비공개형 다자간 컨퍼런스의 보안성 확보를 위한 SIP 확장 기법

김현태* · 김형진* · 나인호*

A SIP Extension Method for Closed Multiparty Conference with Guarantee of Security

Hyun-tae Kim* · Hyoung-jin Kim* · In-ho Ra*

이 논문은 2003년도 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초기술 연구지원사업의 연구결과입니다.

요 약

VoIP(Voice over IP) 네트워크에서 제공되는 SIP(Session Initiation Protocol) 기반의 다자간 컨퍼런스(Multiparty Conference) 서비스는 점차 그 사용이 확대되고 있으며 계속적인 개발과 표준화 작업이 진행 중에 있다. 그러나 현재 사용 중인 SIP는 비공개형 다자간 컨퍼런스 서비스를 위해 필요한 공통의 제어 메커니즘 중에서 참가자 정보(identity)의 획득과 분배를 위한 기능을 제공하지 않고 있다. 본 논문은 SIP 기반의 다자간 컨퍼런스에서 보안성(security) 확보를 위한 SIP 확장 기법에 관한 연구로서 비공개형 다자간 컨퍼런스에서 호 설정이 이루어질 때 사용자의 정보를 획득하고 이것을 각 컨퍼런스 참가자들에게 분배하는 것이 가능하도록 하는 새로운 SIP 헤더와 메소드를 설계하여 새로운 참가자가 컨퍼런스에 참여하기 전에 이것이 다른 참여자에게 알려지는 것을 보장할 수 있도록 하였다.

ABSTRACT

Multiparty conference service based on SIP supported by VoIP network is gradually increased in use and the continuous development and standardization works on SIP are in the process of advancing. But SIP used in currently does not support identity discovery and distribution of each participant for multiparty conference. In this paper, a SIP extension method for guaranteeing security from the multiparty conference based on SIP is proposed. We design a new SIP header and method for discovering and distributing a participant's identity in closed multiparty conference when the call initiation is established. And it can ensure that each participant is notified before a new participant joins.

키워드

SIP, Multiparty Conference, SIP Extension, Security

Ⅰ. 서 론

ATM과 B-ISDN을 중심으로 한 초고속통신망과 같은 네트워크 인프라가 완성되어가면서 네트워크는 광대역의 멀티미디어 망으로의 단계를 넘어서 유·무선 네트워크 서비스를 제공하는 통합망으로 발전하고 있으며, 이와 함께 우리의 커뮤니케이션 방식도 많은 변화가 일어나고 있을 뿐만

* 군산대학교 전자정보공학부

접수일자 : 2003. 12. 26

아니라 이에 병행하여 사용자들의 다양한 요구를 수용하기 위한 응용 서비스들도 활발히 개발되고 있다.

VoIP(Voice over Internet Protocol)가 제공하는 다자간 컨퍼런스(Multiparty Conference) 서비스는 사용자간의 편리한 커뮤니케이션 환경을 제공할 수 있으며 다양한 응용솔루션과 각종 부가서비스 개발을 통해 발전 가능성이 매우 높은 서비스로 평가되고 있다. 이러한 서비스를 위한 표준 호 설정 프로토콜로서 H.323과 SIP가 사용되고 있다. 과거에는 H.323을 기반으로 하는 다양한 서비스들이 주로 개발되었으나 최근 H.323의 복잡성을 보완할 수 있고 여러 가지 장점들을 지닌 특징으로 인하여 SIP는 차세대 VoIP 표준 프로토콜로 자리잡고 있다[2].

SIP를 기반으로 한 다자간 컨퍼런스와 관련하여 진행 중인 여러 가지 표준화 작업 중에서 보안성(security) 제공을 위한 표준화 작업은 신속히 해결되어야 할 중요한 문제로서 현재 이를 위한 다양한 논의가 진행되고 있다. 다자간 컨퍼런스의 보안성 확보에 있어서 사용자 정보(identity)를 획득하고, 이를 각 사용자들에게 분배하는 기능은 매우 중요한 부분으로 인식되고 있으나 현재 SIP는 다자간 컨퍼런스에서 사용자 정보의 획득과 분배를 위한 기능을 제공하지 않고 있다. 이러한 점은 SIP를 기반으로 하는 비공개형(closed) 다자간 컨퍼런스에서 더 큰 문제점으로 나타나게 된다[3][4].

