크에 대한 침입에 대응할 수 있는 SIP 기반 홈 네트워킹인 SSIP(Secure Session Initiate Protocol) 모델을 제안한다. 본 논문에서 제안하는 SIP 기반 홈네트워킹인 SSIP(Secure Session Initiate Protocol) 모델은 홈 게이트웨이에서 수행하는 Cluster-to-Cluster 환경에 SIP 의 인증기능을 추가하여 효과적인 인증과 세션 재설정시에 세션 시간 및 셋업 시간을 줄여 주는 효율적이고 신뢰성 있는 시스템이다.

Abstract

Generally home networks are based on wired network and wireless network. This makes customers be capable of using electric home appliances and full-duplex multimedia services and controlling the machines without any restrictions of place or time. Now that the scope of home security is being extended, the home networks can be formed with not only personal computer but also home automation, electric home appliances, and etc. But this causes many of attacks of invasion and damages. Therefore in this paper we suggest the SSIP(Secure Session Initiate protocol) model for solving those problems. The SSIP model is able to provide an efficient authentication and reduce the time of session re-establishment and set-up by adding ability of SIP authentication to Cluster-to-Cluster environment performed on home gateway.

▸ Keyword : 홈네트워크(home networks), 보안(security), 인증(authentication), SSIP(Secure Session Initiate Protocol)

• 제1저자 : 함영옥 교신저자 : 신용태
• 투고일 : 2009. 08. 27, 심사일 : 2009. 09. 03, 게재확정일 : 2009. 12. 24.
* 숭실대학교 컴퓨터학과 박사과정 수료 ** 교신저자 : 숭실대학교 컴퓨터학과 교수

Ⅰ. 서 론

IT 기술의 급속한 발달과 초고속망을 통한 인터넷 보급에 힘입어, 기업이나 공공기관의 사무실 중심으로 구축되던 네트워크 환경이 가정내의 디지털 전자기기로 확산되어 가면서 홈 네트워크 산업과 관련기기 시장에 대한 관심이 높아지고 있다. 홈 네트워크란 정보의 처리, 관리, 전달 및 저장에 있어 가정 내에 설치되어 각종 계산, 관리, 감시 및 통신기능을 수행하는 기기들을 연결하고 통합할 수 있게 해주는 구성요소들의 집합으로서 데이터와 통신의 공유 및 상호이동을 가능하게 하는 2개 이상 장비의 조합으로 이루어진다.

홈네트워크 구성 기술은 보안이라는 문제를 간과 할 수 없다. 홈네트워크는 인증 절차의 신뢰성을 통해 악의적인 공격으로부터 내부 네트워크를 안전하게 보호하는 방법을 요구한다. 본 논문에서 제안하고자 하는 보안 메커니즘은 위 문제를 해결하기 위해 검증되고 안전한 SIP(Session Initiation Protocol)를 게이트웨이에 적용한 Cluster-to-Cluster 홈 네트워크를 제안한다.

Ⅱ. 관련 연구

1. SIP(Session Initiation protocol)

1.1 SIP의 특징

인터넷 프로토콜 기반 네트워크에서 하나 이상의 단말간에 멀티미디어 세션이나 호를 생성, 변경, 종료할 때 쓰이는 SIP는 응용계층 제어 프로토콜로 이러한 세션(Session)에는 멀티미디어 컨퍼런스(Multimedia Conference), 인터넷 텔레폰, 원격교육 등이 포함된다.

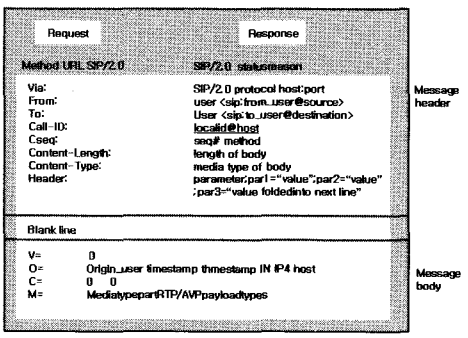

그림 1. SIP 메시지
Fig. 1. SIP Message

SIP 메시지는 클라이언트에서 서버로 보내는 요청(Request)과 서버에서 클라이언트로 보내는 응답(Response)이 있다. 그림 1.에서 보듯이 SIP 메시지는 start line, header line, message body 로 구성되는데 다양한 header field 호 서비스, 주소, 프로토콜 특성에 관한 정보를 그림 1. SIP 메시지가 갖고 있다. SIP 요청을 메소드(Method)라 하며 SIP 메소드는 다른 UA(User Agent) 또는 프락시 서버(Proxy Server)에 의해서 수행될 특정 서비스를 요청한다. 여섯 가지 메소드(INVITE, REGISTER, BYE, ACK, CANCEL 및 OPTIONS)들이 SIP 2.0 Specification Document 에 정의되어 있으며 INFO 와 PRACK 메소드는 ID(Internet Draft)에 정의되어 있다.

1.2 SIP의 네트워크 구성요소

SIP 네트워크는 UA(User Agent), 프락시 서버(Proxy Server), 리다이렉트 서버(Redirect Server), Register 로 구성된다. SIP 에서는 두 종류의 클라이언트와 서버들이 정의되며 클라이언트와 서버는 SIP 주소에 의해서 인식된다.

1.2.1 SIP UA (User Agent)

SIP 를 지원하는 단말기를 SIP UA(User Agent)라 한다. SIP 프로토콜의 주목적은 두 SIP 들간의 미디어 세션을 설립하는 것이다. UA 는 사용자로부터 입력을 받아 다른 UA 와의 미디어 세션을 설립 및 종료를 중계하는 역할을 한다. SIP 는 어떤 프로토콜이든 사용되기 때문에 UA 는 메시지 전송을 위하여 TCP 또는 UDP 를 지원해야 한다.

UA 는 초기화 또는 참가하고 있는 호의 state 정보를 유지해야 한다. 최소한의 state 정보는 local&remote URL, local&remote CSeq 헤더 및 미디어에 필요한 정보등을 가지고 있어야 하며 이러한 정보는 신뢰성과 호 구별을 위해서 필요하다. Remote CSeq 는 두 번째 INVITE 와 재전송 사이를 구별하는데 필요하다. 두 번째 INVITE 메시지는 기존 호의 파라미터를 변경할 때 사용된다. 이 때 같은 Call-ID 를 사용하지만 새로운 요청이기 때문에 CSeq 는 하나 증가된다. 한편 재 전송된 INVITE 는 전번 INVITE 와 같은 Call-ID 와 CSeq 를 사용한다. 호가 종료된 후에도 호 종료 메시지의 분실 가능성이 있기 때문에 UA 는 적어도 32초 동안은 호 상태 정보를 유지해야 한다.

