퍼지 및 지능시스템학회 논문지 2005, Vol. 15, No. 1, pp. 65-68

익명기반 유비쿼터스 환경의 프라이버시 보장 ID기반 서비스

Privacy-Preserving ID-based Service in Anonymity-based Ubiquitous Computing Environment

김학준[1], 황경순[2], 이건명[2]

Hak-Joon Kim, Kyoung Soon Hwang, Keon Myung Lee

[1]호원대학교 멀티미디어정보학과

[2]충북대학교 전기전자컴퓨터공학부, 유비쿼터스 바이오정보기술연구센터

[1]College of Information, Howon University

[2]School of Electrical and Computer Engineering and RIUBIT, Chungbuk National University

요 약

유비쿼터스 환경에서는 프라이버시에 민감한 다양한 정보가 수집되고 이들이 통제되지 않은채 배포될 수 있기 때문에 프라이버시 보호가 필수적이다. 유비쿼터스 환경에서 프라이버시 보안을 위해 사용되는 대표적인 방법론의 하나인 익명(anonymity) 기반 기법은, 사용자가 새로운 서비스 영역에 참여할 때 가명(pseudonym)을 사용할 수 있도록 하여, 사용자의 신분을 노출시키지 않도록 하는 방법이다. 이 방법은 사용자의 신분을 보호하는데는 효과적이지만, 친구찾기 서비스, 위험지역경보, P2P통신 등 ID 기반의 서비스를 제공하기 어렵게 하는 단점이 있다. 이 논문에서는 익명기반의 프라이버스 보호 기법을 사용하는 유비쿼터스 환경에서 ID 기반의 서비스를 제공할 수 있도록 하는 시스템 구조를 제안한다.

Abstract

Privacy preservation is crucial in ubiquitous computing environment in which lots of privacy-sensitive information can be collected and distributed without appropriate control. The anonymity-based approach is a famous one used for privacy preservation communication, which allows users to use pseudonyms instead of real ID so as not to reveal their identities. This approach is effective in that it can hide the identity of users. However, it makes it difficult to provide ID-based services like buddy service, dangerous area alert, P2P communication in the ubiquitous computing. We proposes a system architecture which enables ID-based services in the ubiquitous computing environment employing anonymity-based privacy-preserving approach.

Key words : ubiquitous computing, privacy preservation

1. 서 론

언제 어디에서든 별 의식하지 않고 컴퓨팅 서비스를 사용할 수 있는 유비쿼터스 컴퓨팅 환경에 대한 연구가 최근 활발히 수행되고 있다. 사용자가 단말기를 통해서 작업의 처리 과정을 구체적으로 지시하지 않아도 원하는 컴퓨팅 서비스를 사용할 수 있도록 하기 위해서, 유비쿼터스 환경에서는 사용자의 신분, 위치, 서비스 시간, 주변 객체 등과 같은 상황정보를 사용자의 직접적인 간여없이 획득하여 사용해야 한다. 따라서 유비쿼터스 컴퓨팅에서는 환경에 내장된 다양한 센서들을 통해서 많은 상황정보가 수집되어 어디엔가 저장되게 된다. 어떤 상황정보는 프라이버시에 관련되어 있기 때문에, 누군가 이들 정보를 접근하게 되면 사용자의 프라이버시가 침해될 수 있는 개연성이 있다. 대표적인 이러한 상황정보로는 사용자의 신분, 서비스 위치 등을 들 수 있다.

유비쿼터스 컴퓨팅 분야에서는 사용자의 프라이버시를 보장하기 위한 여러 기법들이 개발되어 왔는데, 이들은 다음과 같이 정책(policy) 기반 접근방법, 익명(anonymity) 기반 접근방법, 익명통신(anonymous communication) 기반 접근방법으로 대별해 볼 수 있다.[1-13] 정책기반 접근방법에서는 프라이버시에 민감한 정보에 대한 접근을 통제하기 위해, 사용자가 자신의 정보에 대한 접근허용정책을 지정하고, 정보에 접근하려는 응용프로그램이나 사용자는 해당정보 사용정책을 정보접근시에 제시하도록 함으로써, 프라이버시에 민감한 정보에 대한 접근통제를 하는 방법이다.[1] 정책기반 접근방법에서는 실제 정보접근제어를 수행하는 제3의 서버가 있다. 이 서버는 하부의 센서 네트워크를 통해서 사용자의 프라이버시에 관련된 정보도 수집하게 된다. 사용자는 자신의 프라이버시 정책을 이 서버에 등록하게 되고, 다른 응용프로그램이나 사용자는 이 서버에 정보의 사용정책과 함께 정보를 요청하게 된다. 사용자의 접근허용정책과 응용프로그램의 정보사용정책을 바탕으로, 해당 서버가 정보의 접근여부를 결정하게 된다. 이 접근방법에서는 사용자는 무조건적으로 해당 서버가 신뢰성있게 행동할 것이라고 믿어야 하는 맹점이 있다.