본 논문은 차세대 VoIP 표준기술로서 주목받고 있는 SIP를 기반으로 하는 비공개형 다자간 컨퍼런스에서 컨퍼런스 보안성 확보를 위한 SIP 확장 메커니즘에 관련된 연구로서 새로운 SIP 헤더와 메소드를 설계 및 구현하여 그것의 동작과 성능을 분석하였다.

본 논문의 구성은 다음과 같다. II장에서는 관련 연구를 통해 현재 SIP의 특징과 SIP에서 사용되는 메시지들의 동작을 기술하였다. III장에서는 비공개형 다자간 컨퍼런스의 보안성 확보를 위한 SIP 확장과 구성을 소개하고, IV장에서는 SIP 확장의 동작과 성능 평가를 하였다. 마지막으로 V장에서 결론을 맺는다.

II. 관련연구

2.1 SIP

SIP는 단말간 또는 사용자들 간에 기존의 VoIP 서비스뿐만 아니라 다양한 서비스의 호 설정(call signaling) 프로토콜로서 사용자간의 멀티미디어 세션에 대한 세션간의 변경, 초기화 및 종료를 정의한 응용계층의 프로토콜이다. SIP는 단순하게 세션 설정만을 다루는 프로토콜로서 간단하면서도 여러 다른 프로토콜들과 함께 사용될 수 있는 확장 가능한 프로토콜이며, 다양하고 넓은 범위에서의 응용 서비스에 활용될 수 있도록 확장이 진행되고 있다[5]. SIP는 기존의 텍스트 기반 인터넷 표준들에 기반을 두고 설계되었다. SIP는 클라이언트/서버 구조에 기반을 두고 있으며, URL (Uniform Resource Location) 사용 방식을 이용하는 프로토콜이다. TCP, UDP, ATM 등의 하위 레벨의 트랜스포트 프로토콜과 독립적으로 동작하도록 설계되었다[6].

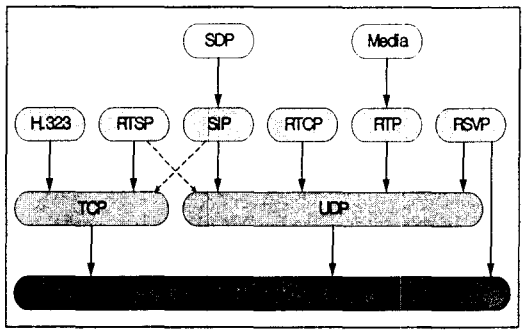


그림 1. Internet Telephony 프로토콜
Fig. 1 Internet Telephony Protocol

그림 1은 VoIP에서 사용되는 프로토콜들과 SIP의 위치를 보이고 있다.

2.2 SIP 메시지

SIP 메시지는 헤더(header)와 메시지 바디(message body)로 구성되며 헤더에는 SIP 제어정보가 포함되어 있다. 메시지 바디는 SDP(Session Description Protocol)로 기술되어 호 설정시 음성 및 비디오 코덱과 같은 양측의 기능과 처리능력을 조정하기 위한 정보를 나타낸다[7]. 그림 2는 SIP

메시지의 종류와 포맷을 나타낸 것이다.

2.2.1 헤더 영역

- General Header : Request/Response 메시지에 모두 사용된다.
- Entity Header : 메시지의 기타 정보를 나타내거나 전송되는 데이터가 없을 때에는 Request 메시지에서 지정한 해당 자원에 대 한 정보를 알려줄 때 사용된다.

그림 2는 SIP 메시지의 구조를 보이고 있다.

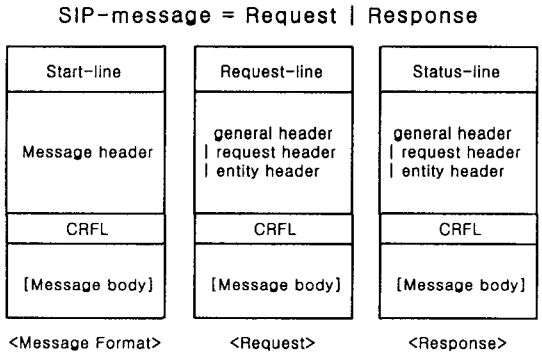


그림 2. SIP 메시지 구조
Fig. 2 SIP message architecture

2.2.2 Request 메시지

현재 SIP 2.0에는 6가지의 메시지가 사용되고 있고 이것들은 메소드(method)로서 처리되며, 기능에 따라 다음과 같이 분류된다.

