유비쿼터스 센서 네트워크(USN)의 개인정보보호 고찰

최 성, 백계현
남서울대학교 컴퓨터학과
-comsa@hanmail.net

Ubiquitous UNS for Individual Information Protection

Choi Sung, Back gae hyun
Namseoul University, Dept. of Computer Science

요 약

본 논문에서는 신성장 동력 기술 중의 하나인 유비쿼터스 환경에서의 개인정보 보호 기술에 관하여 연구하였다. 유비쿼터스 환경에서는 사람이나 물건의 상황과 주변 환경 등을 센싱하여 다양한 대량의 데이터를 수집하게 되며, 또한 서비스 제공에 의해 개인 프라이버시에 관한 정보를 센싱 노드나 네트워크 상에서 주고받게 된다. 지능형 유비쿼터스 센서 네트워크(USN) 기술에서 RFID 태그 시스템에서의 프라이버시 보호 방법에 관한 기술들을 연구하였다.

1. 서론

정보통신 기술이 발전하면서 많은 사람들은 미래 사회는 유비쿼터스 시대가 열리고 있다. 그리고 이러한 시대를 이루기 위해서 유비쿼터스 컴퓨팅에 관한수많은 연구가 이루어지고 있다. 유비쿼터스 컴퓨팅은 문자적 의미로 직역하면 '편재하는 컴퓨팅'로 해석된다. 즉, 언제, 어디서나 컴퓨터를 이용할 수 있다는 것이다. 이러한 기본적인 의미를 바탕으로 유비쿼터스 컴퓨팅은 컴퓨터가 위치할 수 있는 곳에 따라서 사이버 공간의 가상 컴퓨팅과 실세계의 리얼 컴퓨팅으로 나누어 볼 수 있다. 하지만 최근 유비쿼터스 컴퓨팅의 연구동향은 소프트웨어, 하드웨어, 물리적인 개체를 차세대 컴퓨팅 환경으로 통합하여 가상세계와 실세계를 병합하려는 모습을 보인다 그래서 개인정보는 인터넷에서 이루어지는 시장 경제의 활성화를 위해 반드시 필요한 것으로, 기업의 입장에서 보면 이러한 개인정보를 통해 온라인의 특성을 활용한 마케팅과 판매활동을 적극적으로 수행할 수 있다. 그러나 개별적인 인터넷 사용자들의 입장에서 볼 때 이들은 자신의 개인정보를 제공함으로써 발생할 수 있는 위험에 노출되어서 우려되는 것은 사실이다. 이러한 면에서 개인정보 보호기술은 개별적인 사용자 혹은 기술 관리자가 어떠한 경우에 정보를 공개할 것인지에 대한 통제 능력을 부여한다는 점에서 효율적인 프라이버시 보호 솔루션을 제공해야만 한다.

그러므로 개별 기업들은 우선 프라이버시 보호기술을 자사의 네트워크에 결합함으로써 사용자들의 프라이버시를 보호할 수 있는지에 관해 평가하는 것이 필요하다. 기업은 어떻게 프라이버시 보호기술이 브라우저나, 다른 하드웨어 혹은 휴대용 제품들과 호환되어 표준화될 수 있는지를 고려하여야 할 것으로 보인다. 마찬가지로 인터넷 서비스 제공자는 프라이버시 보호기술을 제공함으로써 가입자들이 우려하고 있는 프라이버시 보호 문제가 경감될 수 있는지를 고려하는 노력이 필요하다.

유비쿼터스 환경에서는 사람이나 물건의 상황, 그

의 주변 환경 등을 센싱하여 다양하고 대량의 데이터를 수집하게 된다. 이와 같은 데이터 중에는 영상이나 바이오 메트릭스 처럼 직접 개인의 프라이버시에 관계되는 정보가 있으면, 체온이나 혈압 등의 미세한 정보를 조합하여 건강상태를 알 수 있듯이 통합 또는 분석에 의해 의미 있는 정보로 되는 것도 있다. 따라서 서비스 제공에 의해 개인 프라이버시에 관한 정보를 센싱 노드나 네트워크 상에서 주고받게 된다. 또한 센싱하거나 센싱 된 정보의 소유자가 누구의 것인가? 그 정보의 처리, 가공, 유통, 삭제의 권리는 누구인가 등에 관해방법을 정리할 필요가 있다. 유비쿼터스 센서 네트워크의 실현, 보급에 있어서 현장 실험 등을 통해 어떠한 정보를 누가 어떻게 취급하는가에 관한 기본적인 생각을 이용자를 포함한 관련자간에 충분히 검토하여 기술적인 대책을 연구할 필요가 있다.