접수일자 : 2004년 9월 30일
완료일자 : 2004년 12월 6일
감사의 글 : 본 연구는 충북대 산업협력단 부설 유비쿼터스 바이오정보기술연구센터의 일부 지원을 받아 수행된 것임.

익명기반 접근방법은 사용자가 서비스를 사용할 때 가명을 사용할 수 있도록 하여 다른 사용자나 응용프로그램이 사용자의 신분을 확인할 수 없도록 하는 방법이다.[2] 이 방법은 사용자가 익명을 사용함으로써, 센서 네트워크에 의해 정보가 수집되더라도 사용자의 ID와 연계시킬 수 없기 때문에 효과적으로 사용자의 프라이버시를 보호할 수 있는 장점이 있다. 반면, P2P 통신, 친구찾기(buddy) 서비스 등 ID 기반의 서비스를 제공하기 어려운 단점도 있다.

익명통신 기반 접근방법에서는 프라이버시 보호의 일환으로 통신을 도청하여 트래픽을 분석하더라도 누가 누구와 통신하는지 확인할 수 없도록 하는 통신채널을 확보하는 기법이다.[14] 이를 구현하는 방법으로는 중간의 제3자를 통해서 통신을 중개하는 방법과 통신네트워크에서 특별한 조작을 하는 방법 등이 있다.

이 논문에서는 익명기반의 프라이버시 보호 기법을 사용하는 환경에서 ID기반의 서비스를 할 수 있도록 하는 시스템 구조를 제안한다.

2. 제안한 ID기반 서비스 시스템 구조

이 논문에서는 다음과 같은 상황에 대한 ID기반 서비스를 대상으로 한다. 통신 상대방은 시시각각 변할 수 있는 익명을 사용하지만 서로 통신을 하고자 하고, 프라이버시를 보호하기 위해 센서 네트워크에 자신들이 실제 ID를 노출시키지 않는다. 익명을 사용할지라도 익명을 통해서 유비쿼터스 통신 환경에 있는 해당 사용자와 통신을 할 수 있는 통신 인프라를 가지고 있다고 전제한다. 이러한 환경에서는 사용자는 통신할 상대방에 대한 현재 가명을 알고 있어야 한다.

2.1 시스템의 구조

(그림 1)은 익명기반 시스템에서 ID기반 서비스를 위해 제안한 다중 에이전트 기반의 시스템 구조를 나타낸 것이다. 화이트페이지(white page) 에이전트(WPA)는 적합한 키(key)를 가지고 있는 사용자가 자신의 친구에 대한 현재 가명 정보를 얻을 수 있도록 하기 위한 화이트페이지 역할을 한다. 이 에이전트는 사용자의 가명 갱신 요청을 받아서, 사용자 디렉토리 에이전트(UDA)에 전달하고, UDA들의 요청에 따라 사용자들의 가명정보를 수정하는 일을 한다.

사용자 에이전트(UA)는 사용자가 휴대한 단말기에서 동작하는 프로그램으로, 사용자를 위해서 다른 에이전트 또는 응용 프로그램들과 프라이버시를 보장하면서 통신을 대행하는 역할을 한다.