- INVITE : UA(User Agent)들 간의 미디어 세션을 설립할 때 사용된다.
- ACK : INVITE에 대한 최종 응답의 확인에 사용된다.
- BYE : 설립된 미디어 세션을 종료하기 위해 사용된다.
- CANCEL : 진행 중인 요청을 취소하는데 사용되며 이미 완료된 경우에는 영향을 주지 않는다.
- OPTIONS : 통신 능력에 대한 정보를 요구하는데 사용되며, 연결 설정 시에는 관여하지 않는다.
- REGISTER : 사용자 위치에 대한 정보를 SIP 서버에게 전달한다.

2.2.3 Response 메시지

SIP Response 메시지는 UAC(User Agent Clent)의 요청에 대한 응답으로 Response 메시지는 각각의 상태코드(Status Code)로 구분되며 6개의 응답 클래스가 존재한다. 표 1은 SIP Response의 클래스들과 코드들을 보인 것이다.

표 1. SIP Response 코드와 클래스
Table. 1 SIP Response Code and Class

Response Code	Class	Status
1XX	Informational Messages	Provisional
2XX	Success Responses	Final
3XX	Redirection Responses	Final
4XX	Client-Error Responses	Final
5XX	Server- Error Responses	Final
6XX	Global Failure Responses	Final

III. 비공개형 다자간 컨퍼런스를 위한 SIP 확장

다자간 컨퍼런스는 접근 성격에 따라 공개형(open)과 비공개형(Closed) 다자간 컨퍼런스로 구분되며, 비공개형 다자간 컨퍼런스에서는 각 각의 참가자들에 대한 사용자 정보를 획득하고 분배하여 컨퍼런스의 보안성을 확보하는 것이 매우 중요하다. 또한 새로운 사용자가 컨퍼런스에 참여할 때 새로운 사용자의 호 설정이 완료되기 이전에 컨퍼런스 참가자들은 새로운 사용자의 신원을 알 수 있어야 한다. 그러나 현재 SIP에서는 이러한 참가자 발견, 분배 및 획득을 위한 기능을 지원하지 않고 있다. 그렇기 때문에 SIP 확장을 통해 각 참가자들의 사용자 정보 획득과 분배하는 방법이 요구되며, 이를 위해서는 호 설정 이전에 새로운 사용자 정보의 획득을 위한 INFORM 메소드와 Users 헤더를 설계하여야 한다. 그림 3은 본 논문에서 설계한 SIP 확장 메커니즘에 관련된 알고리

즘을 나타내고 있다.

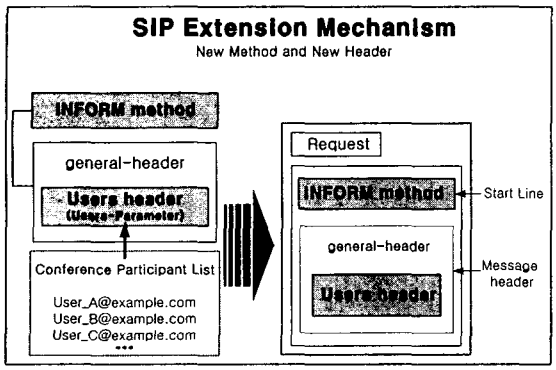


그림 3. SIP 확장 메커니즘의 알고리즘
Fig. 3 Algorithm of SIP Extension Mechanism

3.1 INFORM 메소드

INFORM 메소드는 Users 헤더를 포함하여 컨퍼런스내 사용자 정보를 각 컨퍼런스 참가자들에게 분배하며, 각 참가자들이 가지고 있는 컨퍼런스 참가자 리스트를 업데이트 하는데 사용된다. 기본적으로 Request 메시지와 같은 메커니즘을 갖는다. INFORM 메소드는 컨퍼런스 내에서만 동작이 허용되며, 그렇지 않을 경우에 INFORM 메소드는 481(call leg or transaction doesn't exist) Response로 응답하고 정확한 수신 여부는 200 (ok) Response로 응답한다. INFORM 메소드는 각 사용자 정보와 상태 정보를 표시하는 Users 헤더를 통하여 사용자 정보를 포함하여 컨퍼런스 참가자들의 정보를 분배하게 된다.