표 1. User Agent 유형
Table 1. A type of User Agent

User Agent type	Supports
Minimum	INVITE, ACK, SDP, response classes
Basic	Minimum plus BYE
Redirection	Basic plus Contact header
Firewall friendly	Redirection plus Route, Record-Route, and default proxy server
Negotiation	Firewall plus OPTIONS, Warning, 380 response
Authentication	Negotiation plus 401 response, WWW-Authenticate, and Authorization headers

UA 는 전혀 모르는 호에 대한 ACK 메시지에 대해서는 조용히 버려지며 잘 모르는 URL 에 대한 요청은 "404 Not Found Response" 메시지를 받는다. UA 가 전혀 모르는 호에 대한 BYE 요청을 받으면 "481 Transaction Does Not Exist" 메시지를 보내며 한편 전혀 정보를 알 수 없는 호에 대해 응답하지 않고 조용히 버려진다. 만약 응답하면 정보 유출 가능성이 있기 때문에 조용히 버려지는 것은 보안상 필요하다.

표 1. 은 표준에 의해서 제공하는 UA 기능 구현에 따라 UA 종류가 Minimum, Basic, Redirection, Firewall friendly, Negotiation, Authentication 들로 구별된다. UA 는 지원되지 않는 요청에 대해서는 "501 Not Implemented" 메시지로 응답하여야 한다.

1.2.2 SIP 서버 (Server)

SIP 서버는 UA 로부터 SIP 요청을 받아 응답하는 응용 서버이며 SIP 서버 종류에는 프락시, 리다이렉트, 등록(Registration) 서버 등이 있다. SIP 서버는 UA 에게 서비스를 제공하기 때문에 TCP 와 UDP 모드를 제공하여야 한다.

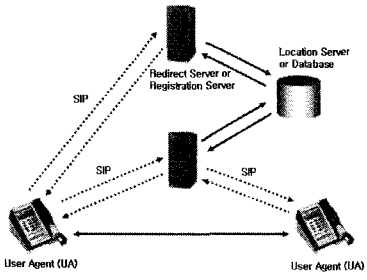

그림 2. SIP UA 및 Server
Fig. 2. SIP UA and Server

그림 2. 는 SIP UA, SIP 서버 및 위치 서비스의 상호 연관성을 나타내고 있다. SIP 프락시 서버는 UA 로부터 SIP 요청을 받고 이 요청 메시지를 포워딩(Forwarding) 또는 응답한다. SIP 프락시 서버는 데이터베이스를 엑세스하거나 다음 홉 주소를 알기 위해서 위치 정보 서비스(Location Service)를 받는다. SIP 프락시 서버와 위치 정보 서비스와의 인터페이스는 SIP 프로토콜에 의해서 정의되지 않는다. 따라서 SIP 프락시 서버는 UA 에게 사용자 위치 서비스를 제공하며 SIP 의 동작에 의해서 프락시 서버를 구별한다.

1.2.3 SIP의 동작

SIP 동작에서 SIP 서버는 들어오는 요청을 처리하는 방법에 있어서 프락시 모드(mode)와 리다이렉트 모드로 나눌 수 있다. 먼저 그림 3. 의 프락시 모드에서의 SIP 동작을 살펴보면, 프락시 서버는 INVITE 요청을 받아 그 요청의 주소를 보고 로케이션 서버에 접속하여 수신자의 정확한 위치정보를 얻는다. 그리고 프락시 서버는 로케이션 서버에서 받은 주소로 SIP요청을 보내고, 요청을 받은 UAS 는 수신자에게 INVITE 메시지가 왔음을 알리고 프락시 서버에게 메시지를 잘 받았다는 응답을 보낸다. 그러면, 프락시 서버는 UAC 에게 OK 응답을 보내고, UAC 는 프락시 서버에게 ACK 메시지를 보내며 프락시 서버는 UAS 에게 ACK를 포워딩함으로써 메시지 전송이 성공적으로 이루어졌음을 확인한다. 여기서 ACK 는 프락시 서버를 거치지 않고 수신자에게 직접 보내질 수도 있다.

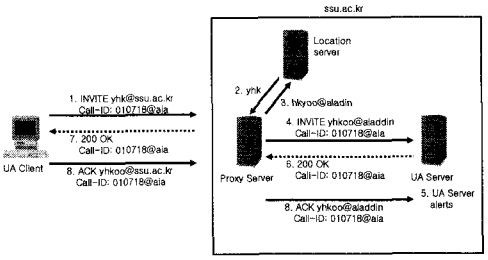

그림 3. 프락시 모드에서 SIP 동작
Fig. 3. SIP operation on the proxy mode

리다이렉트 모드에서 SIP 동작은 그림 4. 와 같이 이루어지는데 리다이렉트 서버는 INVITE 요청을 받아 프락시 서버처럼 요청의 주소를 보고 로케이션 서버에 접속하여 수신자의 정확한 위치정보를 얻는다. 리다이렉트 서버는 새로 얻어진 주소로 수신자와 연결을 시도하지 않고 UAC 에게 그 주소를 되돌려 주면, UAC 가 서버에게서 되돌려 받은 주소로 새로운 요청을 보낸다. 그리고 호가 성공적으로 이루어지면 UAC 와 UAS 는 ACK 를 주고받는다.

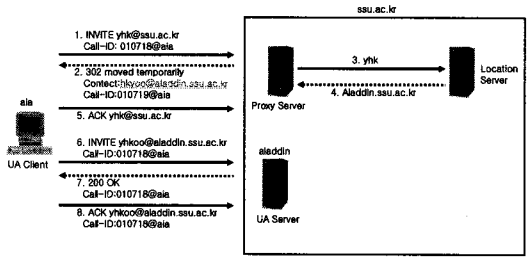

그림 4. 리다이렉트 모드에서 SIP 동작
Fig. 4. SIP operation on the redirect mode

1.3 SIP 보안 메커니즘

1.3.1 SIP 보안 메커니즘의 적용 영역

SIP 는 기본적으로 시스널링을 위한 프로토콜로서 인터넷을 이용한 원격회의, 인터넷 전화, 인스턴트 메시지 등의 서비스에 적용할 수 있다. SIP 보안 기술은 크게 Hop-by-Hop 보안과 End-to-End 보안 기술로 분류될 수 있으며, Hop-by-Hop 보안에는 digest 인증, TLS, IPSec 등의 기술이 포함되며, End-to-End 보안은 S/MIME 을 적용할 수 있다. SIP 를 이용한 VoIP 시스템에서는 실제 음성 데이터를 보호하기 위해서 RTP 페이로드를 암호화하여 기밀성을 제공할 수 있는 SRTP 를 이용하여 보안 서비스를 제공할 수 있다. 이와 같은 보안 메커니즘은 어플리케이션과 환경에 따라 선택적으로 사용할 수 있고, 이를 통해 시그널링 메시지에 대한 기밀성, 무결성, 인증을 제공하고 있다. 그림 5. 에서는 전체적인 SIP 보안 기술의 적용 영역을 보여주고 있으며 () 안의 보안 기술은 선택적으로 적용할 수 있는 영역을 나타내 주고 있다. 현재 TLS 와 digest 인증은 기술적으로 적용해야 할 보안 기술이며, 종단간의 보안을 지원하는 S/MIME 이나 IPSec 은 사용자의 선택에 따라 선택적으로 적용할 수 있다. SRTP는 미디어 보안을 위하여 선택적으로 적용할 수 있다.

