Journal of Digital Contents Society Vol. 7 No. 4 Dec. 2006(pp. 301-308)

유비쿼터스 센싱 네트워크 환경 하에서 정보 프라이버시의 보호 기술과 영역에 관한 연구 (상황인식시스템과 개인정보를 중심으로)

강장묵*, 방기천**

요 약

유비쿼터스 시대를 앞당길 기술로는 USN, RFID, Homenetwork 등이 있다. 이와 같은 기술들은 상황 인식 시스템을 구현하게 된다. 상황을 인식한다는 것은 사람, 사물, 환경이 실시간으로 정보를 유선 및 무선으로 제공할 수 있는 환경을 뜻한다. 따라서 개인정보, 정보 프라이버시, 광의의 프라이버시가 심각한 위협에 직면할 것이다. 본 연구는 USN 환경 하에서 상황 인식 시스템이 가지고 있는 개인정보의 위협을 분석하고 이를 보호할 수 있는 기술들을 제시하였다. 각 기술들은 보호의 영역들을 세분화 시킨 정보 프라이버시에 적용할 수 있는 기술들이다. 본 연구를 통하여 정보 프라이버시의 개념적 재해석과 기술적 제시를 통한 통찰력과 종합적 해결 방안을 기대해본다.

A study on protection technology and scope about information Privacy in ubiquitous Sensing Network Environment (A focus on context awareness system and personal information)

Jang-Mook Kang*, Kee-Chun Bang**

Abstract

There are some technologies such as USN, RFID, Home-network to advance the ubiquitous era. Those technologies embody Context-Awareness System. To Context-Awareness System is that human, objects and environment supply information with cable and wireless at real time. So private information, information privacy, a wide sense privacy will be faced on serious menace. In this article, I analyze threat of private information in Context-Awareness System under USN(ubiquitous Sensing Network) surroundings and present technology to protect private information. Each technology can apply subdivided protection province information privacy. I expect definition of information privacy, insight through technological presentation and total solution in this article.

Keywords : Personal information control, Ubiquitous networking, Context awareness system, Privacy, Information privacy

1. 서론

유비쿼터스 센싱 네트워트(USN : Ubiquitous Sensing Network, 이하 USN으로 표기함)는 정보통신부에서 주도적으로 추진하고 있는 우리나라의 정보화 프로젝트의 일환이다. 오늘날 RFID 등의 센싱(sensing) 칩을 활용하여 국토를 살아있는 유기체로 전환하는 USN 환경은 산업 및 사회에 미칠 정보화의 순기능 외에 역기능도 클 것으로 예상되고 있다. 따라서 유비쿼터스화의 첨병으로 역할을 할 USN 환경에서 개인정보는 이동하는 가장 취약하면서도 중요한 데이터가 될 전망이며, 동시에 증강된 현실이 투영된 정보로 부가가치를 창출하는 원동력이 될 것이다. 이러한 USN 환경은 정보인권, 특히 프라이버시와 전자공간을 이동하는 식별정보인 개인정보에 대

※ 제일저자(First Author) : 강장묵
접수일자:2006년09월20일, 심사완료:2006년11월03일
* 세종대학교 컴퓨터공학과 교수
redsea@sejong.ac.kr
** 남서울대학교 멀티미디어학과 교수

한 커다란 위협으로 다가오고 있다.

하지만 정보인권은 정보기술의 발전과 함께 태동한 까닭에 다른 권리 및 개념들에 비하여 일천한 역사를 가지고 있으며 정보기술의 발전과 함께 끊임없이 발전하고 있는 개념이어서 정확한 이해가 확립되지 못한 실정이다. 따라서 아날로그 시대에서 디지털 시대 그리고 유비쿼터스 컴퓨팅 시대로 진입하면서 정보인권의 개념과 보호 영역이 발전하고 있으며 이에 대한 명확한 이해가 요구된다[1]. 본 연구에서는 발전중에 있는 정보인권의 개념 중에서 정보 프라이버시에 대한 이해과 범위를 유비쿼터스 컴퓨팅 기술의 특징인 이동성과 내재성이 구현된 상황인식시스템을 중심으로 분석하여 살펴보았다.

특히 정보 프라이버시에서 주로 다루는 개인정보, 개인정보통제권 그리고 정보프라이버시에 대한 범위와 내용을 상황인식서비스가 가능하도록 구현할 RFID 시스템 환경을 중심으로 분석해 봄으로 정보 프라이버시(Information Privacy)에 관한 범위와 정의를 명확히 할 수 있는데 의의가 있다고 사료된다. 더불어 기술적인 보호방안으로 어떻게 개인정보를 USN 환경에서 보호할 수 있는지를 소개하고 각 기술의 개인정보 보호의 정도에 따라 선택적으로 사용할 수 있는데 도움을 줄 것으로 예상된다.