3.2 Users 헤더

Users 헤더는 모든 컨퍼런스 참가자들의 SIP 어드레스 정보와 각 참가자들의 컨퍼런스 참여 상태를 파라미터로서 나타낼 수 있다. Users 헤더는 SIP에 사용되는 General Header에 추가된다. Users 헤더 구문(syntax)은 다음과 같다.

```
Users = "Users" ":" ( name-addr | addr-spec )
        [ *( ";" Users-parameter )]
```

각 참가자들의 상태 정보를 나타내는 Users 파라미터들은 아래와 같으며 선택적으로 사용가능하다. 특별한 파라미터가 없을 경우 기본값은 active로 설정 된다.

```
Users-parameter = "status" "=" ( "active"
                  | "joining" | "departed"
                  | "failed" )
```

각 파라미터 값들은 다음과 같이 정의된다.

- active : 컨퍼런스에 참여하여 활성화되어 있는 상태
- joining : INVITE Request를 수신받고 컨퍼런스에 들어오고 있는 상태
- departed : BYE Request를 전송하여 컨퍼런스를 떠나고 있는 상태
- failed : 사용자 정보 표시 오류 상태(failed 상태인 사용자는 다시 한번 사용자 정보가 조회된다.)

각 참가자들이 이러한 Users 헤더를 수신하게 되면 헤더에 담겨있는 참가자 리스트와 참가자들이 가지고 있는 참가자 리스트를 비교하여 차이점이 있으면 업데이트를 수행한다. 즉, INFORM 메소드와 Users 헤더를 사용하면 비공개형 다자간 컨퍼런스에 필요한 보안성 확보가 가능해 진다.

IV. SIP 확장 메커니즘의 동작 및 성능분석

비공개형 컨퍼런스에서 참가자의 보안성 확보를 위해 제안된 SIP 확장 메커니즘을 2가지의 시나리오에 적용하여 동작 및 성능을 분석하였다.

4.1 Dial-in 컨퍼런스 시나리오-1

- 컨퍼런스 시나리오 : 각 사용자 A, B, C 는 동시에 컨퍼런스를 시작하려 한다. 사용자들은 모두 사전에 컨퍼런스 서버에 대한 URI를 알고 있으며 컨퍼런 URI를 통해 컨퍼런스에 참여하게 된다. 그림 4는 컨퍼런스 시나리오를 나타내고 있다.

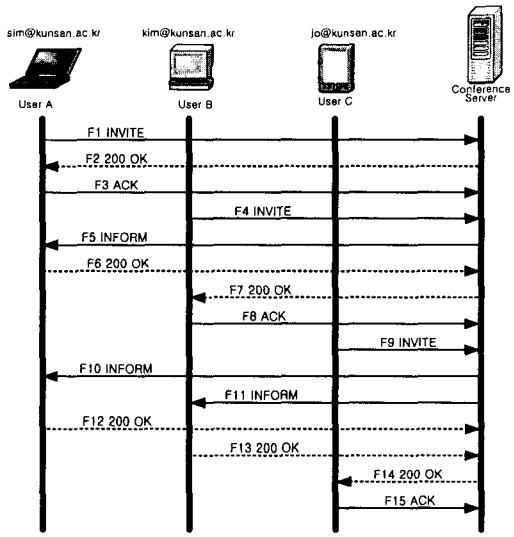


그림 4. Dial-in 컨퍼런스 시나리오<1>
Fig. 4 Dial-in Conference Scenario<1>

호 설정과정에서 INFORM 메소드와 Users 헤더는 아래 표 2, 3, 4와 같이 동작한다.

표 2. F5 INFORM 메소드와 Users 헤더
Table. 2 F5 INFORM method and Users header

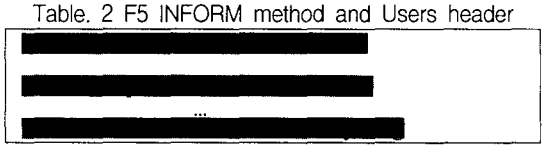


표 3. F10 INFORM 메소드와 Users 헤더
Table. 3 F10 INFORM method and Users header

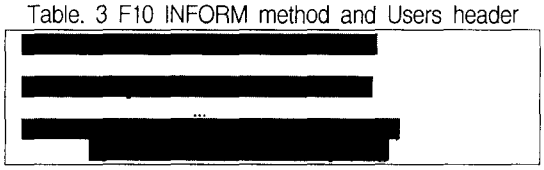
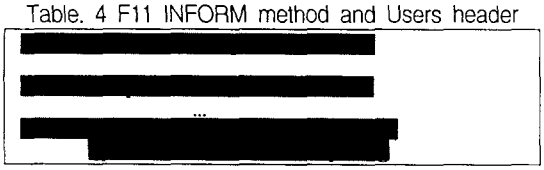