2. 본론

1) USN 구조

USN은 여러 개의 센서 네트워크 Field가 Gateway를 통해 외부 네트워크에 연결되는 구조를 갖는다. 센서 노드들은 가까운 Sink 노드로 데이터를 전송하고센서 노드로 집적된 데이터는 Gateway로 전송된다. Gateway에서 관리자에게 전달되는 데이터는 위성통신, 유무선 인터넷 등을 통해 전송될 수 있으며, 이런 Access Network는 기존의 인프라를 이용한다.

전체적인 USN의 아키텍처는 <그림 1 >과 같다.

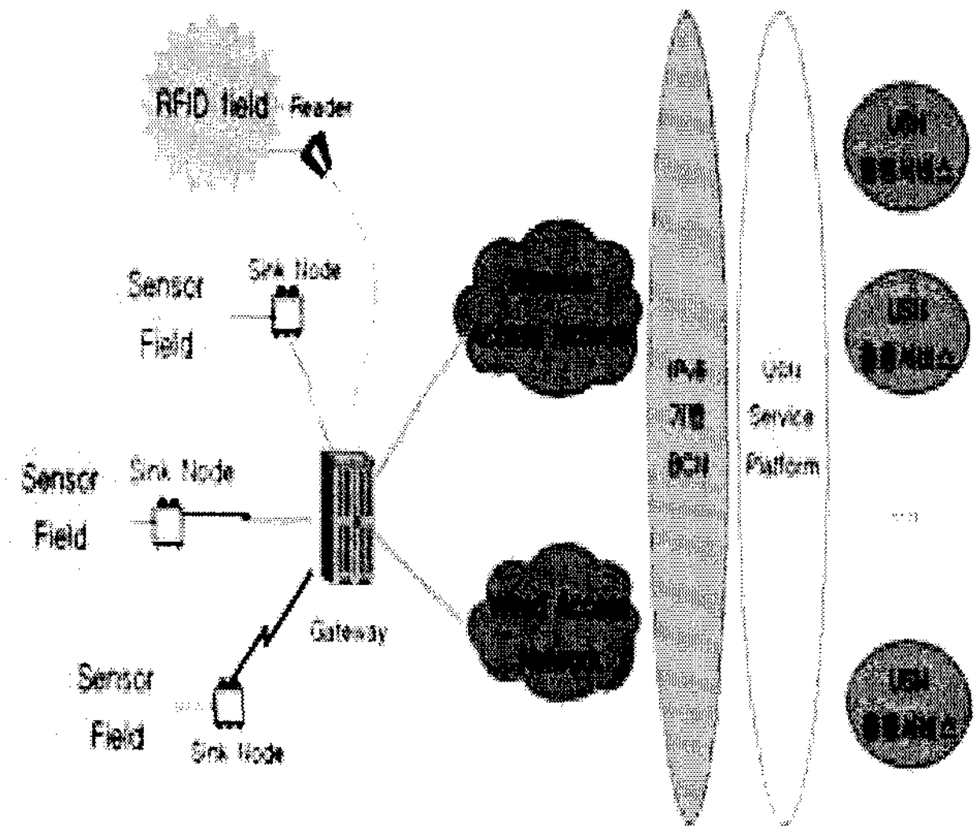

그림 1. USN 아키텍춰 구조

Access Network는 IPv6 기반의 BcN으로 인터넷 통합망을 가정하며 이는 곧 모든 센서 노드에 IPv6가 적용될 것을 뜻한다 또한 센서 네트워크의 애플리케이션을 위해 미들웨어로써 서비스 플랫폼이 제공되어 사용자는 이를 통해 차세대 네트워크인 지능형 센서 네트워크를 자유롭게 이용한다.

USN이 완성되기 위해 우선 주목해야 하는 부분은센서 네트워크 field 부분이다 Sink 노드에서 gateway를 거쳐 Access Network 이상의 분야는 USN의 통합적인 발전을 위한 기술로써 정책적으로 발전되며, 센서 네트워크 field 분야는 연구진의 기술개발로 발전된다. 센서 네트워크는 네트워크를 구성하는 일정 지역에 크기가 1mm3 정도의 작은 노드들이 수 백 개에서 수천 개까지 설치하여 통신하는 구조를 갖는다. 또한 노드들이 주고받는 데이터는 그 크기도 작고 데이터의 발생 빈도 또한 매우 낮아 통신하는 양은 많지 않을 것으로 가정한다.
센서 노드의 크기가 작은 만큼 그에 따른 제약 조건이 존재 한다. 가장 큰 문제는 배터리의 크기이다.

