韓國 컴퓨터情報學會 論文誌
第13卷 第4號, 2008. 7.

2008-13-4-4-3

유비쿼터스 환경을 위한 CASA 기반의 동적 접근 제어 기법

김 경 자*, 장 태 무**

A CASA-Based Dynamic Access Control Scheme for Ubiquitous Environments

Kim Kyoung Ja *, Chang Tae Mu **

요 약

기존의 상황 인식 서비스 모델에서는 리소스에 대한 접근 권한을 사용자의 인증으로만 리소스에 대한 접근을 허용하였으나, 사용자의 주변 상황 정보가 빈번하게 변화하는 유비쿼터스 환경에서는 상황 변화에 따른 리소스 접근 제어가 제공될 필요가 있다. 본 논문에서는 사용자의 상황 정보가 변경되는 경우에 따라 리소스에 대한 접근 권한을 동적으로 제어하고자 한다. 접근 제어는 기존의 CASA(Context-Aware Security Architecture)를 기반으로 하지만 현재 서비스를 받고 있는 사용자라 할지라도 리소스 접근 권한을 제한할 수도 있다. 즉, 주위 환경 정보를 실시간으로 검사하여 주위 환경에 따라 동적으로 접근 권한을 달리 부여하여 기존의 상황 인식 서비스보다 리소스에 대한 강인한 보안 서비스를 제공한다.

Abstract

Conventional context-aware service models permit the access of resources only by user authentication, but the ubiquitous environments where the context information around users is changing frequently require the resource access control according to the rapid changes.

This paper proposes a scheme to control access permission of resource dynamically as context information of user changes. Our access control model is based on traditional CASA (Context-Aware Security Architecture), but can restrict the access of the user already has been authorized. With the real-time checking of context information, our scheme gives different access controls according to changes in environmental information, and provides more secure services than conventional context-aware models.

▸ Keyword : 상황 인지 보안 구조(CASA, Context-Aware Security Architecture), 상황 인지 서비스(Context-Aware Service), 접근 제어(Access Control), GRBAC

• 제1저자 : 김경자 • 교신저자 : 장태무
• 접수일 : 2008. 5. 13, 심사일 : 2008. 7. 1, 심사완료일 : 2008. 7. 25.
* 동국대학교 컴퓨터공학과 강사 ** 동국대학교 컴퓨터공학과 교수
- 본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음. [2008-F-041-01, 학습 및 진화를 통한 S/W, H/W적 재설계가 가능한 지능로봇 기술 개발]

Ⅰ. 서 론

유비쿼터스 컴퓨팅을 완성하기 위해서는 인간이 지능을 가지고 주변 상황 정보에 기반하여 서로 대화를 나누며 결정을 내리는 것처럼 컴퓨팅 환경도 주변 상황을 인식하고 판단하여 인간에게 유용한 서비스를 제공해야 한다. 이를 실현하기 위해 많은 상황 인식 서비스에 대한 연구가 진행되어왔다[1]. 그러나 특정 상황과 시스템에 한정적인 기존 연구 사례는 주어진 상황 정보가 변화하면 적용될 수 없다는 한계점을 가지고 있다. 이를 해결하기 위해서 동적으로 주변 상황에 적응될 수 있는 상황 인식 서비스 인프라에 대한 연구가 활발하게 진행되고 있다. 이러한 상황 인식 서비스 인프라에 대한 연구의 대부분은 리소스의 보안 정책을 거의 고려하지 않고 있는 실정으로 내부의 악의적인 사용자에 의해 남용될 가능성이 높다고 본다. 이에, 본 논문에서는 보안 정책을 고려하여 동적으로 서비스를 제공할 수 있는 상황 인식 서비스 인프라 설계에 초점을 맞추고자 한다.