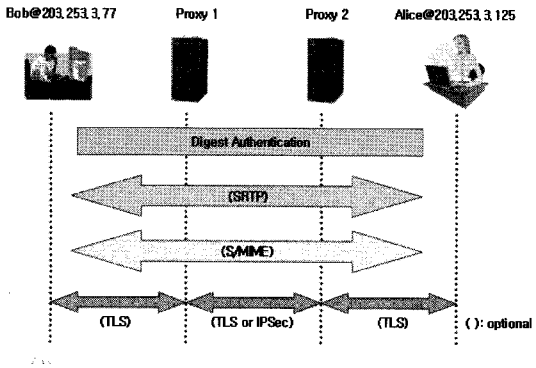

그림 5. SIP 보안 기술의 적용 영역
Fig. 5. An area effected by SIP security technologies

1.3.2 SIP 보안 메커니즘의 협상 절차

SIP 에서는 여러 보안 기술의 지원으로 확장성과 유연성을 가지고 있으나 이를 위해서는 기본적으로 각 노드들 간에 보안을 위한 협상 절차가 필요하다. 그림 6. 은 RFC 3329 (Security mechanism Agreement for Session Initiation Protocol(SIP)) 에서의 협상절차를 나타낸 것이다. 이 방법에서는 SIP 메시지에 보안 협상을 위한 헤더를 정의하고 이를 통해서 상대방과의 보안 협상을 하게 되며, SIP 메시지인 INVITE, REGISTER, OPTIONS 등의 메시지를 적용할 수 있다.

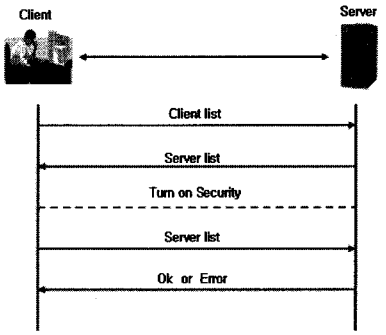

그림 6. SIP 보안 협상 절차
Fig. 6. The SIP security co-operation procedure

1.4 홈 네트워킹

홈 네트워킹은 PC, 이동전화, 디지털 TV, 개인정보단말(PDA), 게임기 등 가정내의 정보 기기간에 네트워크를 구축하여 디지털 데이터를 공유하고 광대역 통신을 사용하는 것을 말한다. 넓은 의미에서는 유무선 네트워크 장비뿐 아니라 정보기기 사이의 통합과 운영을 위한 소프트웨어와 서비스등을 포함한다.

홈 네트워킹의 기본 구조는 내부와 외부 네트워크를 연결하는 홈 게이트웨이, 전화선 · 전력선 · 무선 등 가정 내 통신망, 정보기기를 제어하며 상호 연동시키는 미들웨어, 홈 네트워킹 기능이 추가된 정보기기 등으로 구성된다. 홈 네트워킹 기술은 크게 유선과 무선으로 나눌 수 있으며, 유선기술로는 전화선, 전력선, 이더넷, IEEE1394, USB등이 있고, 무선에는 IEEE802.11x 계열의 무선 LAN, HomeRF, Bluetooth, UltraWideBand(UWB), Zigbee, HiperLAN 등이 대표적인 기술이다.

아직까지는 IEEE1394 프로토콜을 이용한 방식이 개발방향을 주도하고 있으며 가전기기의 연동 표준화 방식으로 자

리 잡고 있으나, 장기적으로 볼 때 이동단말 기기의 확산에 따른 무선 네트워크 솔루션이 부각됨에 따라 홈 네트워크에서의 적용도 확대될 것으로 보인다.

III. 본 론

1. 제안하는 서비스 모델 및 보안 메커니즘

1.1 Client-to-Client 서비스 모델

홈 네트워크 환경은 홈 클러스터가 내부 노드들과 외부 노드들의 참여와 인증 및 제어하는 역할을 수행한다. 홈 클러스터는 CA 로부터 발급된 인증서를 통한 내 외부 노드들의 제어까지 모든 것을 수행한다. 따라서 게이트웨이에 기반한 Cluster-to-Cluster 네트워크 환경은 홈 클러스터를 중심으로 홈 클러스터가 하나의 클러스터로 설계되었다. 그림 7. 에서 각 홈 네트워크가 홈 클러스터를 중심으로 제안된 두 개 이상의 네트워크인 Cluster-to-Cluster 서비스 모델을 제안하였다.

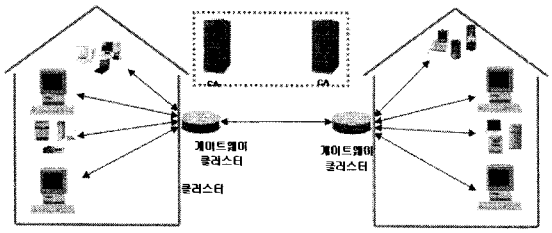

그림 7. Cluster-to-Cluster 서비스 모델 보안 협상 절차
Fig. 7. The security co-operation procedure of the Cluster-to-Cluster service model

그림 7. 에서와 같은 Cluster-to-Cluster 서비스 모델은 게이트웨이 클러스터가 CA(Certificate Authority)의 관리하에 동작한다. Cluster-to-Cluster 환경은 게이트웨이 클러스터가 타 네트워크의 게이트웨이 클러스터와의 세션 연결을 통하여 인증 및 단말을 제어하고, CA 는 게이트웨이 클러스터 사이에서 인증서를 발급하고 공개키 및 개인키를 발급하는 역할을 수행한다. CA 가 발급하는 인증서는 X.509 를 사용한다. [표 2]은 Cluster-to-Cluster 환경에서 각 구성요소와 역할에 대하여 설명하고 있다.

Cluster-to-Cluster 환경에서 각각의 클러스터 네트워크는 각각의 영역에 CA 를 가지고 있으며, CA 는 다수의 클러스터 네트워크의 게이트웨이 클러스터에 CA 가 가지고 있는 클러스터 네트워크 정보를 갱신한다. 두 개의 게이트웨이 네트워크가 서로 통신을 할 때, 게이트웨이 네트워크는 각각 다른 CA 를 가지고 있을 수 있으며, 게이트웨이 클러스터는 CA 가 가지고 있는 게이트웨이 네트워크 정보를 받아 외부에서 현재 속해 있는 네트워크의 단말을 인증 할 수 있다.