현 기술력으로 센서 노드에 적용할 수 있는 크기의 배터리로는 가용 에너지가 너무 적다 따라서 센서 네트워크의 연구는 일차적으로 에너지 효율성을 고려해서 진행되고 있다 네트워크 분야에서는 두 노드간의 통신이 가장 많은 에너지를 소모한다고 판단하여 가능하면적은 양의 데이터와 시그널을 주고받는 것이 중요한 이슈가 되고 있다. 노드의 크기가 작은 것은 메모리의 크기에도 한계를 가져온다. 메모리 기술은 상당히 발전하였지만 기본적으로 크기가 너무 작기 때문에 많은 데이터를 저장하고 있을 수 없다 따라서 네트워크나 라우팅 정보들을 필수적인 것들만 저장하여 이용하도록 간단한 프로토콜이 요구된다. 또 다른 문제로 통신 거리와 방법에 한계가 있다.

센서 노드들은 서로 가까이 존재하여 통신 할 수 있다고 가정하더라도, 원격지에 있는 사용자와 관리자는 센서노드가 직접 통신할 수 없는 거리에 존재하게 된다. 센서 네트워크는 항상 네트워크 Field 안에 다른 네트워크와 통신할 수 있는 다른 형태의 노드가 필요하다 이런 노드를 Sink라고 부르며, Sink 노드는 크기가 크고 배터리의 한계를 가정하지 않는다. 센서 네트워크 내에서 발생된 데이터는 모두 Sink 노드로 집적되어 센서네트워크와 다른 방식으로 외부 네트워크에 연결된다. 이 방식은 Sink 노드의 특성에 따라 위성 통신, 무선랜(Wireless Local

Area Network), 블루투스(Bluetooth), 유선 인터넷 등의 방식을 가질 수 있다.

2) RFID 시스템의 특성

RFID 태그는 무선 통신용 안테나와 IC 칩을 조합한 저가의 소형 장치이다. 태그에 질의를 발생시켜,RFID 태그 메모리에 쓰여져 있는 ID를 읽어내는 무선 장치를 Reader라 부른다. Reader에 의해 질의를 할 때, 전원도 함께 보내며, 이 경우 RFID 태그 자신에는 전원이 필요 없다. 이 때문에, RFID 태그는 장차 바코드를 대신하는 식별 기능으로 활용될 것이다. 바코드와 같이 폭 넓은 이용을 위해서는 RFID태그 하나 당 가격은 50원정도, 크기는 0.4mm×0.4mm 이하로 종이에 심을 수 있을 정도로 얇은 것이 바람직하다. 따라서 RFID 태그의 계산 능력은 제한되어, RFID 태그가 복잡한 능력을 처리하는 것은 곤란하다. 또한 전파를 이용하는 특성상, RFID태그와 reader 사이에 주고받는 내용을 쉽게 도청할 수 있다.

RFID 태그에는 몇 종류가 있으며, 통신 거리, 메모리 종류, 전원의 유무에 의해 분류된다. 우선, 통신 거리에는 밀접형(0~수mm), 근접형(수mm~수10cm), 원격형(수10cm~수m)이 있다. 메모리에는 읽기 전용형, 한번만 쓰기 및 읽기형, 읽기 및 쓰기 가능형이 있다. 쓰기 가능한 메모리를 탑재한 경우,RFID 태그의 ID 정보를 Reader/Writer라 부르는 무선통신 장치에 의해 써넣기가 가능하다. 또 RFID 태그의 전원에는 능동형과 수동형이 있다. 능동형은 RFID 태그에 전원을 내장하고 있고, 수동형은 reader로부터 전원을 얻는다. 이 태그와 Reader를 이용한 개인정보 식별 시스템을 RFID 시스템이라 부른다.