2. 이론적 고찰

2.1 상황인식시스템과 정보인권

2.1.1 유비쿼터스 컴퓨팅과 상황인식시스템

사용자가 처한 환경에서 사용자의 현재 위치, 행동, 작업, 감정 상태 등을 객체(object)로 나타낼 수 있으며, 사용자나 사용자의 객체에 대한 정보 값과 그 정보들의 변화를 상황(context)이라고 표현할 수 있다[2]. 이러한 상황 정보를 사용자의 환경으로부터 얻어내는 과정을 상황인식이라 하며 상황인식을 위한 다양한 지원환경을 상황인식시스템(context awareness system)이라고 한다.

상황인식기술은 편재된 센서 및 컴퓨터 칩들로부터 수집된 정보를 효과적으로 처리, 공유, 명령에 대한 요청, 이동, 저장 등을 가능하게 하는 기술이다. 즉 상황 관리 기술로 정보수집, 처리, 통신 등을 제공하는 컴퓨터들이 기능적으로 공간적으로 연결되어 사용자에게 필요한 정보를 제공하기 위하여 다양한 형태의 자료를 처리하기 위한 기술들을 의미한다[3]. 상황인식에 기반한 다중 명령 및 자동 변환 등의 기능은 사용자가 원하는 정보를 어디에서든지(anywhere), 언제든지(anytme) 얻을 수 있는 유비쿼터스 컴퓨팅 환경을 특징짓는 요소가 되며, RFID는 상황인식을 구현하는 주요한 기술 중 하나이다.

이와 같이 상황인식시스템은 커다란 의미로 유비쿼터스 컴퓨팅 기술의 일부분이다. 하지만 유비쿼터스 컴퓨팅과 상황인식시스템의 기술 및 적용은 아래 <표 1>와 같은 차이점이 있다. 즉, 유비쿼터스 컴퓨팅이란 컴퓨팅 통신, 접속방식, 제공하는 콘텐츠 및 사람이 컴퓨터의 존재를 인지하지 않도록 조용히 처리하는 특성(5C : Computing, Communication, Connectivity, Contents, Calm)을 이용하여 언제 어디서나 어떠한 형태의 네트워크에서도 모든 다른 기종 기기 간의 연동을 통하여 다양한 서비스를 제공하는 것(5ANY : Anytime, Anywhere, Any Network, Any Device, Any Service)을 지향하고 있으나, 상황인식 시스템은 이를 구현하는 수단과 과정에 차이를 보여주고 있다. 따라서 상황 인식 시스템과 유비쿼터스 컴퓨팅은 궁극적으로 인터넷 기반의 근거리 무선 통신 인터페이스가 장착된 지능형 단말 기능을 제공하는 스마트 오브젝트(smart object), 능동형 및 수동형 센서, 스마트 스페이스(smart space), 스마트 라이프(smart life)를 실현하기 위한 기술 요소 간의 유기적 결합과 융합을 통해 가능하다.

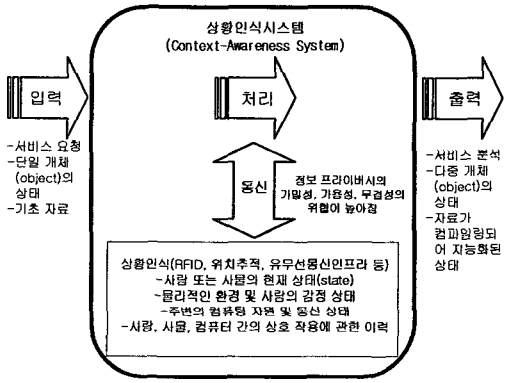
<표 1> 유비쿼터스 컴퓨팅과 상황인식 시스템의 비교[4]

구분	유비쿼터스 컴퓨팅	상황인식시스템
기술의 정의	물리공간(제1공간)과 가상공간(제2공간)을 연결하는 증강된 공간(제3공간)을 통한 컴퓨터, 네트워크 및 인간을 조화시킬 수 있는 차세대 컴퓨팅 기술	물리공간과 가상공간을 연결하여 현실의 상황을 정보화 하고 이를 활용하여 사용자 중심의 지능화된 서비스를 제공하는 기술
기술의 특징	주변의 모든 물체 안에 컴퓨터(마이크로 프로세서)가 내장되어 물체 간 그리고 물체와 인간 간의 효과적인 정보 교환 및 활용이 가능하게 하는 기술	현실 세계의 모든 상황을 표현하는 기술적 수단을 제시하며, 이를 기반으로 상황 인식 상황 중 특징 추출, 학습, 추론 등의 지능화된 기법을 적용 인간 중심의 자율적인 서비스를 가능하게 하는 기술