기존의 상황 인식 서비스 인프라에서는 리소스에 대한 접근 권한을 사용자의 인증 단계만을 거치고 권한을 부여 받게 된다. 그러나 유비쿼터스 환경에서는 사용자의 권한이 주변 상황 정보에 따라 자원이나 서비스의 사용 가능 유무가 달라질 수 있음을 배제하고 있다. 예를 들어, 서비스를 받고 있는 사용자는 사용자 정보로 권한 인증을 받았으나, 인증을 받지 않은 사용자가 같은 공간에 있는 것만으로도 간접적으로 동일한 서비스를 받을 수 있는 경우에는 문제가 될 수 있다. 이에 본 논문에서는 사용자의 상황 정보에 따라 리소스의 접근 제어를 통제할 수 있는 모델을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 유비쿼터스 환경에서 리소스에 대한 접근 권한의 중요성과 이를 위한 인프라 설계의 필요성을 1장에서 제시하고, 2장에서는 상황 인식 서비스를 고려한 인프라들의 종류들을 살펴본다. 3장에서는 주변 상황 정보 변화에 따른 리소스 접근 권한을 제한하는 모델을 제시한다. 즉, CASA에서 상황 인식 정보를 고려하여 서비스의 접근을 통제함으로 보안상 취약했던 기존의 CASA방식을 확장한다. 4장은 기존의 상황 인식 서비스 인프라 모델들과 제안 방식을 상황 인식 서비스 인프라에서 가져야 되는 필수 요구 기술들을 비교한다. 마지막으로 5장에서는 결론과 향후 연구 과제를 제시하며 본 논문의 끝을 맺고 있다.

Ⅱ. 상황 인식 서비스 인프라

상황 정보(Context Information)는 사용자의 요구와 주변 상황이 수시로 변화하는 이동 통신 환경에서 더욱 중요하게 활용된다. 즉, 다양한 센서 및 컴퓨터들이 수집한 각종 환경 정보를 효과적으로 상호 공유하여 사용자 및 주변 환경의 상황(Context)들을 알아내고, 그에 맞는 다양한 정보에 근거하여 자발적으로 서비스를 제공하는 상황 인식 정보의 활용이 더욱 필요하게 된다. 이에 상황 인식 서비스를 가능하게 하기 위해서는 사용자 및 사물 들의 객체를 인식하고, 이들의 현 상태에 따른 상황 정보를 수집하여 서비스에 적용하는 기술이 필수적이다.

현재 상황 인식 서비스 인프라는 다양한 연구 목적으로 많은 연구가 이루어지고 있다. 그 중에서도 주된 연구 분야로는 다양한 상황 인식 서비스를 제공할 수 있는 인프라를 표준화하거나 사용자의 서비스를 손쉽게 제공할 수 있도록 하는 미들웨어에 대한 연구가 가장 많이 진행되고 있다. 이러한 상황 인식 서비스 인프라에 대한 많은 연구에도 불구하고 서비스 제공 여부에 관련하여 보안 측면을 강화하려는 방안이 많이 미흡하다. 이에 본 논문에서는 리소스에 접근 제어를 사용자의 상황 정보에 따라 달리 부여함으로 보안 문제를 조금이나마 해결할 수 있는 방안을 제안한다.

본 논문의 제안 기법을 기술하기에 앞서 현재까지의 상황 인식 서비스 인프라의 연구 들을 살펴보면 Scarlet-Context-Aware Infrastructure, ServiceGlobe, Gaia, SOCAM, CASA로 크게 5가지의 연구들을 볼 수가 있다[2][3]. Scarlet-Context-Aware Infrastructure는 이질적인 플랫폼간에 상황 정보를 서로 교환할 수 있도록 하였고, HTTP를 기반으로 한 SOAP와 WSDL을 활용하여 플랫폼간의 호환성을 유지하도록 하였다. ServiceGlobe는 다양하고 이질적인 고객 단말의 능력과 고객의 위치 정보를 고려하여 더 나은 상황 인식 웹 서비스를 제공하기 위함이 목적이다. 서비스에서 고려되는 상황 정보로는 고객 단말의 종류, 스크린 해상도, 지원 색상수 그리고 고객의 위치 정보를 사용한다. 고객의 상황 정보는 HTTP을 기반으로 하는 SOAP을 통해 서비스 플랫폼으로 전송되고, 서비스 플랫폼에서는 SOAP 헤더에 포함된 상황 정보를 추출하고 처리하여 고객의 상황에 적절한 서비스를 제공하게 된다. Gaia는 상황 인식 서비스 구조로 응용이 다양한 상황 정보를 얻고 추론할 수 있게 해준다. Gaia의 상황 인식 서비스 구조는 다른 센서나 다른 데이터 소스로부터 상황 정보를 수집하여 응용에 제공하는 Context Provider와 수집한 상황 정보를 상위의 상황 정보로 추론하고 추상화하여 응용에 제공하는 Context Synthesizer로 구성된다. National University of Singapore에서 상황 인식 정보를 모바일 서비스로 제공하기 위한 미들웨어로