RFID 시스템을 이용하면, 상품의 포장을 개방하지 않아도, 상자 속에 태그가 부착된 상품 인식이 가능하기 때문에, 상품의 재고 관리나 물류 관리에 이용된다. 태그는 상품에 붙여져 있으며, 바코드 같은기능이 부여되어 있으므로 도난 방지 역할을 기대할수 있다. 또한 상품 구입 후에도 RFID 시스템은 소비자에 편리한 기능을 준다. 예를 들면, 리더가 부착된 냉장고가 태그에 부착된 식료품의 유통 기한을 감시한다든지, 양복장에 보관되고 있는 옷에서 양호한 조합을 제공하는 것이 가능하게 될 것이다. 또한 유럽중앙은행은 유로 지폐에 RFID 태그를 심는 것을 제안하고 있다. RFID 태그의 ID와 지폐에 인쇄된 일련번호를 조합한 식별을 이용하면, 위조 방지 능력 및 가짜 금융차용의 억제를 기대할 수 있다.

3) 블로커 태그의 구성 및 역할

(1) 블로커 태그를 이용한 프라이버시보호 방법

프라이버시 보호를 위한 Blocker-Tag 방식을 설명한다. 블로커태그가 Tree-walking Singulation 프로토콜과 어떻게 선택적으로 조화를 이루는가를 이해하는 것이 중요하다. 블로커 태그는 Active jamming 형태는 아니다. 아주 정확한 방법으로 태그 reading 과정에 참여함으로써, passive jamming의 한 종류로 생각할 수 있다.블로커 태그는 태그의 가능한 모든 일련번호의전 스펙트럼을 방해하여, 다른 태그들의 일련번호를 감출 수 있다. 고객에 의해 수행될 때, 블로커 태그는 프라이버시 보호인 물리적 영역에 야기되어, reader가 태그를 구별하지 못하도록 한다. 여기에서 블로커 태그의 2가지 형태, 즉 프라이버시 보호도구와 악의의 도구로 사용될 수 있음을 설명하기로 한다.

첫째, 블로커 태그는 프라이버시 protection tool로 제공할 수 있다. 블로커 태그는 자연스럽게 일련번호의 어떤 제한된 영역에 대해 Singulation을 방지하도록 설계, 즉 특정 지역에 맞도록 설계된다. 다시 말해, 특정 지역의 프라이버시를 보호할 목적으로 'E1'E로 시작하는 모든 일련번호 영역 지역에 맞도록 설계하는 것을 의미한다. 선택적인 블로킹 특성은 고객에 의해 아이템을 보호하는 데 이용될 수 있다. 동시에 영업적 환경에서는 태그의 reading을 방해하지 않는다.

둘째, 악의의 모습으로 동작하는 블로커 태그를 말한다. 다시 말하면, DOS 공격을 준비하는 도구로서의 기능을 설명한다. 블로커 태그는 일련번호의모든 스펙트럼을 읽지 못하도록 차단하거나 특별한 영역(예를 들면, 특별한 제조 회사에 할당된 일련 번호의 집합)을 reader가 읽지 못하도록 차단시킬 수 있다. 이런 형태의 블로커 태그는 비즈니스를 방해하거나 물품 명세서 제어 메커니즘으로부터 상품을 차폐시킴으로써 좀도둑이 침입하는 데 도움을 줄 수 있다.

(2) 프라이버시 보호도구로서의 블로커 태그

고객의 프라이버시 보호를 위해 널리 이용되는도구로서 매력을 확인시켜 주기 위해, 블로커 태그는 재고 관리와 같은 정상적인 RFID 기반 상업과정은

조금도 방해하지 않는 방식이다. 이 관점에서, Universal 블로커 태그는 의도에 반대되고 있다. 프라이버시 개선을 목적으로, Universal 블로커태그 대신에 선택적인 블로커 태그 사용을 요구한다. 이는 프라이버시 보호를 위해 한 개 혹은 그 이상의 영역의 특별한 명령을 가지고 있다. 따라서 "프라이버시 영역"은 선택적인 블로커 태그에 의해 보호될 태그 일련번호(Restricted number)로 구성된다. 선택적인 블로커 태그는 reader가 프라이버시영역으로서 블로커 태그에 의해 규정된 영역에 들어갈 때마다 reader의 tree-walking 알고리듬 수행을 방해한다. 그리고 이외의 영역에서는 reading이허용되며, 블로커 태그는 inactive 상태로 남는다.프라이버시 영역과 태그 일련 번호의 동적 변경을 이용하여, 상인 및 고객이 동시에 만족할 수 있는 프라이버시 정책의 영역(natural range)을 구현하는 것이 가능하다. 우리는 사용하는 환경에 의존하여 프라이버시 영역 내외로 움직일 수 있는 일련번호를 갖는 시스템을 상상할 수 있다. 프라이버시 영역에 상응하는 선택적인 블로커태그는 아주 간단하게 구현할 수 있으며, 이는 single 노드의 서브트리로 구성된다. 예를 들면, 그러한 영역이 일련번호 트리의 오른쪽 반으로 간단하게 구성된다. 즉 모든 일련번호가 Leading bit가 1인 것을 의미한다.