분야별기술	단말기술	SoC 오감인터페이스, 유기 EL, 초소형 칩 기술, 저전력-저소모 기술	복합형 지능 단말 기술(유무선 네트워크 연동, 센서 네트워크 연동, 음성 및 입력 인터페이스 기술)
	시스템 기술	Web 서비스 기술, 실시간 운영 체제 기술, 제어/관리 기술, 센싱 기술, 데이터 그리드 기술, 내장형 S/W 기술	내장형 S/W 기술, Web 서비스 기술, 센싱 기술, 그리드 컴퓨팅 기술
	플랫폼 기술	스마트 카드, 보안, 통합 인증, 생체 인식 기반 인증	센서 네트워킹 플랫폼, 상황인식 공통 플랫폼, 지능형 에이전트 플랫폼
	애플리케이션 기술	에이전트(검색, 협상, 추출) 멀티미디어 저장, 추출 및 분리 기술, (음성, 화상, 이미지) 인식 기술	지능형 에이전트(특징 추출, 학습, 추론)
	인공지능 기술	추론 엔진 기술, 학습, 규칙 엔진 기술	특징 추출, 추론 엔진 기술, 학습, 규칙 엔진 기술
	개발환경 기술	개발도구기술	개발도구기술

2.1.2 상황인식시스템과 정보인권

정보인권이란 헌법상 보장된 기존의 인권개념을 정보화시대의 특성에 맞추어 확대·발전시킨 것이라 할 수 있으며, 정보인권에서 다루는 정보보호란 진정한 의미의 개인정보통제권의 보장을 지향하는 '정보의 자유(Freedom of information)'라 사료된다[5]. 따라서 정보인권에서 고려해볼 수 있는 정보보호를 위한 구체적인 보호 권리로는 일반적으로 정보통제권, 정보접근권, 정보공유권, 역감시권 등을 들 수 있다. 여기서 정보보호란 정보화에 따른 정보인권에 있어서의 역기능을 최소화하고 정보화의 순기능을 극대화하는 데 그 목적이 있다. 또한 정보인권에서 정보보호를 이루기 위한 해결 방안으로는 정보에 대한 자기정보통제권을 효과적으로 실현할 수 있도록 암호학 및 보안 알고리즘에 의한 기술적 해결방안과 보안정책, 법 등 제도적 해결방안 그리고 정보윤리 등을 통한 자발적 해결방안을 들 수 있다. 상황인식시스템에서 상황이란 "사용자가 처한 현재의 위치, 사용자의 작업 상태 및 주변 환경 인식 그리고 감정 및 사용자 상태의 변화 등을 객체(object)로 표현하고 사용자나 사용자의 객체에 대한 정보 값과 정보들의 변환 값"을 의미한다[6]. 따라서 상황인식시스템은 필연적으로 특정 개인이 현재 처한 주변 여건과 더 나아가 개인의 감정 상태까지 감지할 수 있는 기술이다. 즉 상황인식의 응용은 다양한 분야에서 활용될 전망인데 특정 개인에 대한 상태, 물리적인 환경, 주변 컴퓨팅 자원의 상태, 기존 정보를 통한 분석 등의 상황정보를 통해 개인의 상황에 맞는 결과 값을 제공하는 것이다[7]. 즉 아래 (그림 1)와 같이 상황 인식 처리를 위해 필수적인 요소로 상황탐지(context detection), 상황 표현 및 데이터베이스 저장 기술, 관련성 있는 상황의 검색 및 선택 기술, 상황에 기반 한 개인화된 서비스 자동 실행 기술 등이 요구되어진다.



(그림 1) 상황인식 시스템의 정보이동[8]

결국 이와 같은 고도의 기술을 구현하기 위해서는 개인정보는 빠르게 수집되어야 하며 실시간으로 최신화될 것이며 중앙 서버의 유사한 상황 및 정보와 비교하기 위한 개인정보의 이동과 저장 등이 이루어져야 할 것이다.