표 2. Cluster-to-Cluster 환경의 구성요소 및 역할
Table 2. The components and functions of the Cluster-to-Cluster environment

구성 요소	역할
게이트웨이 클러스터	게이트웨이 네트워크 간 인증 및 단말 제어
CA	공개키 인증 및 개인키 인증
단말	게이트웨이 클러스터가 관리하는 장치
인증서	X.509

1.1 제안하는 SSIP 프로토콜

SSIP(Secure Session Initiate protocol)은 기존의 클러스터 네트워크에서 사용되고 있는 SSL 프로토콜에 SIP 의 인증기능을 추가하여 효과적인 인증과 신뢰성 및 세션 설정시에 세션 시간 및 셋업 시간을 줄임으로써 효과적인 보안을 위하여 제안된 프로토콜이다. 예를 들어 자신의 클러스터 네트워크를 떠나 타 네트워크에서 필요한 정보나 데이터를 송수신하고자 할 때, 매번 인증을 시도 한다면 인증에 대하여 신뢰하지 못할 뿐 아니라, 세션을 재설정할 때 매번 인증서를 생성해야 하는 시간 낭비를 초래할 것이다. 그러나 SSIP 를 사용하면 이와 같은 문제점을 해결할 수 있을 것이다. 이러한 응용은 SSIP 가 동작하는 클러스터 네트워크에서의 응용으로 실시간 인증 서비스 모델의 변화에도 쉽게 적용할 수 있다.

SSIP 에서는 공통적으로 SIP 를 통한 인증이 수행된다. SIP를 이용한 인증이 끝나고 나면 SSL 를 이용한 인증서 교환 부분과, 세션 재설정 시 SSL 인증서 재사용 부분으로 나뉜다.

SSIP 는 클러스터 네트워크 환경에서 클러스터를 중심으로 설계된 프로토콜이다. SSIP 는 클러스터 네트워크에서 노드와 게이트웨이 클러스터 간의 통신을 위한 세션을 위하여 설계되었다. 게이트웨이 클러스터에서 게이트웨이 클러스터는 외부 네트워크와 게이트웨이 네트워크 사이와 내부의 단말들을 제어하는 기능을 가지고 있기 때문에 게이트웨이 클러스터 간의 보안이 가장 중요하다고 인식 하였고, 게이트웨이 클러스터는 보안적으로 안전하다고 가정하였다.

1.2 SSIP 프로토콜의 구성

SSIP 는 SIP 를 통한 인증 부분과 SSL 인증서 교환 부분, SSL 인증 세션을 마치는 부분과 멀티미디어 및 데이터

전송 부분 그리고 SIP 와 SSL 세션을 모두 끝내는 총 4가지의 부분으로 구성되어 있다.

SSIP에서 사용하는 제어 메시지는 [표 3]에서 나타난 것과 같이 5가지의 메시지가 추가되었다. Invite_Clinet 제어 메시지는 클라이언트가 처음 SIP 세션을 시작할 때 SSL 의 인증서를 사용한다는 신호 메시지와 SSL 의 사용이 가능함을 나타내고, Ringing_Server 메시지는 서버에서 SSL 인증서를 사용하여 세션을 맺을 수 있다는 허가를 의미한다. Ack_Permit 제어 메시지는 SIP 를 통한 인증을 마치고 클라이언트와 서버 사이에 이전에 사용되었던 인증서를 모두 검증한 후, 같은 인증서를 가지고 있다면 재사용에 동의할 때 사용한다. 만약 거부하면 Ack_Deny 메시지를 통하여 SSL 인증서 발급 절차를 다시 거치게 된다. Bye 메시지는 SSL 과 SIP 세션이 모두 종료됨을 나타낸다.

표 3. SSIP 제어 메시지
Table 3. SSIP control message

메시지	설명
Invite_Client	SIP의 세션을 시작할 때
Ringing_Server	서버에서 응답을 보낼 때
Ack_Permit	인증서 재사용에 동의 할 때
Ack_Deny	인증서 재사용에 동의하지 않을 때
200 OK	SSL과 SIP의 세션을 끝낼 때

1.3 SSIP 프로토콜의 동작

총 네 개의 부분으로 이루어진 SSIP 프로토콜은 우선 Invite_Client 메시지와 Ringing_Server 메시지를 통하여 SIP 인증과 함께 세션이 시작된다. SSIP 프로토콜은 기존 SSL 의 기능에 SIP 인증 세션을 추가하여 설계한 프로토콜이다. SSIP 는 SIP 의 세션연결을 시작함과 동시에 클라이언트와 서버는 SSL 인증서 발급 여부를 확인한다. 서로에 대한 식별이 끝나면 두 가지 경우의 세션 설정 경로가 발생할 수 있다. 첫 번째는 세션 설정 시 클라이언트와 서버가 이전 세션 연결을 사용한 적이 없거나, 인증서가 불일치하는 경우, 혹은 새롭게 세션을 설정해야 할 때이다. 그림 8. 와 같이 SSL 인증 교환 부분에서 Ack_Permit 메시지를 수신 받으면 인증서의 재사용에 동의하거나 Ack_Deny 메시지를 수신 받으면 인증서를 받거나, 갱신하는 절차를 수행한다.

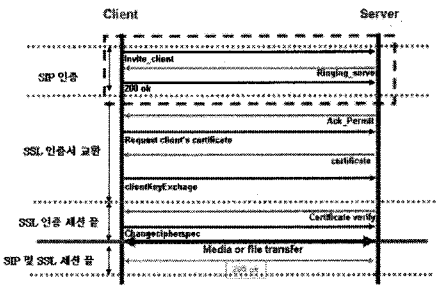

그림 8. SSIP 기본 동작
Fig. 8. SIP UA with

1.3.1 전체 동작 개요

① 클라이언트는 세션 설정을 위하여 Invite_Client 메시지를 서버에게 보낸다. 메시지에는 나중에 사용될 SSL 인증서의 종류 및 사용가능 여부들의 요소들이 포함되어 있다.

② 서버는 세션 설정을 맺기 위해 Ringing_server 메시지를 클라이언트에게 보낸다.

③ 클라이언트는 200 ok 메시지를 통해 서버를 확인한다.

④ 서버는 Ack_Permit 혹은 Ack_Deny 메시지를 통해 인증서의 가용 여부를 클라이언트에게 보낸다.

⑤ 클라이언트와 서버는 서로 인증서 및 키를 주고받는다.

⑥ 서버는 인증서를 확인하여 클라이언트에게 보내고 클라이언트는 cipherspec 을 교환한다.

⑦ 서버와 클라이언트는 통신 세션이 설정되고 통신이 이루어진다.

⑧ 통신을 마친 서버와 클라이언트는 200 ok 메시지를 통해 세션을 마친다.

1.3.2 세션 재설정(인증서를 가지고 있지 않을 경우)

그림 9. 은 SSIP 동작 중 인증서를 가지고 있지 않은 경우에 대한 그림이다. 클라이언트와 서버는 SIP 인증을 시작한 후 SSL 인증을 거친 후 SIP 및 SSL 세션을 200 ok 메시지로 세션을 종료한다. 이 과정은 그림 8. 의 SSIP 의 기본 동작과 유사한 과정을 거친다. 그러나 SSIP 의 기본적인 동작과 다른 점은 인증서를 발급하기 전에 Ack_Permit 이나 Ack_Deny 메시지를 보내지 않고 Ack 메시지를 통하여 인증서를 요청하는 과정이 SSIP 기본 동작과 다르다.

