

항공보안 무선검색시스템의 요소 기술 분석

Element Technologies of Wireless Scanning System

전동구*, 김장환, 강자영(한국항공대학교)

I. 서론

미국의 9/11 사건 이후 국제적으로 항공보안이 강화되고 있다. 항공기 탑승자 및 휴대 수화물에 대해서도 철저히 검색을 하고 있는 실정이다. 그래서 각 나라에서는 보안강화를 위해 막대한 예산을 들여 보안장비를 개발하고 있고 유비쿼터스 시대를 맞이하여 수준 높은 IT기술을 도입하려 하고 있다. 항공보안 분야 뿐 만아니라 최근 정보통신기술을 이용하는 각 부문에 있어서 유비쿼터스 컴퓨팅과 네트워크의 중요성이 점점 강조되고 있다. 이 유비쿼터스 컴퓨팅이란 '동시에 여러 곳에 존재하는', '언제 어디서나 존재하는'이란 뜻으로 1988년 Xerox사의 마크와이저에 의해서 불려지기 시작했다. 마크와이저는 21세기 정보 기술의 바람직한 모습을 컴퓨터 중심이 아닌 사람 중심에서 이루어진다고 생각하였다, 예컨대 정보기술이 업무를 도와주는 보조적인 수단이기 보다는 그 자체가 업무가 되어 버리는 문제를 안고 있었다. 마크와이저는 이 문제점을 보완하기 위해 유비쿼터스 컴퓨팅을 주창하게 된 것이다[1]. 그리하여 이 기술을 통해 우리 생활공간 도처에 컴퓨팅 기능이 내재된 모든 사물들이 서로 연결되어 지는 것이다. 이러한 유비쿼터스 분야의 핵심 기술로서 무선인식(Radio Frequency Identification : RFID)기술이 있는데 이 기술은 교통카드, 전자 신분증 등에 삽입된 식별표시(Tag)가 판독기(Reader)의 발사전파를 일시적으로 흡수해 그 전파에 식별표시 고유정보를 실어 반사하는 것이 기본원리이다. 이 RFID 기술을 기반으로 하여 센서네트워크 기술, 보안 기술을 이용한 것이 무선검색시스템이라 할 수 있다.

본 논문에서는 항공안전을 보장하기 위해 적용된 이 무선검색시스템의 기술 요소들을 연구하고 보다 안전하고 확실하게 구축하기 위한 기술 도입을 제안하고자 한다.

II. 무선검색시스템의 기술 요소

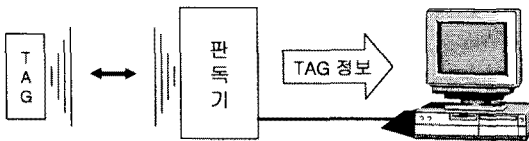
1. RFID

오늘날 대부분의 상품에는 바코드가 부착되어 있다. 바코드를 통해 읽어드린 정보는 판매한 물품에 대해 총금액을 계산하고, 적정재고 유지, 효과적인 입·출하 관리, 판매관리 등의 업무에 편리하다. 그러나 바코드는 특정 상품에 속하는 각 개체들은 구별하지 못하며 동일 상품에 속하는 모든 개체에는 동일한 바코드가 부착되어 있기 때문에 1회성 소비로 끝나는 제품에 대해서는 편리한 도구이다. 이러한 바코드의 한계를 극복하기 위한 기술이 RFID 기술이다.

RFID 시스템의 기본적인 구조는 물체에 부착되는 RFID택과 무선으로 RFID택과 정보를 주고받는 트랜시버(transceiver)로 이루어진다. RFID트랜스폰더(transponder)라고도 불리는 RFID택은 물체의 식별코드(code)와 물체와 관련된 다른 정보가 저장되는 마이크로칩과 무선으로 트랜시버와 정보를 주고받는 안테나로 구성된다. 최근에는 하나의 마이크로칩에 저장기능과 전송기능을 통합하는 RFID택이 상용화되고 있다. RFID택에 저장된 정보를 읽는 리더(reader)를 포함하는 트랜시버는 RFID택으로부터 정보를 받아서 컴퓨터로 보내고 컴퓨터에서 받은 정보를 RFID택으로 보내는 역할을 한다. 이 RFID는 짧은 시간에 많은 택을 인식 할 수

있고, 실시간 정보의 인식은 물론 수 cm ~ 수 m의 인식거리를 가지면서도 보안성이 뛰어나 세계적으로 바코드를 대체할 수 있을 것이라고 전망한다. RFID택은 현재 저주파(125KHz), 고주파(13.56KHz)택을 중심으로 10cm 내외의 출입관리, 교통카드 등에 많이 보급되어 있다. RFID 기술에 대하여 국제 표준화가 진행되면서 급부상하고 있으며, 특히 극초단파(900MHz, 433.92MHz)와 마이크로파(2.45GHz) 대역의 택이 등장함으로써 인식거리가 길어지고 다양한 응용 시스템에 적용이 예상된다[2].