SOCAM(Service-oriented Context-aware Middleware)을 제시하였다. 미들웨어 내에서 상황 정보 모델링을 위해 OWL(Web Ontology Language)를 제안하며, [그림 1]에서 보는 바와 같이 여러 컴포넌트로 구성되어 있다. 여러 센서들로부터 상황 정보를 받아서 추상화하고, 상황 정보를 변환하는 상황 정보 제공자(Context Provider)와 변환된 정보를 전달받는 상황 정보 번역자(Context Interpreter)로 구성된다. 이러한 상황 정보 번역자는 해당 정보를 논리적인 추론 방식을 적용하여 유용한 정보로 번역한다. 또한, 생성된 정보를 DB에 저장하거나 다른 상황 인식 서비스에게 제공하게 된다.

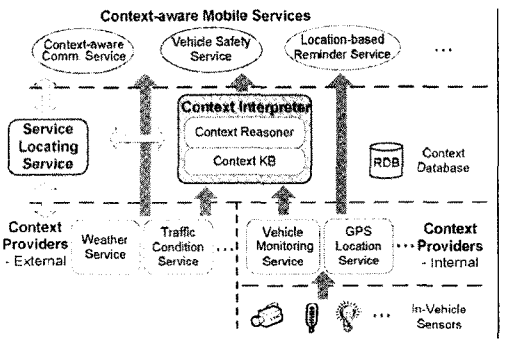

그림 1. SOCAM 상황 인식 서비스 구조
Fig 1. SOCAM Context-Aware Serviece Structure

CASA(Context-Aware Security Architecture)는 사용자 생체 정보나 위치 정보를 위한 미들웨어 레벨의 보안 플랫폼이다. CASA에서 상황 인식 인증(Context-aware authorization)은 생체 인식 기술 또는 Active Badge와 같은 센서를 이용하여 사용자의 ID, 위치, 역할을 인식하여 사용자를 인증하게 된다. 상황 인식 접근 제어(Context-aware Access control)는 다양한 접속 네트워크와 서비스, 장치등과 상호 작용이 빈번하게 발생하는 이동 컴퓨팅 환경에서 접속 제어 및 권한 부여와 같은 보안 서비스를 제공한다. 또한 정책 결정을 위해서는 GPDL(Generalized Policy Definition Language) 과 사용자 인식, 시간, 장소 등을 고려한 권한 부여를 위하여 GRBAC (Generalized Role-Based Access Control)모델을 제안하고 있다[4].

위에서 제시한 여러 상황 인식 서비스 인프라들은 다양한 각도에서 다양한 목적을 위해 연구되고 있다. 그러나, 기존의 여러 상황 인식 서비스 인프라에서는 사용자의 정보들을 이용하는 측면에서 가장 중요한 보안 문제를 위한 부분이 미흡하다고 본다. ServiceGlobe는 서비스 제공 여부를 고객 단말의 능력과 고객 위치 정보만을 고려하여 서비스를 제공하고 있다. 또한 Gaia의 경우에는 수집한 상황 정보가 신뢰 할 수 있는 정보인지를 판단하는 과정이 없다. CASA에서 사용되는 역할 기반 접근 제어(Role-Based Access Control)기법은 빈번하게 변화하는 상황 정보에 따른 서비스의 차별화가 없다는 한계가 있고, 사용자의 주변 환경 정보로 활용되는 위치 식별 정보를 제외하고는 사용하지 않기 때문에 더욱 많은 상황 정보들을 고려해야 할 필요가 있다고 본다. 본 논문에서는 상황 인식 정보를 더욱 확장하여 보다 동적인 리소스 접근 제어를 가능하게 하고자 한다.