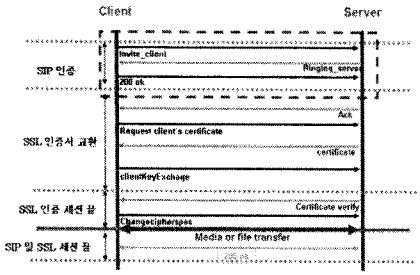

그림 9. SSIP 동작 중 인증서를 가지고 있지 않을 경우
Fig. 9. SSIP operation without an authentication

1.3.3 세션 재설정(인증서를 가지고 있을 경우)

그림 10. 은 SSIP 동작 중 인증서의 재사용이 가능한 경우에 대한 그림이다. SIP 인증 세션을 통하여 이전에 클라이언트에서 사용했던 인증서와 서버의 인증서가 일치함을 확인하면 서버는 클라이언트에게 Ack_Permit 메시지를 통하여 인증서의 재사용을 허가하게 된다. 그러면 클라이언트는 SSL 인증서를 사용하여 세션을 믿을 수 있다는 허가를 의미한다. 서버는 SSL 인증서를 확인하는 Certificate verify 메시지를 보낸다. 서버는 클라이언트에게 cipherspec 을 보내면 세션은 설정되고 통신이 이루어진다. 통신이 끝나면 200 ok 메시지를 통해 세션을 마친다.

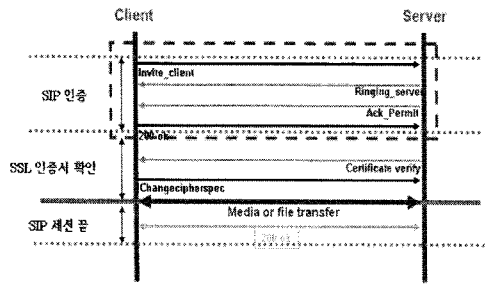

그림 10. SSIP 동작 중 인증서의 재사용이 가능한 경우
Fig. 10. SSIP operation with reusability of an authentication

1.4 SSIP 프로토콜을 적용한 Cluster-to-Cluster 보안 메커니즘

1.4.1 통신하는 단말 및 게이트웨이 클러스터가 동일한 CA 영역에 있을 때

단말이 하나의 클러스터 네트워크에 속해 있을 경우에는 CA 와 게이트웨이 클러스터 간에 발생하는 이벤트가 크지 않다. 이 경우 게이트웨이 클러스터는 단말을 인증하고 있는 상태이고, 게이트웨이 클러스터는 자신이 속한 CA 에게 이미 인증을 받은 상태이다. 게이트웨이 클러스터가 단말을 인증하는 것만으로 게이트웨이 네트워크간 통신이 가능하다. 그림 11. 는 동일한 CA 를 가지고 네트워크 간 통신에 대한 설명을 하고 있다.

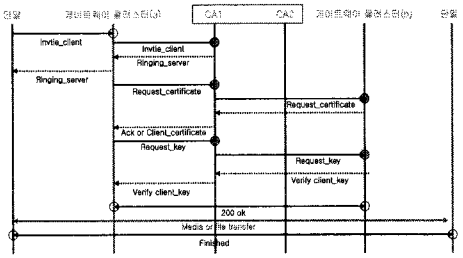

그림 11. 동일한 CA 를 가지고 있는 경우
Fig. 11. a node known as having a identical CA

① 단말은 (게이트웨이 클러스터(a): 이하 a)와 세션 설정을 위해 Invite_Client 메시지를 보낸다.

② (a) 는 CA1 로부터 (a)를 인증 받기 위한 세션 설정을 위해 Invite_Client 메시지를 보낸다.

③ CA1 는 자신이 (a)를 관리하는 CA 임을 확인하기 위하여 Ringing_server 메시지를 보낸다.

④ (a)가 단말을 인증함을 확인하기 위한 절차를 수행하기 위하여 (a)는 Ringing_server 메시지를 보낸다.

⑤ (a)는 CA1 로부터 인증을 받기위해 Request_certificate 메시지를 통해 인증서를 요청한다.

⑥ CA1 은 (a)의 인증서를 확인하고, 요청 받은 (a)가 통신을 원하는 (홈 클러스터(b): 이하 b)가 자신이 관리하는 게이트웨이 클러스터인지를 확인하고 (b)에게 인증서를 요청한다.

⑦ (b)가 자신이 관리하는 영역에 있는 것을 확인한 CA1 은 (b)에게 (a)로부터 받은 자신의 인증서를 확인하고 Client_certificate 메시지를 통해 인증서를 전송한다.

⑧ CA1 는 (b)의 인증서를 확인하고 (a)에게 인증서를 전송한다.

⑨ (a)는 Request_Key 메시지를 통해 키를 요청하고, CA1은 (a)의 키를 확인한다.

⑩ CA1 은 Request_key 메시지를 통해 키를 요청하고, CA 는 (b)의 키를 확인한다.

⑪ 서로 인증을 마친 (a)와 (b)는 세션을 설립하고 CA 를 통해 200 ok 메시지를 보낸다.

⑫ 단말간에 통신 세션이 설립되고, 통신이 이루어진다.

⑬ 통신이 끝나고 난 후, Finished 메시지를 통해 세션은 닫히고, 통신이 끝났음을 알린다.

1.4.1 통신하는 단말 및 홈 클러스터가 다른 CA 영역에 있을 때

① 단말은 (a)에 세션설정을 위한 Invite_Client 메시지를 보낸다.

② CA1 로부터 (a)를 인증 받기 위하여 (a)는 CA1 에게 Invite_Client 메시지를 보낸다.

③ 자신이 관리하는 CA 임을 확인하기 위하여 CA 는 Ringing_server 메시지를 보낸다.

④ (a)가 단말을 인증함을 확인하기 위한 절차를 수행하기 위하여 (a)는 Ringing_server 메시지를 보낸다.

⑤ (a) 는 CA1 으로부터 인증을 받기 위하여 Request_certificate 메시지를 통해 CA1 에게 인증서를 요청한다.

⑥ CA1 은 자신이 (b)의 정보를 검색한 후 자신이 관리하는 네트워크가 아님을 확인하고 단말에게서 얻은 정보를 가지고 CA2 를 검색한 후 CA2 에 Request_certificate 메시지를 통해 인증서를 요청한다.

⑦ CA2 는 인증서를 확인하고 (b)에게 인증서를 요청한다.

⑧ (b) 는 (a)가 통신을 원하는 대상임을 확인하고 인증서를 확인한 후, CA2 에게 Response_certificate 메시지를 통해 응답을 한다.

⑨ CA2 는 CA1 에게 응답을 보내어 인증서를 확인하고, CA1 은 (a)에게 인증서를 확인하는 메시지를 보낸다.

⑩ CA1 과 CA2 는 서로 (a)가 통신을 원하는 대상이 (b)임을 확인하고 서로 200 ok 메시지를 통해 상대를 확인한다.

⑪ (a) 는 Request_Key 메시지를 통해 키를 전송하고, CA1 는 (a)의 키를 확인한다.

⑫ (a) 는 CA1, CA1 은 CA2 에게 키를 전송하고, CA2 는 (b)에게 키를 전송한다.