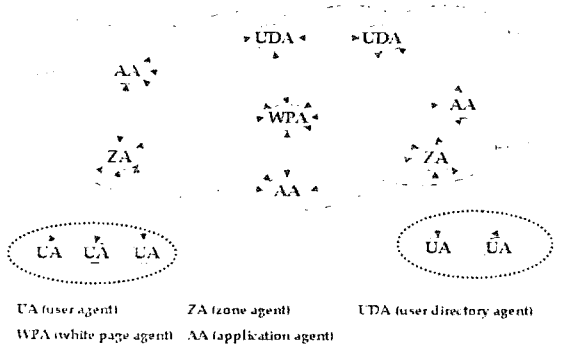

그림 1. 제안한 ID기반 서비스 시스템 구조

영역(zone) 에이전트(ZA)는 특정 물리적인 영역을 관리하는 에이전트로서, 해당 영역에 들어오거나 나가는 사용자 에이전트를 모니터링하여, 영역에 참여하는 새로운 사용자 에이전트에 새로운 식별자(가명)을 할당한다. 또한 사용자 에이전트와 다른 사용자 에이전트 또는 응용 프로그램과의 통신을 중개한다.

사용자 디렉토리 에이전트(UDA)는 사용자의 요청에 따라 화이트페이지 에이전트에 저장된 사용자의 가명정보를 갱신하도록 하는 일을 수행한다. 제안한 구조에서는 여러 사용자 디렉토리 에이전트가 있고, 각각은 여러 사용자를 담당할 수 있다. 응용 에이전트(AA)는 응용프로그램의 인터페이스 역할을 하는 에이전트로서, 해당 응용 프로그램에 대한 요청을 받아들이고, 처리결과를 전달하는 일을 한다.

2.2 안전한 가명 등록

제안한 방법에서는 사용자의 현재 가명을 허가받은 사용자나 응용 프로그램만 획득할 수 있도록 하기 위해, 사용자는 자신의 가명을 암호화하여 화이트페이지 에이전트(WPA)에 등록해 둔다. WPA는 각 사용자별로 (사용자의 실제 ID, friend 키들로 암호화된 사용자 가명의 리스트)로 된 레코드를 관리한다. 어떤 사용자나 응용 프로그램도 사용자의 실제 ID를 알고 있으면, WPA에 등록된 암호화된 사용자의 가명을 접근할 수 있다. 그렇지만, 가명이 암호화되어 있기 때문에, 암호화에 사용된 키를 모르면, 실제 가명을 얻을 수 없다. 제안한 방법에서는 허가된 사용자, 응용 프로그램별로 별도의 friend key라고 하는 키(key)를 생성하고, 현재 가명을 이들 각 friend key로 암호화하여 WPA에 등록한다. 사용자가 직접 암호화된 자신의 가명값을 바꾸도록 WPA에게 요청하면, 트래픽 분석을 할 수 있는 공격자는 어떤 주소(IP 등)의 사용자가 해당 레코드를 수정하였는지 알 수 있기 때문에, 실제 ID와 현재 사용자의 주소를 대응시킬 수 있다. 따라서, 제안한 방법에서는 이러한 공격에 대응하기 위해서 UDA(user directory agent)라는 에이전트를 통해서 이러한 가명을 관리하는 작업을 대행하도록 하는 접근방법을 택하고 있다.

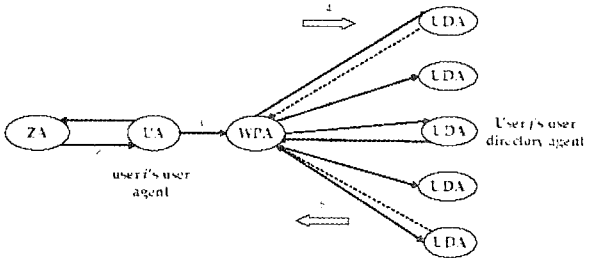

그림 2. 새로운 가명 등록 과정

(그림 2)는 사용자가 안전하게 자신의 가명을 WPA에 등록하기 사용하는 과정을 보인 것이다. 제안한 시스템에서는 먼저 사용자가 특정 서비스 영역에 들어가게 되면, UA가 해당 영역의 ZA에게 새로운 가명을 요청하여 받게 되고(1, 2단계), UA는 자신의 UDA와 공유하는 암호키로 새로운 가명정보를 암호화하여 WPA에게 전달한다(3단계). WPA는 받은 메시지를 모든 UDA에게 방송하고, 이를 받은 UDA는 메시지를 해독하려고 시도하는데, 실제 대응되는 UDA만 메시지를 해독할 수 있게 된다(4단계). 해독에 성공한 UDA는 해당 사용자의 friend key값들로 해당 가명을 암호화한 메시지

를 WPA에 전달하여 레코드 갱신이 일어날 수 있도록 한다(5단계). 이때 트래픽 분석이 가능하면 어떤 UDA가 어떤 사용자와 대응되는지 파악할 수 있기 때문에, 실제 사용자의 가명을 수정하지 않는 UDA도, 무작위로 지정된 확률로 실제 정보는 수정하지 않지만 저장된 레코드를 수정하는 메시지를 WPA로 전달한다.