표 4. F11 INFORM 메소드와 Users 헤더
Table. 4 F11 INFORM method and Users header



이와 같이 전송된 INFORM 메소드들을 통해 새로운 사용자가 컨퍼런스에 들어올 경우 호 설정 과정이 완료되기 이전에 컨퍼런스 참가자들에게 새로운 사용자의 정보를 통보함으로서 컨퍼런스 보안성 확보가 효과적으로 이루어지게 된다. 그림 5은 컨퍼런스 내에서 동작된 SIP 확장 메커니즘을 통해 획득된 사용자 정보를 보이고 있다.

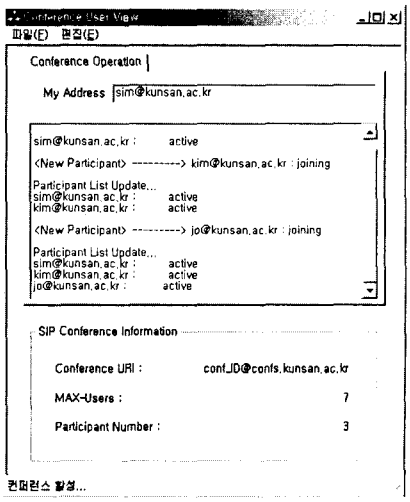


그림 5. Dial-in 컨퍼런스 User View
Fig. 5 User View on Dial-in Conference

4.2 Dial-in Conference 시나리오-2

- 컨퍼런스 시나리오 : 각 사용자 A, B, C는 컨퍼러스 활동을 하고 있다. 이때 사용자 C는 컨퍼런스를 떠나기 위해 컨퍼런스 서버에게 BYE Request를 보낸다. 그림 6은 Dial-in Conference 시나리오-2의 호 설정 과정을 나타낸 것이다.

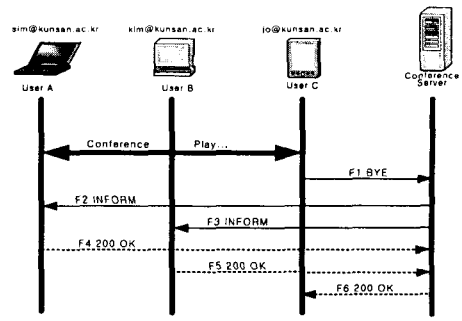


그림 6. Dial-in 컨퍼런스 시나리오<2>
Fig. 6 Dial-in Conference Scenario<2>

표 5. F2 INFORM 메소드와 Users 헤더
Table. 5 F2 INFORM method and Users header

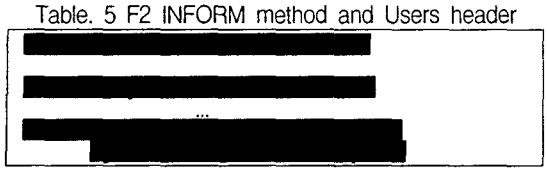
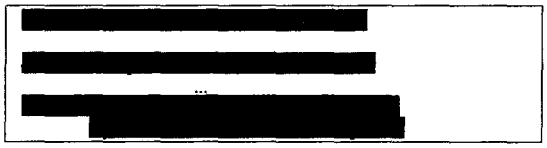


표 6. F3 INFORM 메소드와 Users 헤더
Table. 6 F3 INFORM method and Users header



사용자 C가 컨퍼런스를 떠나기 위해 BYE 메시지를 전송하고 난 후 사용자 C에 대한 정보가 표 5, 6과 같이 다른 사용자들에게 분배되었다.

동작된 SIP 확장 메커니즘을 통해 사용자는 그림 7과 같은 사용자 상태 정보를 확인할 수 있다.