III. 주변 상황 정보를 고려한 D-CASA

초기의 상황 인식 서비스 구조는 다양한 상황 정보와 상황 정보 센싱 기술을 조합하여 특정 플랫폼만을 위한 개별적인 프로토타입 형태를 응용한 것으로 확장을 위해서는 많은 사전 지식을 필요로 하는 문제점을 갖는다. 또한 기존의 모듈을 재사용하는 측면에서는 공통된 기능들의 모듈화가 이루어지지 않아서 많은 어려움이 있다. 이에, 상황 인식 서비스를 일관된 방법으로 제공하기 위한 인프라를 개발하는 연구들이 많이 진행되어 왔다. 상황 인식 서비스 인프라를 위한 연구는 상황 인식 응용 개발에 필요한 공통 기능을 응용 레벨에서 분리하여 미들웨어 형태로 개발자에게 공급하게 된다. 즉, 사용자는 일반화된 응용 서비스만을 제공하게 됨으로 서비스 제공을 위한 구조를 이해할 필요가 없게 된다[5][6][7]. 그러나, 위에서 제시하고 있는 인프라의 연구에서도 리소스의 보안 정책을 거의 고려하지 않고 있는 실정으로 보안 측면에서 많은 문제점들이 거론되고 있다. 이에 보안 문제를 다루기 위한 인프라들이 등장하게 되었다.

본 논문에서는 보안 정책을 고려하여 CASA(Context Aware Security Architecture)를 기반으로 리소스를 동적으로 접근하는 기법을 제안한다. 일반적으로 상황 인식 서비스 구조 설계는 리소스의 보안 정책을 거의 고려하지 않고 있는 실정이고, 권한을 가진 사용자의 서비스 공간의 개방성을 고려하지 못하고 있다.

[그림 2]은 CASA의 구조를 나타내고 있다. 다양한 센서로부터 여러 상황 정보들을 수집하고, 사용자가 리소스에 대해 접근을 요청하게 되면 허가 요청이 허가 서비스(Authorization Service)에게 전해지고 여러 상황 정보를 바탕으로 인증과 허가 서비스를 행하게 된다.

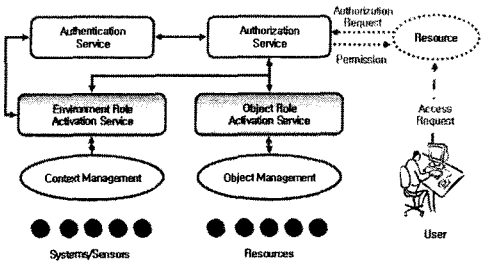

그림 2. CASA의 구조
Fig 2. A Structure of CASA

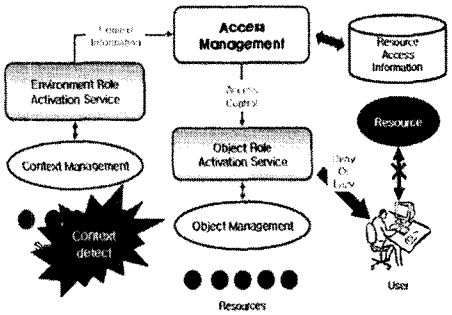

그림 3. 리소스의 동적 접근 제어를 하는 D-CASA 구조도
Fig 3. D-CASA Structure for Dynamic Access Control of Resources