⑬ (b)는 CA2 의 키를 확인하고, CA1 은 CA2의 키를 확인하며, CA1 은 (a)의 키를 확인한다.

⑭ (a) 와 (b) 는 CA1 과 CA2 를 거친 안정된 세션임을 확인하며, 200 ok 메시지를 통해 상대를 확인한다.

⑮ 단말은 (a) 를 통해 상대방 클러스터 네트워크에 있는 (b)를 연결하여 (b)에 속해 있는 단말과 통신을 하게 된다. 통신이 끝난 후에 finished 메시지를 통해 세션이 끝났음을 알린다.

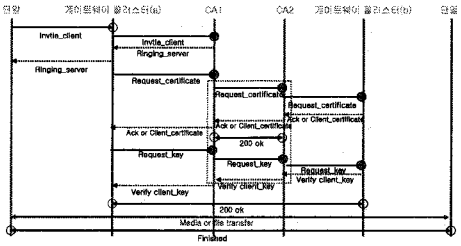

그림 12. 다른 CA를 가지고 있는 경우
Fig. 12. a node known as having a different CA

1.5 성능 평가 결과

제안한 SSIP 프로토콜 및 메커니즘에서 SSIP에 대한 성능 분석을 실시한다. 성능분석을 통해 SSIP를 사용하면 클러스터 네트워크 환경인 Cluster-to-Cluster 환경에서 SSL〈PKI〈SIP 과 같은 프로토콜을 사용한 클러스터 네트워크 환경보다 노드의 수가 증가 되더라도, 예전보다 인증 비용에 있어 더 효과적이라는 것을 확인할 수 있다. 즉, SSIP 인증 절차를 SSL 보다 우수한 성능을 가진다는 것에 여러 가지 변수를 두어 이로 인해 발생하는 절차적 분석을 통해 본 논문에서 제안하는 SSIP 성능의 우수성을 증명한다.

1.5.1 보안 요구사항 분석

Cluster-to-Cluster 네트워크에서 외부, 내부 공격으로부터 안전하게 하기 위해서는 네 가지의 보안 요구사항을 만족시켜야 하는데 본 논문에서 제안하고 있는 Cluster-to-Cluster 네트워크에서 SSIP 를 적용한 메커니즘은 기밀성, 인증, 세션의 안전성을 만족한다. 즉, 인증서를 사용하고 SIP 를 통하여 상대를 인증하기 때문에 인증 및 세션의 안전성을 보장받을 수 있으며, 초기 세션 시 상대를 검증하기 때문에 기밀성 무결성을 보장할 수 있다.

본 논문에서 제안하고 있는 SSIP 프로토콜은 Cluster-to-Cluster 환경에서 보안적 요구사항 네 가지의 보안 요구사항을 만족시키기 위해 다음의 세 가지를 고려한다. 첫째 홈 클러스터는 DoS/DDoS 스푸핑 공격에 대한 취약성 보완을 위하여 단말 및 클러스터 간 보안성을 제공하므로 홈 클러스터 및 노드는 외부의 공격에 안전해야 한다. 둘째 세션을 재 설정 할 때마다 인증서를 생성하지 않아도 되기 때문에 프로토콜이 경량화 되었음을 보여야 하므로 홈 클러스터의 인증서 재사용이 가능해야 한다. 마지막으로 세션 프로세스를 처리하는 게이트웨이 클러스터가 인증서를 가지고 있으므로 세션 개설 요구에 대한 인증 오버헤드는 크게 증가하지 않아야 한다.

그림 13. 과 같이 PKI 은 동일 노드의 반복적인 세션 요구, 인증서의 재요구등과 같은 요건 설립 때문에 DoS 공격에 노출되어 있다. 또한 SSL 프로토콜은 초기 세션 설립 시 IP

및 세션 IP 노출, 키 교환 방법의 노출등과 같은 문제 때문에 스니핑 및 DoS 공격에 취약하다. 그러나 SSIP 는 인증서 사용, Ack, Nack 메시지를 통한 인증서의 재사용을 통하여 스니핑 및 DoS 공격에 대한 다른 프로토콜보다 효과적임을 증명한다.

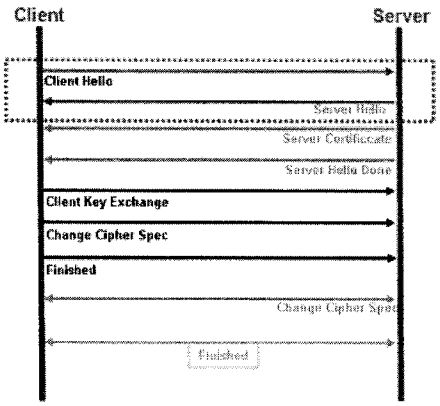

그림 13. PKI 및 SSL 보안 취약부분
Fig. 13. A security weakness part of PKI and SSL

표 4. 는 각 프로토콜의 보안 취약 부분인 초기 세션 설정 시 전송되는 요소를 통하여 SSIP 를 비교 하였다.

SSIP 가 가지고 있는 요소는 PKI 와 SSL 이 가지고 있는 요소들과 매우 유사하나, Ack, Nack 가 추가되어 있는 요소이다. 이것은 Ack 메시지를 수신할 때 동반하는 것으로 인증서의 재사용이 가능 하다면 Ack 요소가 포함되고, 인증서를 재사용 할 수 없으면 Nack 요소를 포함한다.

표 4. 각 프로토콜의 요소 비교
Table 4. The comparison between components of each protocol

프로토콜	초기 세션 설정 시 전송 되는 요소					
PKI	세션 ID	난수	Cipher suite	인증서		
SSL	세션 ID	난수	Cipher suite			
SSIP	세션 ID	난수	Cipher suite	인증서	Ack	Nack

1.5.2 성능 분석 모델

기존의 클러스터 네트워크 환경에서 SSL 을 사용한 모델과 우리가 제안하는 SSIP 를 사용한 Cluster-to-Cluster 환경에서의 적용 모델과 비교하기 위해서 그림 14. 와 같은 모델을 정의하였다.

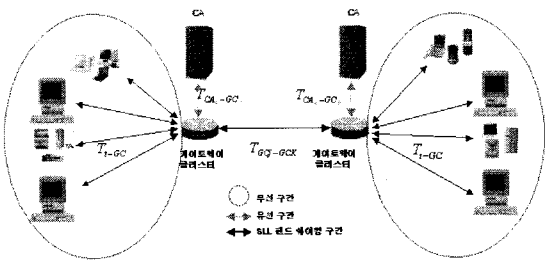

그림 14. PKI 및 SSL 보안 취약부분
Fig. 14. A security weakness part of PKI and SSL

본 논문의 성능 평가 기준은 다음과 같다. 첫 번째는 안전성 측면에서 제안한 SSIP 와 SSL 을 비교하여 효과적인 인증서를 사용하여 기존에 제안되었던 프로토콜보다 더 우수한 성능을 보이는 프로토콜임을 증명하는 것이다. 두 번째는 세션 시간 측면에서 제안한 SSIP 와 PKI 를 비교하여 PKI 보다 세션 처리 시간 및 비용에서 효과적임을 보인다.