2.3 사용자의 가명 검색

어떤 사용자 i가 다른 사용자 j와 통신을 하고자 할때는 j의 현재 가명을 알고 있어야 하고, j의 실제 ID도 알고 있어야 한다. i는 j의 현재 가명을 알기 위해 j를 포함한 여러 개의 사용자에 대한 암호화된 가명을 WPA에게 요청하는데, 이때 메시지의 스니핑을 방지하기 위해 메시지를 WPA의 공개키로 암호화하여 보내고, 메시지에는 응답메시지를 암호화할 때 사용할 비밀키도 함께 보낸다. WPA는 요청받은 사용자들의 (실제 ID, friend key들로 암호화된 가명의 리스트)를 i가 보낸 비밀키로 암호화해서 i에게 보낸다. i가 j와 친구관계라면, j에 대한 friend key를 가지고 있기 때문에, 받은 메시지로부터 j에 대한 현재 가명을 획득할 수 있게 된다.

2.4 사용자의 가명갱신에 대한 확인

사용자는 자신의 가명에 대한 갱신을 요청한 후 WPA가 제대로 갱신을 했는지 확인하고 싶어 한다. WPA가 레코드를 갱신한 후 직접 사용자에게 갱신 성공여부를 알려주게 되면, 트래픽 스닝핑을 하여 데이터마이닝 기법등을 적용할 경우 사용자와 가명간의 연관관계 추정이 가능할 수도 있다. 따라서 제안한 방법에서는 사용자가 자신을 포함한 몇 개의 사용자에 대한 가명정보를 WPA에게 비정기적으로 요청하는 방법으로 가명갱신의 성공여부를 확인하도록 하는 전략을 채택하고 있다.

2.5 가명 명칭부여 방법

제안한 방법에서는 가명에 기반해서 서비스가 일어나기 때문에, 각 사용자가 이용하는 가명은 전체 유비쿼터스 환경에서 다른 사용자의 것과 중복되면 안된다. 이러한 제약을 만족시키기 위해서 제안한 방법에서는 사용자가 현재 위치하고 있는 영역의 ID와 해당영역에서 사용자에게 임시로 할당한 사용자 번호의 조합으로 사용자의 가명을 나타낸다. (그림 3)은 제안한 방법에서 사용하는 가명 표현형태를 보인 것이다. 가장 오른쪽 필드는 영역에이전트가 할당한 임시 사용자 번호이고, 나머지 왼쪽 필드들은 해당 영역의 ID를 나타낸다. 이와 같은 가명 표현방법을 사용함으로써, 가명에 기반하여 해당 사용자에 대한 메시지를 네트워크에서 쉽게 라우팅(routing)할 수 있고, 또한 위치기반(location based) 서비스를 효과적으로 제공할 수도 있다.