본 논문은 기존 CASA에서 상황 정보로 사용되는 사용자 ID, 시간 그리고 장소뿐만 아니라 사용자의 주변 환경 정보를 리소스 접근 제어의 요소로 적용한다. 간단하게 시나리오를 살펴 보면, 일정 장소에 접근이 가능한 상위 권한자(상위 권한을 가진 사용자)와 하위 권한자가 있다고 가정한다. 상위 권한자가 상위 레벨의 리소스를 접근 중일 경우에 상위 레벨의 리소스에 대한 접근 권한을 가지지 못한 하위 권한자가 해당 장소에 들어 오게 되는 경우에 적용된다. 리소스 관리자는 하위 권한자의 등장을 상위 권한자에게 알려주게 되고, 하위 권한자의 간접적인 리소스 접근을 방지하도록 경고 메시지를 알려주거나 상위 권한자의 리소스 접근을 막아 뜻하지 않은 하위 권한자의 리소스 접근을 봉쇄하도록 한다. 또한, 소리 또는 비전 정보를 통해 권한자의 리소스 사용에 집중도가 떨어지는 주위 환경의 발생시 리소스 접근을 늦추어 잘못된 입력을 미리 방지하는 기법을 생각해 볼 수도 있다. 즉, CASA의 리소스 접근 기법에 적용되는 상황 인식 정보 중에서 주위 환경 정보인 ERoles (Environment Role)을 여러 가지 요소로 확장시켜 리소스 접근에 대한 동적 제어를 하고자 한다.

위의 시나리오 처리 과정은 [그림 3]에서 보는 바와 같이, 주위 환경에 대한 상황이 인식되면 Environment Role Activation Service에 의해 번역된 상황 정보를 접근 제어자에게 통보하고 리소스에 대한 접근 정보를 저장하고 있는 내용을 토대로 리소스 접근에 대한 제어 정보를 생성한다. 만약 이 때 접근 제어가 필요한 상황으로 인식되면 상위 권한자에게 경고 메시지 또는 리소스 차단을 지시하게 된다.

$$\text{Authenticated(Alice)} \quad \cdots\cdots (3.1)$$

$$\text{CanAccess(Alice, V)} \quad \cdots\cdots (3.2)$$

$$\text{Location(Alice, In, Room407)} \cap \text{Activity(Alice, V)} \cap \exists_{people} \text{ x Location(x, In, Room407)}$$
$$\text{-> NOT Access(Alice, V)} \quad \cdots\cdots (3.3)$$

위 식은 Resource Access Information이 주변 상황 정보에 따라 변화됨을 보인다. 식(3.1)과 식(3.2)는 Alice가 V라는 리소스에 접근 권한을 가지고 있음을 나타내고, V라는 리소스는 Alice외에 누구에게도 접근이 허용되어서는 안 된다. 실시간 상황 인지 모듈에 의해 Alice각 리소스 V를 사용하고 있는 장소에 누군가가 들어온다면 Alice의 리소스 접근을 제한하게 된다. 식(3.3)은 Alice가 Room407호에 위치하고 있고, 리소스 V에 대해서 권한을 행사하고 있을때, Room407에 누군가가 들어온다면 Alice는 V를 접근할 수 없음을 나타낸다.

기존의 CASA는 GRBAC을 적용하여 사용자에 대한 정보와 제한적인 상황 정보를 바탕으로 권한이나 서비스를 부여하였다. 그러나 본 논문에서의 제안 모델은 권한을 가진 사용자의 서비스일지라도 주변의 환경 정보가 해당 서비스를 제공해서는 안 되는 상황이 발생하게 되면 접근 권한이나 서비스를 중지하게 된다. 즉, 권한을 가진 사용자가 서비스를 받는 도중에 서비스에 대한 정보 노출 가능성을 줄이고자 한다.

기존의 CASA에서는 Authorization Service 모듈이 리소스 접근 권한을 결정하게 된다. 사용자에게 접근 권한을 부여하기 전에 Environment Role activation Service와 Object Role Activation Service 모듈에서 사용자에 대한 리소스의 사용 권한이 있는지를 검사한 후에 리소스 접근 권

한을 부여하게 된다. 반면에, 본 논문은 접근 관리 모듈(Access Management)에서 사용자의 리소스 접근 권한을 부여 받았다 할지라도 상황 인지 모듈(Context Management)에서 새로운 상황이 인지 되면 Environment Role activation Service을 통하여 상황 정보를 번역하여 전달하고, 전달받은 상황 정보를 바탕으로 Object Role Activation Service에게 접근 제어 여부를 전달하여 해당 리소스나 사용자에게 변화된 접근 권한을 적용하게 된다.