2.2 정보 프라이버시와 개인정보의 이해

2.2.1 정보 프라이버시와 개인정보의 이해

1995년 미국 행정부의 국가정보화추진위원회(Information Infrastructure Task Force, IITF)에서 제시한 개인정보보호원칙(principles for providing and using personal information)에서 처음 사용한 용어가 정보 프라이버시이다[9]. 그 후 정보 프라이버시(information privacy)란 자기 자신의 재산에 대한 권리 행사(개인정보통제권)의 관점에서 자신의 개인정보에 대한 배타적 통제권을 가질 권리로 발전하였다[10]. 따라서 다른 사람이나 혹은 다른 기관에 제공된 자신에 관한 개인정보의 유통과 활용과정에 관여

할 수 있는 권리를 포함하는 것으로 이해된다. 따라서 개인정보가 개인정보를 수집하고 활용하는 기업에게 경제적인 이익을 향유하게 한다는 측면에서 개인정보에 대한 재산권적 배타적 권리를 부여함으로 스스로 자신의 개인정보를 관리할 수 있도록 보호해주어야 한다는 필요성이 강조된 결과였다. 즉 타인으로부터 감시당하지 않을 권리와 함께 감시당하지 않음을 보장하기 위하여 국가나 제 3자의 자신에 대한 정보 수집 활동과 내용 그리고 이용을 감시할 수 있는 권리이다[11].

개인정보(personal information)란 개인을 특정할 수 있는 모든 정보라고 할 수 있다. 여기서 개인정보는 단순한 원시자료(data)라 할지라도 컴파일링되었을 때 개인을 식별할 수 있는 위험성이 있는 모든 정보라고 할 수 있다. 예를 들면 우리나라와 같이 주민등록번호로 모든 국민을 식별할 수 있는 주민제도를 가진 국가에서는 주민등록번호를 중심으로 관련 정보가 쉽게 컴파일링될 수 있다는 측면에서 개인정보침해의 위험이 높다고 볼 수 있다. 따라서 디지털화된 공간에서 여러 사람에게 동시에 실시간으로 이용될 수 있는 정보의 위험성을 인식하게 되면서 개인정보를 강조하는 개념으로 제시된 개념이 정보 프라이버시라고 사료된다. 즉 정보 프라이버시는 개인정보 소유자의 개인 정보에 대한 통제권 측면에서 개인정보를 강조하기 위해 사용된 개념이다. 따라서 정보 프라이버시란 전통적인 프라이버시의 개념을 전제로 하면서 세부적인 범주에서 '정보(information)' 또는 '자료(data)'까지 포함한다는 측면에서 '개인정보'가 핵심적인 요소라 할 수 있다.

2.2.2 USN 환경에서의 정보 프라이버시

정보 프라이버시란 기존의 사생활 보호(주거침입으로부터 홀로 있을 권리, 황색 저널리즘에 의해 세간의 가십거리가 되지 않을 권리 등), 통신 프라이버시(전화 등을 도청당하지 않고 안심하고 할 수 있는 권리 등)의 개념을 전제로 하되 기존의 사생활과 통신에서의 프라이버시 보호에서 더 나아가 인터넷 공간에 이동하는 정보에 대한 개인정보통제권이라는 적극적인 성격으로 발전되어 도출된 개념이라 사료된다. 따라서 정보 프라이버시는 주로 인터넷 공간에 이동하는 개인정보에 대한 프라이버시 보호라는 측면에서 이해되었다. 즉 기존의 아날로그 공간인 물리공간에서의 침입으로부터 보호받고자 하는 프라이버시, 유무선 전화 등에 대한 통신 프라이버시와 구분되는 가상공간인 인터넷에서의 프라이버시로 이해된 것이다. 하지만 USN 환경은 MEMS 기술에 의한 초소형 칩 설계 기술의 발달로 컴퓨팅 칩의 내재성이 높아지고, RFID기술에 의한 이동성의 극대화를 통한 끊김없는 네트워킹을 가능하게 함으로 물리공간으로 침투하는 가상공간을 생성한다. 즉 물리 공간 속에 RFID 등을 중심으로 한 USN 환경을 구성함으로 물리공간과 가상공간이 끊김없이 실시간으로 연결되어 제3공간(유비쿼터스 공간)이 만들어진다. 이 제3공간은 상황인식시스템을 통해 구체화될 것이다. 따라서 인터넷 공간으로 대표되는 디지털 공간의 개인정보에 대한 프라이버시 보호는 결국 물리공간까지 연계되는 프라이버시 보호로 확대되어질 것이다. 그것은 개인 정보가 물리공간으로 침투되고 확대되는 것을 의미한다.