다음 표 5. 은 성능 평가에 사용되는 변수들에 대한 설명을 나타낸 것이다.

표 5. 성능 평가에 사용되는 변수
Table 5. The variables used in performance evaluation

변수	설명
$Cost$	N 개의 노드들간 통신하기 위한 전체 통신 시간
$C_{session}$	총 세션 비용
C_{auth}	총 인증 비용
T_{tHG}	단말에서 게이트웨이 클러스터 까지의 전송 비용
T_{CAj-HG_j}	CA 와 게이트웨이 클러스터 사이의 전송 비용
T_{CAk-HG_k}	CA 와 게이트웨이 클러스터 사이의 전송 비용
T_{HGj-HG_k}	게이트웨이 클러스터간 SSL 세션 연결 시간
P_{HG}	게이트웨이 클러스터에서의 인증서 유무 확인 처리시간
P_{CA}	CA에서 인증을 처리하기 위한 시간
$P(i)$	n 개의 노드들 중 i 개의 노드가 인증서를 가지고 있지 않을 확률

표 5. 은 성능 비교, 분석을 효과적으로 하기 위해 시나리오를 바탕으로 총 세션 비용을 산출하기 위하여 다음과 같이 정의 하였다. 본 성능 평가 모델에서의 총 비용 값을 산출하기 위해 아래와 같은 요소를 정의하였다. 논 논문의 비용 분석을 위하여 수식(1) 에서의 같이 총 비용 (C) 은 $C_{session} + C_{auth}$ 값을 더한 비용이다.

C ..... 수식(1)

$C_{session}$ 값은 홈 클러스터 간에 세션 설립 비용값인 C_{GG} 값과 홈 클러스터와 단말간의 세션 설립 비용인 C_{CN} , C_r 값으로 나누어진다.

수식(2) 에서처럼 $C_{session}$ 값은 다음과 같다. 또한 C_{auth} 값은 CA 가 게이트웨이 클러스터를 인증하는데 드는 비용에 대하여 설명하고 있다.

$$C_{session} = C_{HGj-HGk} + C_{t-HG} + C_r$$

..... 수식(2)

본 성능 모델의 각 객체들의 세션 값을 살펴보면, 수식(2)와 같으며 게이트웨이 클러스터간의 비용과 게이트웨이 클러스터가 단말 간의 세션시 비용과 세션 설립 시 처리 비용의 합으로 나타낼 수 있다. 그림 14. 의 모델에서 살펴보면, 게이트웨이 클러스터 간 비용은 $T_{HGj-HGk}$ 로 정의 되며, 게이트웨이 클러스터가 인증을 위한 값은 P_{HG} 로 나타내었다.

$$C_{auth} = C_{CA} + C_{HG}$$ ..... 수식(3)

SSIP 프로토콜은 세션과 인증이 같이 일어나므로 세션값만으로는 성능 평가를 수행 할 수 없다. 수식(3)은 인증에 대한 비용에 대하여 수식으로 나타낸 것이다. C_{auth} 값은 노드 및 게이트웨이 클러스터 및 CA 가 인증할 때 드는 처리 비용(C_{CA}) 값과 인증서 및 키 값을 전송하는 값(C_{HG}) 을 합한 값이다.

(1) 성능 분석 모델의 세션 비용 및 인증 비용

Cluster-to-Cluster 환경에서 SSIP 을 사용한 절차는 세션값과 인증값을 사용하여 다음과 같은 값을 가진다. 각 구간에 대한 시간은 총 4 개의 단계로 나누어 볼 수 있으며, 인증, 유선, 무선, SSL, 핸드쉐이킹 구간의 각 시간은 표 6. 과 같다.

표 6. 각 구간 시간
Table 6. Time at each section

구 간	시 간
PKI 인증	1.414 sec (1)
무선 구간의 인증	0.34 ms(2)
유선 구간의 인증	4.01 ms(3)
SSL 핸드쉐이킹	0.9 ms(4)

$C_{session}$ 값은 성능 분석 모델에서 세션이 일어나면서 발생하는 비용을 계산한 값으로써, 게이트웨이 클러스터와 단말간에는 2번의 a 와 b 의 비용이 든다. 게이트웨이 클러스터와 게이트웨이 클러스터 간의 비용은 인증서 및 키를 위한 세션이 일어나므로 b 와 c 를 통한 세션설정이 발생한다. 실험 환경에 대한 확률과 계산식은 다음과 같다.

$$P(i) = \frac{i}{n}$$ ..... 수식(4)

$$\text{Total\_Cost} = n \times (2 \times T_{tHG} + P_{HG} + P(i) \times (T_{CAjHGj} + T_{CAkHGk} + T_{HGjHGk} + P_{CA}))$$

..... 수식(5)

수식(4)와 (5)에서 나타낸 것처럼 본 논문에서는 두 가지 형태의 메시지 교환에 따른 인증을 위한 비용 계산을 앞에서 말한 정의 값을 사용하여 성능분석을 하게 된다.

1.5.3 SSIP 성능 분석 결과

1.5.2 의 식을 기준으로 하여 표 7. 와 같은 실험 환경을 적용하였을 때의 결과를 보이고자 한다.

전체 네트워크를 100 개로 제한하고 노드 증가에 따른 인증 시간을 분석하였다. 그림 15. 은 100 개의 노드 중 20 개의 노드가 인증서를 가지고 있을 경우에 대한 설명을 나타낸 것이다.

전체 클러스터 네트워크의 노드를 100 개의 노드가 세션을 하나씩 연다고 가정하고 인증서를 가지고 있는 노드 수는 $\frac{a}{n}$ 로 계산하고 가지고 있지 않은 노드 수는 $\frac{a}{m}$ 로 각각 계산한다. 또한 유선, 무선 구간 시 정송 트래픽을 고려하여 성능평가를 실시하였다. 그림 15. 에서와 같이 SSIP 의 성능 결과는 PKI 보다는 전송시간이 적으며 SSL 전송시산과 근사한 값을 가진다.

표 7. 실험 파라미터들
Table 7. The examination parameters

파라미터	값
전체 네트워크 노드 수	100
인증서를 가지고 있는 노드 수	$\frac{a}{n}$
인증서를 가지고 있지 않은 노드 수	$\frac{a}{m}$

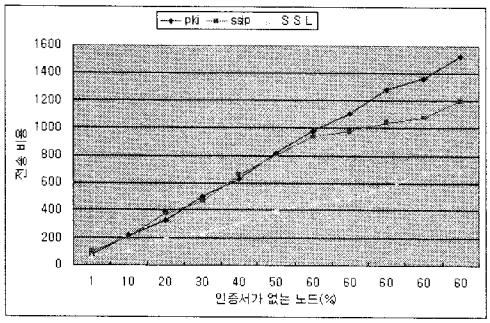

그림 15. 20개의 노드가 인증서를 가지고 있지 않은 경우
Fig. 15. 20 nodes without authentications

또한 60, 100 개의 노드가 인증서를 모두 가지고 있지 않을 때의 그래프는 그림 16. 과 그림 17.에서 처럼 SSL 보다 전송 시간이 더 걸리며 PKI 그래프로 근사됨을 확인할 수 있다.