기존의 사용자 인증만으로 권한을 부여 받았던 방법과는 달리 실시간으로 인지되는 상황 정보를 바탕으로 권한을 달리 설정하게 됨으로 기존 CASA보다는 더욱 동적으로 권한 부여를 하게 된다. 따라서, 이미 인증 받은 사용자라 할지라도 상황 정보에 따라서는 권한을 달리 부여 받게 됨으로 리소스의 보안을 더욱 강인하게 할 수 있다고 본다.

상황 인식 접근 제어(Context-Aware Access control)를 위한 상황 인지 요소에 기존의 사용자 ID, 시간, 장소에 대한 정보 외에, 현 사용자가 있는 장소의 주위 정보를 실시간으로 추가한다. 이러한 방식은 접근 가능한 사용자가 접근을 요청하는 경우에 주위의 환경에 따라 리소스 접근을 제한받게 된다. 즉 리소스 접근 권한을 가진 사용자가 인증을 받아 리소스를 사용하고 있는 경우에 접근 권한이 없는 사용자가 같은 장소에 들어오는 경우나 리소스 사용에 대해 제약을 받는 환경 정보가 발생되면 접근 권한을 가지고 리소스를 사용중인 사용자라 할지라도 제한을 하게 된다. 이와 같이 모든 주위 환경 정보를 실시간으로 받아서 리소스 접근을 제어함으로 리소스에 대한 보안을 더욱 강화시킬 수 있다고 본다. 리소스 접근 정보(Resource Access Information)는 리소스에 대한 접근 정보나 접근 레벨을 저장하여 실시간 상황 정보와 이미 저장되어 있는 접근 정보를 바탕으로 해당 리소스 접근 여부를 판단하게 된다.

Ⅳ. 비교 분석

본 장에서는 기존의 상황 인식 서비스 인프라와 제안 모델을 상황 인식 서비스에 필수적인 요구 기술[2]를 바탕으로 비교한다. 상황 인식 서비스에서의 필수 요구 기술로는 상황 정보를 센싱하는 기술에서부터 상황 정보를 추론하는 기술까지 8가지 정도로 구분해서 살펴볼 수 있다.

가장 먼저 Active Badge나 RFID와 같이 상황 정보를 센싱하는 기술이 필수적이고, 이러한 상황정보가 변화될 때 변화된 정보를 바로 수신할 것인지 특정 조건을 만족할 때만 수신할 것인지를 고려해서 센싱하는 기술이 요구된다. Gaia와 SOCAM의 경우에는 센싱하고 있는 상황 정보만을 고려하고, 그 외의 정보에 대해서는 기존의 DB의 보유 정보에만 의지하여 서비스 제공 여부를 추론하여 결정된다. 상황 정보 모델링 기술은 개발자가 다양한 하드웨어 장치와 인터페이스 하는 부담을 줄일 수 있도록 센서의 추상화를 제공하고, SGML이나 OWL을 이용하여 상황정보의 교환을 위한 표준 모델링 기술이 제공되어야 한다. 상황 정보 융합 및 추론 기술은 다양한 센싱 데이터를 융합하여 적절한 상황 정보를 유도할 수 있는 지능적인 추론 방법이다. 상황정보 교환 기술은 센서, 엑추에이터 그리고 객체와의 상호 작용을 위한 통신 메커니즘이 필요하다. 상황 인식 서비스 묘사 및 발견 기술은 XML을 이용하는 WSDL처럼 서비스를 하기 위한 적절한 묘사방법과 ACAN[9]에서 USA와 SAMA를 이용한 것처럼 필요한 서비스를 찾을 수 있는 기술이 필요하다. 마지막으로 상황인식 서비스 구조 기술은 센서나 서비스, 장치 등이 다른 구성 요소에 영향을 주지 않고 독립적이고 동적으로 추가될 수 있는 기술이 필요하다.