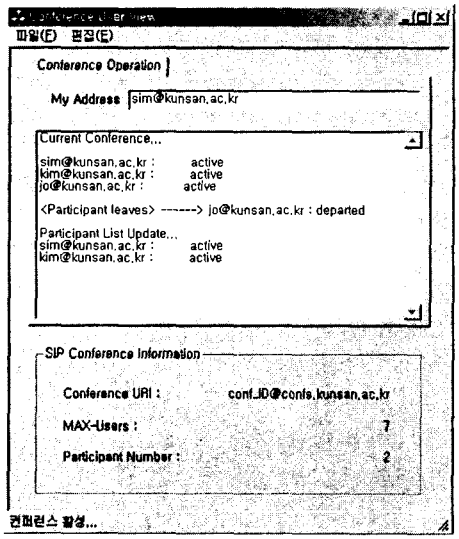


그림 7. Dial-in 컨퍼런스 User View
Fig. 7 User View on Dial-in Conference

V. 결 론

본 논문에서는 비공개형 컨퍼런스에서 컨퍼런스 보안성 확보를 보장하기 위하여 효과적으로 컨퍼런스 보안성 확보가 가능한 INFORM 메소드와 Users 헤더를 포함하는 SIP 확장 메커니즘을 설계하였다. Users 헤더는 각 참가자들의 상태 정보에 대한 파라미터를 이용하여 나타냄으로서 컨퍼런스를 구성하고 있는 모든 참가자들의 사용자 정보를 획득할 수 있으며, INFORM 메소드는 컨퍼런스 내에서 Users 헤더를 포함하여 모든 참가자들의 정보를 각 참가자들에게 분배함으로서 비공개형 컨퍼런스 환경에서 사용자 정보의 획득과 분배가 가능하게 하였다. 또한, 제안한 SIP 확장 메커니즘은 다자간 컨퍼런스 및 비공개형 다자간 컨퍼런스 환경에서 효과적인 사용자 정보의 획득과 분배 메커니즘을 통하여 컨퍼런스 보안성 확보를 통해 차별적인 서비스가 제공되도록 고려 하였다.

향후에는 SIP 확장 메커니즘을 이용한 다양한 서비스를 제공하고 메시지 트래픽을 감소시키기 위해 이에 관련된 알고리즘을 개선 및 보완할 것이며, 다자간 컨퍼런스에서 발생할 수 있는 환경적 요소를 더 많이 고려하여 성능을 평가할 예정이다.

참고 문헌

[1] H. Schulzrinne, J. Rosenberg. "The IETF Internet Telephony Architecture and Protocols," IEEE Network, May. 1999

[2] H. Schulzrinne, J. Rosenberg, "A Comparison of SIP and H.323 for Internet Telephony," Network and Operating System Support for Digital Audio and Video (NOSSDAV), Cambridge, England, July. 1998.

[3] H. Schulzrinne, J. Rosenberg, "A Comparison of SIP and H.323 for Internet Telephony," Network and Operating System Support for Digital Audio and Video (NOSSDAV), Cambridge, England, July. 1998.

[4] F. Fingal, P. Custavsson, "A SIP of IP-telephony," Feb. 1999.

[5] J. Rosenberg, H. Schulzrinne. "Guidelines for Authors of SIP Extensions," IETF Internet Draft, work in progress, 2002

[6] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP : Session Initiation Protocol," IETF RFC 3261, June. 2002.
[7] 유승화, "인터넷 전화," 전자신문사, pp. 159-198, 2002.

저자 소개

김현태(Hyun-tae Kim)

1996년 2월 군산대학교 정보통신공학과 학사 졸업
1998년 8월 군산대학교 정보통신공학과 석사 졸업
2000년 ~ 현재 군산대학교 정보통신공학과 박사과정
※관심분야 : 멀티미디어 스트리밍, RMT,VoIP

김형진(Hyoung-Jin Kim)

1997년 호원대학교 전자계산학과 졸업
1999년 군산대학교 정보통신공학과 석사
2000년~ 현재 군산대학교 정보통신공학과 박사과정
※ 관심분야 : 멀티미디어 시스템, SIP

나인호(In-ho Ra)

1988년 울산대학교 전자계산학과 졸업
1991년 중앙대학교 전자계산학 석사
1995년 중앙대학교 전자계산학 박사
1995.9 ~ 현재 군산대학교 전자정보공학부 부교수
※관심분야 : 멀티미디어 통신시스템, 초고속 통신망