따라서 USN 환경에서는 정보 프라이버시가 인터넷의 개인정보 보호에서 물리공간의 사생활 보호, 유무선 전화와 전자메일 등에 관한 통신 보호를 포함하게 될 것이다.

3. 상황인식시스템 환경 하에서 정보 프라이버시의 영역과 보호기술

3.1 USN 환경을 고려한 정보 프라이버시의 세부 보호 영역

3.1.1 확장된 정보 프라이버시의 보호 영역 및 세부내용

과거에는 물리공간에서의 프라이버시 침해와 정보프라이버시와는 무관하였다. 물리공간인 자택에서 편안한 시간을 보낼 수 있는 자유 등이 오늘날에는 다양한 foreground 장치(전자 감시 장비)와 전자 감시 장비와 실시간으로 연동되어 처리되는 background 장치(인터넷 서버 등)의 이용으로 물리공간은 인터넷공간에 기록되고 저장되며 분석된 후 다른 시스템으로 이동할 수 있다. 이때 다루어지는 모든 내용은 개인정보이

며 개인은 자신의 정보가 누구에 의해 열람, 수정, 저장, 이동, 삭제되는지를 알아야 한다는 적극적인 권리가 개인정보통제권이기 때문이다. 따라서 USN 환경에서는 기존의 정보 프라이버시가 확장되어 물리 공간, 유·무선 통신 공간, 가상공간, 물리공간이 확장된 유비쿼터스 공간으로 프라이버시의 보호 영역과 세부 내용이 확장되어야 한다. 아래 <표 2>는 정보프라이버시에 대한 세부적인 내용을 기술한 것이다.

<표 2> USN 환경을 고려한 정보프라이버시 분류[14]

	프라이버시의 대분류	세부 내용	비고
정보프라이버시	물리공간에서의 정보프라이버시	CCTV - 개인 : 아파트 등 공동 주거 공간 - 기업 : 공장 등 생산현장 또는 상가 등 상업지구 -국가 : 범죄예방 등을 위한 거리에 설치, 국가 시설물 등의 안전을 위한 설치 생체인증기술 및 각 침해주체에서 운영할 수 있는 몰래카메라	물리공간에서 수집된 정보는 RFID 등 통신기술을 통해 실시간으로 연계된 가상 공간에서 새로운 정보로 재생산됨
	유·무선 중심의 정보프라이버시	유선 전화기 FAX 이동 전화 (통화내용 및 단문 서비스) 전자 우편 MSN 등	유선 전화기의 경우 1990년도까지 프라이버시 주요 이슈 및 보호 영역
	인터넷 중심의 정보프라이버시	사생활 침해 사생활 공표(디지털 카메라 등으로 찍은 사진을 공표함) 허위 공표 성명 및 개인식별 정보의 영리적 이용 (주민등록정보, 신용카드정보)	

3.1.2 개인정보관리 주체를 중심으로 살펴본 세부내용

개인정보의 당사자는 국가, 기업, 개인을 상대로 자신의 개인정보가 어떻게 수집, 수정, 저장, 이동되는지에 대해 통보받고 알아야한다는 측면에서 개인정보의 세부내용을 살펴본다.

첫째, 국가는 범죄수사 등을 위한 지문, 유전자 정보, 국가신분등록제도(주민등록제도, 호적제도), 방범 등을 목적으로 한 CCTV, 차량 운행, 기상, 주요 시설물 관리 등을 위한 CCTV, 적법절차에 의한 감청 등의 개인정보를 관리한다.

둘째, 기업은 기업 내 직원에 대한 프라이버시 관련 개인정보를 관리하거나 기업 외부의 고객에 대한 프라이버시 관련 개인정보를 관리한다. 기업 내부의 직원에 관한 내용으로는 CCTV 카메라 설치, 상황인식의 최초 시도였던 Olivetti 사의 액티브 뱃지(active badge)[13] 등과 같은 전자뱃지(유비쿼터스 컴퓨팅 환경에서 Auto-ID 프로젝트 등), 전사적 자원 관리(ERP), 전화 송수신 기록, 컴퓨터보안관리 시스템 구축한 사업장(하드디스크 내용 검사, 인터넷 감시(특정 홈페이지 방문 차단), 특정 전자우편 이용 차단, 전자우편 이용 기술 통제), 물리적 보안 시스템 구축한 사업장(CCTV, IC카드, 홍채, 정맥, 지문인식 등) 등을 통해 개인정보를 관리한다. 기업 외부의 일반 고객에 대한 프라이버시 관련 개인정보로는 스팸, 정크, 광고성 메일 또는 이동전화 단문서비스 등을 통해 얻은 정보, 인터넷에서 로봇, 스크립트, 쿠키 등을 사용한 정보 수집 및 마케팅 도구에 의한 컴파일링 정보 등이 있다.