[표 1]에서 보는 바와 같이, 모든 상황 인식 서비스 인프라는 상황 정보를 센싱한 후에 적절한 서비스를 제공하기 위해 추론이나 정보 융합을 한다. 반면에, 상황 정보가 변화되는 경우를 보면, 다른 모델에 비해 CASA는 변화되는 정보가 수시로 적용되어 서비스를 받는 상황 인식 정보가 가장 최근 정보가 적용된다. 또한 확장된 CASA의 경우에는 상황 정보 융합 및 추론하는 경우에 GRBAC을 사용함으로 기존의 사용자의 ID만을 고려하는 경우와 다르게 여러 주변 환경 정보에 따라 서비스를 받을 수 있다. 기존의 CASA에서는 위치와 시간 정보만을 환경 정보로 고려하였으나, 확장된 CASA의 경우에는 사용자의 사용 시간, 서비스를 받고 있는 장소의 주변 환경 정보를 실시간으로 반영하여 접근 제어를 결정한다.

본 제안 모델은 권한의 보유 유무와 상관 없이 서비스를 받는 상황의 주변 정보를 고려하여 리소스의 접근 제어와 서비스를 제공하는 방식으로 동적인 리소스 접근 방식을 제안하였다. 또한 동적인 리소스 접근 방식을 사용함으로써 보유한 정보에 대한 노출의 가능성을 줄일 수 있다.

〔표 1〕 각 모델 별 상황 인식 필수 요구 기술 비교
〔Table 1〕 The Comparision of Mechanism for Context Aware

요구 기술	Gaia	SOCAM	CASA	D-CASA
상황정보 센싱	Active Badge	GPS receiver	생체인식 Active Badge	생체인식 Active Badge
상황정보 변화 센싱	-	-	GPDL	GPDL
상황정보 모델링	OWL	4-ary predicate	XML	XML
상황정보 융합 및 추론	Context Service Module	RDFS reasonor OWL reasonor	GRBAC	GRBAC
상황정보 교환	SOAP, RMI	OSGi	HTTP over SSL	HTTP over SSL
상황정보 툴킷	CTTK	Jena2	CTTK	CTTK
상황 인식 서비스 묘사 및 발견	LuaOrb	OWL	XML	XML
정보 노출 가능성	High	High	High	Medium

〔표 2〕 보안 관련 기술 모듈
〔Table 2〕 Security Related Module

	보안 관련 모듈
Gaia	User Information DB
SOCAM	User Information DB
CASA	Authentication Service Authorization Service Resource DB
D-CASA	Access Management Module Resource Access Information DB

상황 인식 서비스 인프라의 보안 관련 모듈을 비교해보면 〔표 2〕와 같이 Gaia와 SOCAM은 DB에 등록되어 사용자 정보만을 이용하는 형식이고, CASA는 인증 및 허가 서비스 모듈을 사용하여 리소스에 대한 접근 관리를 한다. 반면에 본 제안 모델은 주변 환경 정보에 변화에 따른 접근 관리 모듈의 동적인 권한 관리나 동적으로 서비스 제공 여부를 판단하게 함으로써 권한을 가진 사용자에 대해서도 주변 환경 정보를 고려하여 보안 레벨을 다르게 적용할 수 있다. 이는 기존의 상황 인식 서비스 인프라와 달리 보유하고 있는 DB에만 의존하지 않는다는 장점을 가진다. 기존의 CASA에서 보안 관련 모듈들을 Access Management Module와 Resource Access Information DB에서 통합 관리하고 상황 인지에 따른 권한 제어를 Access Management Module에 추가하였다.