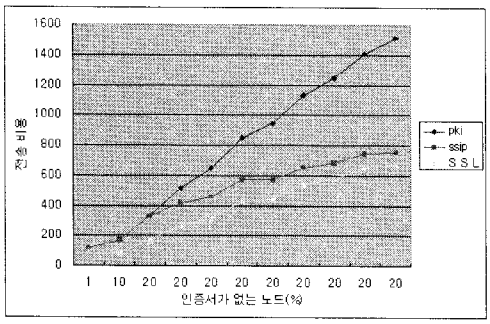

그림 16. 60개의 노드가 인증서를 가지고 있지 않은 경우
Fig. 16. 60 nodes without authentications

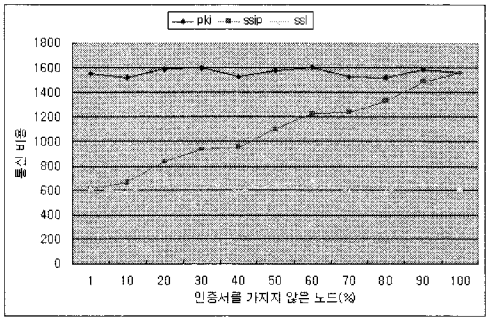

그림 17. 100개의 노드가 인증서를 가지고 있지 않은 경우
Fig. 17. 100 nodes without authentications

IV. 결 론

본 논문에서 제안한 SIP 기반에서의 홈 네트워크 보안 기술에 관한 연구를 수행하였다. 적용 모델의 사례로 Clustre-to-Cluster 네트워크 환경에서 SIP 를 적용한 클러스터 서비스 모델과 보안 프로토콜을 제안 하였다. 기존의 클러스터 네트워크에서 사용되고 있는 SSL 프로토콜에 SIP 의 인증 기능을 추가하여 효과적인 인증과 신뢰성 및 세션 재 설정 시에 세션 시간 및 셋업 시간을 줄임으로써 효과적인 보안을 위하여 새로운 SSIP 프로토콜을 제안 하였다. 세션 재 설정 시에 세션 시간 및 셋업 시간을 적게 하는 것이 해커로부터의 공격에도 적게 노출되므로 신뢰성 및 보안에 안전하다. 또한 세션 재설정 시 기존의 인증서를 가지고 있는 경우와 인증서를 가지고 있지 않을 경우로 나누어서 비교 분석 하였다. 자신의 홈네트워크를 떠나 타 홈 네트워크에서 필요한 정보나 데이터를 송,수신 하고자 할 때, 매번 인증을 시도 한다면 인증에 대하여 신뢰하지 못할 뿐 아니라, 세션을 제설정할 때 매번 인증서를 생성해야 하는 시간 낭비를 초래 할 것이다. 마지막으로 각각의 경우에 관한 성능 평가를 시뮬레이션 하여 분석하였다. 그 결과 노드가 인증서를 가지고 있는 경우 노드의 개수가 많아도 전송 시간이 적게 걸리고 노드의 개수가 적더라도 인증서를 가지고 있지 않은 경우는 전송시간이 더 걸리는 사실을 확인할 수 있었다.

그러므로 본 논문에서 제안한 기존의 인증서를 가지고 있는 경우 SSIP 프로토콜은 세션 시간 및 셋업 시간을 적게 하므로 효과적인 보안과 신뢰성을 가진다.

참고문헌

[1] M. Handy, H.Schulzrinne, J. Rosenberg, "SIP," RFC2543.

[2] Kundan Singh, Gautam Nair, Allard, "Centralized Confencing using SIP," hgs@cs.columbia.edu

[3] 정재학, "홈네트워크에서의 보안 요구사항," 한국정보보호학회, 제14권, 제5호, 19-22쪽, 2004년 10월.

[4] 김상춘, 권혁찬, 나재훈, "MITM공격에 안전한 P2P 신뢰전송 메커니즘의 설계," 한국정보보호학회, 제18권, 제4호, 103-109쪽, 2008년 8월.

[5] 한종욱, 김도우, 주홍일, 이윤경, 남택용, 장종수, "홈네트워크 보안 프레임워크 구축을 위한 고려사항," 한국정보과학회, 제22권, 제 9호, 17-23쪽, 2004년 9월

[6] 박성수, 박광로, 정혜원, "유무선 홈 네트워킹의 동향 및 응용," 한국정보과학회, 제19권, 제4호, 48-56쪽, 2001년 4월.

[7] 구민정, 오창석, "IPv6환경에서 DDoS 침입탐지," 한국컴퓨터정보학회, 제11권, 제6호, 185-192쪽, 2006년 12월.

[8] 정의현, "다중피어 결합을 이용한 P2P 멀티미디어 스트리밍 프로토콜," 한국컴퓨터정보학회, 제11권, 제2호, 253-261쪽, 2006년 5월.

[9] 박대우, 서정만, "TCP/IP 공격에 대한 보안 방법 연구," 한국컴퓨터정보학회, 제10권, 제5호, 237-244쪽, 2005년 11월.

[10] 김상춘, 권혁찬, 나재훈, "MITM공격에 안전한 P2P 신뢰전송 메커니즘의 설계," 한국정보보호학회, 제18권, 제4호, 103-109쪽, 2008년 8월.

[11] 한종욱, 장종수, 손승원, "홈네트워크 보안기술 동향," 한국정보과학회, 제19권, 제2호, 33-47쪽, 2005년 12월.

[12] 장동현, 장재철, 현종웅, 김태근, "홈네트워크 기술개발 동향 및 산업화 전략," 한국정보과학회, 제23권 제25호, 28-37쪽, 2005년 2월.

[13] 문경덕, 박광로, "유비쿼터스 홈을 위한 홈네트워크 표준화 및 토털솔루션 기술 개발," 한국정보과학회, 제22권, 제9호, 13-16쪽, 2004년 9월.

[14] 고훈, "홈네트워크 취약점 분석 및 인증 분석," 한국정보보호학회, 제1권, 제6호, 42-47쪽, 2006년 12월.

저 자 소 개

함 영 옥

1994년 : 서경대학교 전산통계학과 학사

1996년 : 광운대 전자계산학과 석사

2004년 : 숭실대학교 컴퓨터학부 박사과정 수료

관심분야 : 홈네트워킹, 멀티캐스팅

신 용 태

1985년 : 한양대학교 산업공학과 학사

1990년 : Univ. of Iowa 전산학과 석사

1994년 : Univ. of Iowa 전산학과 박사

1994년~1995년 : Michigan State Univ. 전산학과 객원교수

1995년~현재 : 숭실대학교 컴퓨터학부 교수

관심분야 : 멀티캐스팅, 실시간통신, 이동통신, DRM 등