셋째, 개인에 의해 관리되어지는 개인정보로는 친구, 인척, 회사 동료, 지인 등에 관련된 신상정보, 이동전화 등에 기록되어 관리되는 개인정보 등이 있다.

3.2 상황인식시스템 보안위협과 보호기술

3.2.1 상황인식시스템의 보안 위협

상황인식시스템 환경에서 보안을 위협하는 공격 기술은 어떤 것이 있는지 살펴보면 아래와 같다. 상황인식시스템 환경은 무선 통신을 기본으로 기기들 간에 통신을 하게 된다. 따라서 상황인식시스템 환경에서 발생할 수 있는 위협으로는 RFID 시스템 장치(리더 장치, 태그 등)의 절도 및 분실, IP 스푸핑(Spoofing), Dos(Denial of Service) 공격, Rogue AP, 트로이 목마, Worm, 바이러스, 신호방해 공격, 배터리 소진

공격 등에 취약 할 수 있다. 이런 유형의 위협은 결국 데이터 보안이 취약할 경우 기존의 컴퓨팅 환경보다 심각한 문제를 발생시킬 수 있음과 한 번 수집된 데이터가 오·남용되어 원하지 않는 사람에게 전파되거나 이용될 경우, 사회 전체의 심각한 개인정보 유출 문제를 유발할 수 있음을 시사한다. 따라서 위험의 규모가 폭발적으로 증대되었으며 한번 유출된 상황인식정보는 유비쿼터스 컴퓨팅 공간에서 회수할 수 없기 때문에 더욱 큰 문제에 봉착할 것이다. 이러한 개인정보의 위협은 상황인식시스템의 활성화에 커다란 걸림돌로 작용할 것이다. 특히 접근제어 메커니즘을 제공하는 것 이외에 상황인식시스템간의 상호인증이 가능하도록 하여 신뢰할 수 있는 기술적 기반을 마련하여야 하지만 비용을 높여 상황인식시스템의 보급에 장애요인이 될 수 있는 딜레마를 가지고 있다. 이상과 같은 위협을 최소화하기 위해서는 상황인 시스템의 리더와 리더기 사이의 세션 가로채기(hijacking), 재생(replay)공격, 중간자 공격(man in the middle attack)에 대해 안전할 수 있는 기술적인 보호 방안이 마련되어야 한다.

3.2.2 상황인식시스템의 보호 기술

위에서 소개한 상황인식시스템의 위협을 최소화 하는 기술로는 다음과 같은 것이 있다.

상황인식시스템은 Active Jamming, Blocker Tag, Faraday Cage, Hash-Lock Access Control, Kill tag, One-Time Pad, Re-Encryption, Silent Tree-walking 등의 보호 기술로 위협을 최소화 할 수 있다. 이와 같은 응용 보안 기술은 RFID 등 USN 환경에서 주로 활용할 수 있는 보호 기술이다.

첫째, Active Jamming 기술은 RFID 등 USN 환경에서 센싱을 리더하는 장치를 교란하는 방해 신호를 보내는 것이다. 방해 신호는 개인정보를 읽지 못하도록 하거나 특정 지역에 허가받지 않은 전파를 수신하지 못하도록 한다. 과거 북한 방송을 막기 위해 강력한 방해 전파를 휴전선 부근에서 송신하였던 것과 유사한 방식의 기술이다.

둘째, Blocker Tag 기술은 모든 질문 메시지에 대해서 '예'라고 응답하기 때문에 이진 탐색 기법을 사용하여 센서를 읽어 들이는 방식에서는 탐색의 모든 영역을 검색하게 되거나 ALOHA기법을 사용하는 센싱에서는 전혀 읽을 수 없도록 만든다.

셋째, Faraday Cage 기술은 금속성의 그물(mesh) 또는 박막(foil)을 입혀 센싱을 리더하지 못하게 한다. 즉 무선 주파수 교신이 이루어지지 않게 함으로 개인정보의 노출을 막는다.

넷째, Hash-Lock Access Control 기술은 해쉬 함수를 이용한 접근 제어 기술이다. 즉 허가된 사용자만이 태그를 접근할 수 있도록 하며 허가된 사용자라 할지라도 사용권한 등을 제한하는 인증 기술을 뜻한다.