V. 결론 및 향후 연구 과제

기존의 상황 인지 구조에서는 이미 정해져 있는 상황 정보를 바탕으로 사용자에게 권한을 부여하는 방식의 접근 제어 기법을 사용하였다. 이는 이미 권한을 부여받는 사용자가 주변 상황에 따라 권한의 행사 여부를 달리 해야 하는 경우를 고려하지 않는다고 본다.

이에, 본 논문에서는 이미 권한을 가진 사용자가 서비스를 받고 있는 중일지라도 권한을 가지지 못한 사용자나 주변 상황이 해당 서비스를 제공해서는 안 되는 경우에 해당 사용자의 권한도 강제적으로 제한함으로 보안적인 면을 더욱 강화하였다. 즉, 권한을 가진 사용자가 권한을 행사하는 주변 환경 정보를 실시간으로 인지하여 권한를 행사하기에 적합하지 않은 상황인 경우, 즉 해당 리소스에 대한 접근 권한이 없는 사용자가 주변에 있거나 권한을 가진 사용자라 할지라도 시간상 권한 행사를 할 수 없는 환경이 경우에는 접근 제어를 제한한다.

본 논문에서 제안한 모델을 사용하기에 앞서 접근 제한이 필요한 주위 환경 정보를 어떻게 수집할 것인가 하는 문제의 해결이 선행되어야 할 것이다. 또한 기존의 사용자 인증 절차 방식을 그대로 적용을 하는 경우에는 매번 상황 정보의 변경으로 인한 더욱 잦은 인증 절차가 이루어지게 된다. 이를 보완하기 위한 사용자 인증 절차상의 간소화가 필요하다고 본다.

참고문헌

[1] Mark Weiser, "The computer for the 21st century", Scientific American, Sep, 1991.

[2] 김재호, 신경철, "상황인식 서비스 기술 연구 동향", ITFIND, 주간기술동향, 12.29, 2004.

[3] 김재호, 배정숙, 김성희, "차세대 이동통신망에서 상황인식 서비스" 전자 통신 동향 분석, 제19권 제3호 2004.6.

[4] Michael J.Covington, Matthew J. Moyer and Mustaque Ahamad, "Generalized role-based access control for securing future application", NISSC, pp 40-51, Oct 2000

[5] Dey, A.K, Salber, D, and Abowad, G. D, "A Context-aware Infrastructure for Smart Environments", MANSE'99, pp 114-128, Dec, 1999

[6] Paul Castro, "Managing Context Data for smart Spaces", IEEE Personal Communications, October 2000.

[7] Anind K. Dey, Gregory D. Abowd, and Daniel Salber, "A Context-Based Infrastructure for Smart Environment," In st International Workshop on Managing Interactions in Smart Environments (MANSE '99), 1999

[8] Michael J.Covington, Prahlad Fogla, Zhiyuan Zhan, and Mustaque Ahamad, "Context-aware Security Architecture for Emerging Applications", Security Application Conference(ACSAC), 2002

[9] M. Khedr, and A. Karmouch, "ACAN-Ad hoc Context. Aware Network", Proc. Canadian Conference On. Electrical & Computer Engineering (CCECE'02), Winnipeg,Canada,May12-15,2002.

[10] Jalal Al-Muhtadi, Anand Ranganathan, Roy H. Campbell, M. Dennis Mickunas, "Cerberus: A Context-Aware Security Scheme for Smart Spaces", PerCom 2003.

[11] Pierre-Guillaume Raverdy, Oriana Riva, Agnès de La Chapelle, Rafik Chibout, Valérie Issarny, Efficient Context-aware Service Discovery in Multi-Protocol Pervasive Environments. MDM 2006.

저자소개

김 경 자

2004년 8월 : 동국대학교 컴퓨터공학박사

2005년3월 ~ 2008년.2월 : 세종대학교 컴퓨터공학과 초빙교수

관심분야 : MANET, 라우팅 프로토콜, MAC 프로토콜

장 태 무

1995년2월: 서울대학교 전산기공학 박사

1981년3월 ~ 현재: 동국대학교 컴퓨터공학과 교수

관심분야: 컴퓨터구조, 병렬/분산처리, Power-aware computing