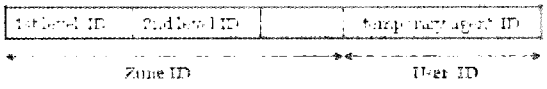

그림 3. 가명의 구조

2.6 친구관계 설정

제안한 방법에서는 프라이버시를 보호하기 위해서 사용자와 '친구관계'인 사용자나 응용프로그램 등만이 해당 사용자의 가명을 WPA를 통해서 알수 있도록 하는 방법을 채택하고 있다. 친구관계는, 어느 사용자 또는 응용 프로그램 i의 친구관계 설정요청에 대해서 j가 이를 취사선택하여 받아들이는 형태로 맺어진다. (그림 4)는 제안한 방법에서 친구관계 설정을 위해 사용하는 프로토콜을 보인 것이다. 먼저, 사용자 i가 자신의 UA를 통해서 자신의 UDA에게 사용자 j와 친구관계 설정을 해 달라는 요청을 한다(1단계). UDA는 WPA에게 (i의 UDA 주소, 사용자 j의 실제 ID, 나중 응답메시지 암호화에 사용될 비밀키)로 구성된 메시지를 WPA와 UDA들이 공유하는 세션키로 암호화시켜 전송한다(2단계). WAP는 어떤 UDA가 사용자 j를 관리하는지 모르기 때문에 받은 메시지를 모든 UDA에 방송한다(3단계). 메시지를 받으면, j를 관리하는 UDA는 i의 UDA에게 (j의 UDA 주소, 나중 통신에 사용할 세션키) 메시지를 이전 메시지에서 들어있던 비밀키로 암호화하여 보낸다(4단계). 이에 대해, i의 UDA는 j의 UDA에게 받은 세션키로 암호화한 i의 친구관계 요청 메시지 (i의 ID, i의 신분확인을 위한 디지털 서명)을 보낸다(5단계). 메시지를 받은 j의 UDA는 j에게 친구관계 요청 사실을 알려서 j가 이를 받아들일지 여부를 확인한다(6,7단계). j가 친구관계 설정을 거부하면, 이를 i에게 해당 UDA들을 통해 알려준다(9,10단계) j가 친구관계 설정을 받아들이면, j의 UDA가 i를 위한 friend key를 하나 만들고, 이것으로 암호화한 j의 현재 가명을 WAP의 j에 대한 레코드에 추가하도록 한 다음(8단계), 이를 i에게 UDA를 통해서 friend key를 알려준다(9,10단계).

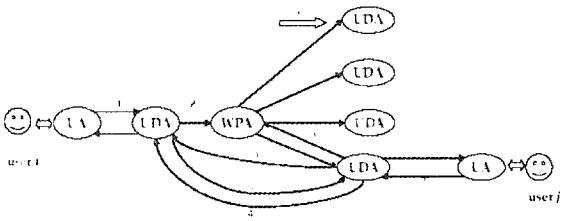

그림 4. 친구관계 설정

3. 친구찾기 서비스 시나리오

(그림 5)는 제안된 시스템 구조를 이용하여 유비쿼터스 환경에서 친구찾기 서비스를 위한, 친구찾기서비스 에이전트(BSA)와 사용자 i, j간의 초기 설정과정을 보인 것이다. BSA에 i와 j가 서로 친구찾기 서비스를 하고 싶다고 등록하면, BSA는 주기적으로 이들의 위치를 파악하여 이들이 서로 근처에 있을 때 이를 알려주게 된다. (그림 5)는 친구관계인 i와 j가 서로 친구찾기 서비스를 하고 싶을 때, BSA를 위한 friend key를 등록한 다음, 이를 BSA에 알려줘서 서비스를 시작할 수 있도록 하는 과정을 보인 것이다.

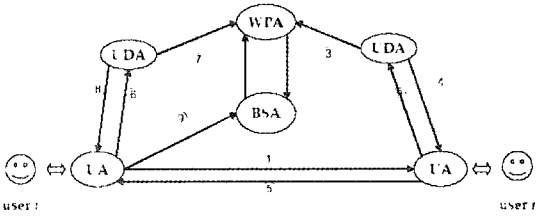

그림 5. 친구찾기 서비스

먼저 i의 UA가 j의 UA에게 친구찾기 서비스 허가요청 메

시지를 보낸다(단계 1). j가 이를 거부하면, j의 UA는 이를 i의 UA에게 이를 통보한다(단계 5). j가 이를 승인하면, j의 UA는 j의 UDA에게 i와의 친구찾기 서비스에 사용할 friend key를 생성할 것을 요청한다(단계 2). 이에 대해 j의 UDA는 friend key를 생성하여, 이 키로 j의 현재 가명을 암호화한 다음, WPA에 등록한다(단계 3). 그다음, j의 UDA는 j의 UA에게 friend key를 알려준다 (단계 4). j의 UA는 친구찾기 서비스 허가요청에 대한 승인 메시지를 friend key와 함께, i의 UA에게 전달한다(단계 5). 이후, i의 UA는 i의 UDA에게 j와의 친구찾기 서비스를 할 때 사용할 friend key를 만들어 WPA에 등록할 것을 요청하고, i의 UDA는 WPA에 이를 등록한다(단계 6, 7, 8). 이 과정이 끝나면, i의 UA는 친구찾기 서비스 에이전트(BSA: buddy service agent)에게 자신과 j의 friend key를 알려주고, i와 j에 대한 친구찾기 서비스를 시작할 것을 요청한다(단계 9). BSA는 friend key 정보를 이용하여, 주기적으로 i와 j의 가명을 확인하고, 이로부터 위치정보를 획득하여, 두 사용자가 인접지역에 있으면, i와 j의 UA에게 이를 알려주게 된다.