다섯째, Kill tag 기술은 MIT의 Auto-ID Center(현 EPCglobal)에서 제안한 방법으로 유명한다. 센싱의 설계에 *8-bit*의 패스워드를 포함하여 센싱이 패스워드와 'Kill' 명령을 받을 경우 센싱의 정보교류가 비활성화 되도록 하는 기술이다.

여섯째, One-Time Pad 기술은 컴퓨터 시스템의 One-Time Pad 기술의 단순함과 강력한 암호화 기능을 USN 환경에 적합하도록 구현한 것이다. 따라서 상호인증을 단순하면서도 강력한 암호로 구현할 수 있으며 인증된 사용자 간의 정보교류를 통해 개인정보를 보호할 수 있다.

일곱째, Re-Encryption 기술은 RSA연구소에서 유료(euro)화에 내장하기 위하여 개발한 보안 기술로 유명하다. 재 암호화를 위한 공개키를 센싱 안에 내장하지 않아도 되는 장점이 있으며 신뢰할 수 있는 외부 공개키 암호 연산기를 통해 상호 인증을 하는 기술이다.

여덟째, Silent Tree-walking 기술은 실행 시간 측면에 있어서도 일반 이진 탐색 기법과 동일한 효율성을 지니면서도 센싱을 리더하는 장치가 요청하는 데이터를 불법 도청자로부터 보호할 수 있다는 장점을 가지고 있다.

이상과 같은 기술들은 주로 RFID 시스템에서 태그와 리더기 그리고 외부 서버 간의 네트워크 상에서 일어날 수 있는 개인정보에 대한 위협을 기술적으로 보호하기 위한 방안으로 소개되고

있다. 그러나 RFID 시스템이 USN 환경에 필수 불가결한 시스템의 구성요소란 점에서 RFID 시스템에서 주로 활용할 수 있는 기술들에 대한 적용이 효과적일 수 있다. 특히 상황인식시스템을 능동적이면서도 지능적으로 구현하기 위해서는 이기종 간의 네트워크와 유·무선이 혼합된 환경에서의 보안을 고려하여야 한다. 특히 조용한 기술을 구현하기 위한 상황인식시스템은 끊김없는 연결을 통해 가능하다는 점에서 개인정보의 위협을 최소화하기 위해서는 위에서 소개한 여러 가지 보호 기술을 시스템의 하드웨어 및 소프트웨어 그리고 주변 환경을 고려한 선택이 요구된다. 이상과 같은 기술들을 통해 개인정보를 해킹하거나 불법적으로 획득하려는 사람은 개인정보를 얻는데 오랜 시간을 걸려야 한다거나 몇 가지 과정을 반복해야하는 번거로움 또는 불편함을 받게 되거나 더 나아가 개인정보를 얻을 수 없도록 정보를 삭제해버리도록 하는 등 다양한 단계에서의 보안 수준을 설정하는데도 기술들의 장·단점을 선택하여 구현할 수 있다.

4. 결론

USN은 RFID 시스템 기술을 중심으로 구현될 전망이다. 특히 USN은 이동성을 중심으로 제3공간을 탄생시킬 전망이다. 여기서 이동성이란 RFID, 위치추적, IPv6, GPS 등의 USN 기반 기술들이 중첩되어 관리되고 상호 연동될 수 있는 다양한 시스템 또는 기술들을 통해 이음새 없는 상황인식서비스를 구현할 전망이다. 이음새 없는 매 순간의 상황을 인식해내는 시스템은 정보의 자유로운 이동을 전제로 발전될 수 있는 기술이다. 이 기술의 일상생활 속에서의 구현은 개인정보의 자유로운 이동을 가져오고 이는 곧 심각한 정보 프라이버시를 위협할 것이다.

오늘날 급속한 기술발달에 따른 프라이버시의 위협은 물리적인 공간에서 통신공간으로 확장되었고 최근에는 인터넷 공간까지 이르렀다. 유비쿼터스 컴퓨팅 시대가 도래 할 경우, 프라이버시의 위협은 가상공간이 침투한 물리공간으로 확대될 것이며, 물리공간에서는 MEMS기술로 소형화된 마이크로 칩에 저장되거나 실시간으로 이동되는 개인정보의 위협이 증대할 것이다. 이와 같은 개인정보와 정보 프라이버시의 위협을 최소화하고 상황 인식 서비스를 가능하게 하는 시스템을 구현하여 USN 기술의 순기능을 극대화하기 위해서는 다가오는 사회에 개인정보와 정보프라이버시의 새로운 개념 정립과 보호 영역에 대한 이해가 선행되어야 할 것이다. 특히 상황 인식 시스템의 기술적인 보호 방법들에 대한 소개를 통하여 각 기술들을 이용한 안전한 USN 환경 구축에 기여할 것으로 기대된다.