예로, 어떤 슈퍼마켓에서는 leading bit가 '1'인 일련번호로 구성되는 프라이버시 영역을 갖는 블로커 태그를 사용하고 있다. 슈퍼마켓에서 패키지 각각은 재고 상품 관리 목적으로 사용될 유니크한 일련번호를 갖는 RFID 태그를 가지고 있다. 사전 프로그램에의해, 제품이 슈퍼마켓 내부 혹은 창고에 있을 때 RFID 태그의 일련번호는 ']0'bit로 시작한다. 이 때, 블로커 태그는 태그의 reading을 방해하지 않는다. 카운터에서 RFID 태그 reader가 구매로 고객에 제품(item)이 넘겨질 때, tag-specific key를 아이템의 RFID로 전송된다. 이것은 태그의 일련번호의leading bit를 '1'로 되도록 유도한다. 슈퍼마켓은 블로커 태그로부터 자유롭게 물건을 제공한다. 이것은 카운터에서 쇼핑백에 넣거나 스티커를 아이템 위에 붙이는 방법이 있다.고객이 슈퍼마켓의 쇼핑에서 집으로 돌아 왔을때, 쇼핑백에서 상품을 끄집어 내거나 privacyenhancing스티커를 제거함으로써 프라이버시 영역에서 unmask 된다. 고객이 "]smart"냉장고에 물건을 넣으면, 냉장고에 부착된 RFID 태그 reader 가내용을 읽어 들인다. 이때, 연동된 컴퓨터는 물건 재고를 파악하여 다음에 구매하여야 할 물건의 목록을 프린트한다.

이와 같은 간단한 방식을 자연스럽게 AutoID 센터의 EPC-code 시스템으로 통합시킬 수 있다.EPC code는 96bit이며, 다음과 같이 나누어져 있다.

1. 8bit header; 2. 28bit "EPC 매니저" 코드는태그를 소유하는 조직이 사용; 3. 24bit "]objectmanager" 코드는 EPC 매니저에 의해 결정되는 object 등급용으로 사용; 4. 36bit 일련번호는 object를 유일하게 구분하기 위해 사용한다. 따라서 표준 "프라이버시 bit"로 설계된 object manager code bit의 하나를 가짐으로써 지금까지 설명한 프라이버시 구조를 구현할 수 있다. 모든 블로커 태그는 그때 유일한 EPC 매니저 코드에 할당할 수 있다.

3. 결론

USN의 궁극적인 목표는 IPv6를 기반으로 하는 BcN과 연동되어 모든 사물이 지능적으로 네트워크를 구성하여 통신하는 것이다. 이것을 이용하여 개인정보를 보호해야 한다.

개인정보는 현재 정보화 사회에서 중요한 위치를 가지고 있는 웹 콘텐츠를 발전시키고 제공하는 서비스나 상품의 수준을 높이는 데 큰 역할을 하고 있고,이러한 이용자의 개인정보는 수집자에 의해 데이터베이스화되고 이를 분석하여 마케팅에 활용할 수 있다. 그러나 정보화 사회의 역기능으로, 이용자의 개별적 동의나 인지 없이 개인정보를 무단으로 수집하거나 수집된 정보를 데이터베이스로 구축하여 이차적으로 사용하는 행위 등 여러 가지 문제를 유발시키고 있으며, 이러한 온라인 프라이버시 보호 문제를 해결하기 위해 기술적 및 제도적으로 해결해 나가야 한다.

참고문헌

[1] ISO/IEC JTC1/SC31, http://usnet03.uccouncil.org/sc31

[2] Ian F.Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, "A Survey on Sensor Networks", IEEE Communications Magazine, August 2002

[3] T. Otsuka and A. Onozawa,""Users Privacy in Ubiquitous Network: Anonymous Communication

Technique for Ad-hoc Network," "Technical Report of IEICE ISEC2003-38, July 2003.

[4] Junichiro Saito and Kouichi Sakurai, ""Privacy Protection Using Re-encryption in RFID Tags,""Technical Report of IEICE ISEC2003-81, Nov. 2003.

[5] 정.보.통.신.부., http://www.mic.go.kr