4. 결론 및 향후과제

유비쿼터스 환경에서 프라이버시 확보는 매우 중요한 문제이다. 이 논문에서는 화이트페이지 역할을 하는 에이전트를 통해서 익명기반 접근방법에 따라 프라이버시 보호를 하는 시스템에서 ID기반의 서비스를 제공하는 방법을 제안하였다. 제안한 방법은 익명기반 접근방법에서 곤란했던 ID 기반 서비스를 제공할 수 있도록 한다. 또한 가명을 영역의 ID와 연관시켜 생성하도록 함으로써 메시지의 효과적인 라우팅이 가능하도록 하고, 또한 친구찾기 등과 같은 위치기반 서비스를 가능하게 한다. 제안한 방법은 아직 정책기반 접근방법에서와 같은 세밀한 접근제어를 하지는 못하기 때문에 이에 대한 향후 연구가 필요하다. 또한 제안된 방법에서 부가적으로 발생하는 통신 부담을 줄이기 위한 효과적인 방법에 대한 연구도 추후 요구된다.

참 고 문 헌

[1] G. Myles, A. Friday and N. Davies. *Preserving Privacy in Environments with Location-Based Applications.* IEEE Pervasive Computing 2(1). (2003). 56-64.

[2] A. R. Beresford and F. Stajano. *Location Privacy in Pervasive Computing.* IEEE Pervasive Computing 2(1). (2002). 46-55.

[3] M. Gruteser, G. Schelle, A. Jain, R. Han and D. Grunwald. *Privacy-Aware Location Sensor Networks.* http://systems.cs.colorado.edu/Papers/Generated/2003PrivacyAwareSensors.html (2003).

[4] X. Jiang and J. Landay. *Modeling Privacy Control in Context-aware Systems.* IEEE Pervasive 1(3). (2002).

[5] M. Langheinrich. A Privacy Awareness System for Ubiquitous Computing Environments. In Ubicomp 2002. (2002).

[6] S. Lederer, A. K. Dey, J. Mankoff. *Everyday Privacy in Uniquitous Computing Environment.* In Ubicomp 2002 Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing. (2002).

[7] A. Smailagic. D. P. Siewiorek, J. Anhalt, D. Kogan, Y. Wang. *Location Sensing and Privacy in a Context Aware Computing Environment.* In Proc. Pervasive Computing, 2001. (2001).

[8] J. Hightower, G. Borriello. *Location Systems for Ubiquitous Computing.* IEEE Computer 34(8). (2001). 57-66.

[9] A. R. Prasad, P. Schoo, H. Wang. *An Evolutionary Approach towards Ubiquitous Communications*: A Security Perspective. In Proc. of SAINT 2004: The 2004 Symposium on Applications & Internet. (2004).

[10] M. Hazas, A. Ward. *A High Performance Privacy-Oriented Location System.* In Proc. of IEEE International Conference on Pervasive Computing and Communications. (2003).

[11] P. Osbakk, N. Ryan. *Expressing Privacy Preferences in terms of Invasiveness.* In Position Paper for the 2nd UK-UbiNet Workshop(University of Cambridge, UK). (2004).

[12] E. Snekkenes. *Concepts for Personal Location Privacy Policies.* In Proc. of the 3rd ACM conference on Electronic Commerce. ACM Press. (2001). 48-57.

[13] U. Jendricke, M. Kreutzer, A. Zugenmaier. *Pervasive Privacy with Identity Management.* In Ubicom2002.(2002).

[14] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. Dennis Mickunas, S. Yi, *Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments.* ICDCS'02, (2002).

저 자 소 개

김학준(Hak-Joon Kim)
서울대 수학교육과 학사
숭실대 전자계산학과 석사
충북대 전자계산학과 박사수료
현 호원대학교 멀티미디어정보학과 교수
관심분야 : 프라이버시 보안, 인공지능, 소프트웨어 공학

황경순(Kyoung Soon Whang)
한국방송통신대학 전산학과 학사
충북대 전자계산학과 석사
충북대 전자계산학과 박사과정
관심분야: 데이터마이닝, 인공지능

이건명(Keon Myung Lee)
제14권 6호 참조