본 연구는 상황인식시스템이 가진 기술적 속성들이 개인정보와 정보 프라이버시의 개념과 보호 영역을 어떻게 새롭게 설정할 것인가를 분석하고 문제점을 고찰하였으며 보호 기술을 제시하였다.

정보 프라이버시의 개념과 보호 영역 그리고 침해 주체 등 다양한 분석에 따른 해석을 새롭게 함으로 다가오는 USN 환경에서 정보 프라이버시의 보호에 기여할 것으로 사료되며 정보 프라이버시의 중요도에 따라 보안 기술의 선택적 적용이 가능할 수 있도록 이론적 개념과 기술적 제시를 병행하였다.

참 고 문 헌

[1] Kang, Jang Mook, "A Study on CVMP(Competing Values Model about Privacy)in Ubiquitous Computing Environment," Springer-Verlag, ICCMSE 2005, pp. 136-139, 2005.

[2] 김정기, 박승민, 장재우, "상황인식처리기술", 정보처리학회지, 제10권 제4호, p. 183, 2003.

[3] 장세이, 우윤택, "유비쿼터스 컴퓨팅 환경을 위한 센싱-기술과 컨텍스트-인식 기술의 연구동향", 정보과학회지, 제21권 제5호, pp. 18-28, 2003.

[4] keizo Watanabe 외 7인(박기환 역), 「유비쿼터스 RFID」, 성안당, 2005, p. 139 <4-3>표를 수정 인용

[5] 하우영, "노동정보처리와 정보인권보호", 정보보호학회논문지 제13권 제6호, p. 18, 2003.

[6] Brown, P.J., Bovey, J.D., Chen, X., "Context-awareness Application : From the Laboratory to the Marketplace," IEEE Personal Communication, Vol.4, No.5, pp. 55-65, 1997.

[7] Dey, A. K., "Context-Aware Computing : The Cyber Desk Project," Proc. of the AAAI 1998 Spring Symposium on Intelligent Environments(AAAI Technical Report SS-98-02), pp. 51-54, 1998.

[8] 강장묵, 「강교수의 UC 특강(유비쿼터스 컴퓨팅과 개인정보)」, 인터비젼, p. 182, 2006.
[9] 정보 프라이버시에 대해서는 아래 두 사이트인 http://www.eff.org/Privacy/GII_NII/iitf_principles.draft 또는 http://www.cdt.org/privacy/comments_iitf.html 에서 상세하게 살펴볼 수 있다.
[10] 서계원, "정보 프라이버시와 개인정보의 보호-개인정보보호기본법안을 중심으로-", 세계헌법연구, 제11권 제1호, p. 196, 2005.
[11] Regan, P., 「Legislating Privacy : Technology, Social Values and Public Policy」, Univ. of North Carolina Press, 1995.
[12] 김철수, "정보공개법과 사생활비밀보호법 서설", 정보의 모집·관리와 사생활보호, pp. 13-59, 1989.
[13] 강장묵, 「강교수의 UC 특강(유비쿼터스 컴퓨팅과 개인정보)」, 인터비젼, p. 187, 2006.
[14] Want, Roy, Hopper, Andy, Falcao, Veronica, Gibbons, Jonathan, "The Active Badge Location System," ACM Transactions on Information Systems, Vol. 10, No. 1, pp. 91-102, 1992.

강 장 묵

1996년: 국민대학교 경제학사
1999년: 고려대학교 경영학석사
2005년: 고려대학교 공학박사
1996년~1997년: (주) 쌍용정보통신 컨설턴트
1997년~2005년: 고려대학교, 상명대학교, 서경대학교, 서울여자대학교, 서울산업대학교 출강
2006년~현 재: 세종대학교 컴퓨터공학과 교수
관심분야 : 유비쿼터스 컴퓨팅(AR), 프라이버시(PET),디지털저작권(DRM) 등

방 기 천

1981년 : 서울대학교 전자공학과(학사)
1988년 : 성균관대학교 정보처리학과(석사)
1996년 : 성균관대학교 전산통계학전공(박사)
1984년~1995년: MBC 기술연구소
1995년~현 재: 남서울대학교 멀티미디어학과 교수
관심분야 : 멀티미디어콘텐츠, 멀티미디어 응용, 인터넷 방송 등