이러한 RFID 기술은 여러 가지 장점과 다양한 응용분야에도 불구하고 현재로서는 저가화, 초소형화, 다양한 기능성 부여, 법제도 표준화 등 해결해야 할 과제들이 많다는 것을 알 수 있다. 이러한 과제들을 해결하기 위하여 세계 선진국에서 5센트 이하의 택 개발을 목표로 프로젝트들이 진행 중에 있다. 곧 이러한 문제들을 해결하고 서비스에 적용 확대함으로써 본격적인 유비쿼터스 컴퓨팅 센서핵심기술로 발전하게 될 것으로 전망된다.



<그림 1> RFID 시스템 구성 요소

2. 센서 네트워크 기술

저전력 무선통신의 발전과 다기능, 저가의 스마트 센서는 원격에서 상태정보를 감지할 수 있는 센서네트워크의 실현이 가능하도록 하고 있다. 센서네트워크는 광범위하게 설치되어 있는 유무선 네트워크 인프라에 상황인지를 위한 다양한 센싱 디바이스를 통합하여 감지된 환경 데이터를 응용 서비스 서버와 연동하는 기술이다 [3].

센서 네트워크는 관찰하려는 지역의 내부나 그에 매우 근접한 거리에 수많은 센서 노드들을 조밀하게 배치하여 구성된다. 이 때 센서 노드의 위치는 미리 설정되지 않으며, 이는 접근이 불가능한 지역이나 재난지역에 무작위 배치를 가능하게 한다. 이를 위해 센서 네트워크의

알고리즘과 프로토콜이 자기 구성(Self-organizing)

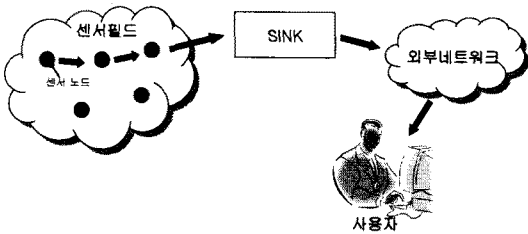
기능을 가져야 하며, 센서 노드간의 협력 처리(cooperative processing)기능이 보다 지능적으로 동작되어야 한다.

이와 같은 무선 센서 네트워크는 기존 유선 센서 네트워크에 비해서 볼 때, 노드간의 협업, 자기구성, 데이터의 온라인 처리, 대규모 수의 센서 노드 면에서 정보의 정확성, 다각도의 관찰, 장애 허용성, 데이터의 원격 접근성, 건물 내 삶의 환경 등에서 향상되었으며 네트워크의 통신비용, 네트워크 배포와 설정의 시간과 비용, 에너지 사용 면에서 개선 되어야 할 것이다.

센서 네트워크의 응용이 구현되기 위해서는 무선 애드혹(ad hoc) 네트워크 기술을 필요로 하지만 기존에 많은 무선 애드혹 네트워크 프로토콜과 알고리즘이 제안되었으나, 이들은 센서 네트워크의 독특한 특성과 응용분야의 요구사항에 적합하지 않다. 센서 네트워크가 기존 네트워크와 차별되는 특징은 다음과 같다[4].

- 센서 네트워크의 노드 수는 기존 애드 혹 네트워크의 노드 수보다 수십 배에서 수 백배 많을 수 있다.
- 센서 노드는 조밀하게 배치된다.
- 센서 노드는 고장 나기 쉽다.
- 센서 네트워크의 토폴로지(topology)는 매우 빈번하게 변경된다.
- 대부분의 애드 혹 네트워크는 점대점(point-to-point) 통신에 기반 하지만, 센서 노드는 주로 브로드캐스트(broadcast) 통신을 이용한다.
- 센서 노드는 전력, 계산 능력, 메모리에 제한을 받는다.
- 센서 노드는 센서의 수와 오버헤드 때문에 전역(global)식별자(ID)를 가질 수 없다.

그러므로 센서 네트워크 기술을 적용하여 에너지 효율성을 증대시키고 감지 데이터의 정확도 증대 및 서비스 품질을 향상시킬 것이다.



<그림 2> 무선 센서네트워크의 구조

3. 보안 기술

무선검색 시스템을 구축하기 위한 보안의 문제는 무선으로 주고 받는다라는 특성, 전력 관리, 무선 기기들의 컴퓨팅 오버 현상 등의 문제를 가지고 있다. 유비쿼터스 시대의 보안 문제는 더 복잡해지고 어려워질 것이다. 또한 유비쿼터스 컴퓨팅의 환경이 도처에 널리 퍼져 있으므로 개인 정보, 시스템 혼란 방지, 확장성, 보안 등의 문제가 있을 것이다.

무선 네트워크의 특성상 개인의 정보가 노출되며, 센서 상황 모델로부터 생성되는 의미있는 정보와 무의미한 정보가 구별없이 폭주할 경우, 무의미한 정보로부터 시스템 혼란 방지를 어떻게 구현할 수 있을 것인지, 분산 환경에서의 유비쿼터스 컴퓨팅 시스템의 응용 레벨에서 하위의 통신 레벨까지 확장성은 어떻게 할 것인지, 마지막으로 네트워크화된 모든 장치나 시스템이 서로 연결된다면 인증되지 않은 소프트웨어나 하드웨어의 공격에 어떻게 대처할 것이 있는지 등이 고려되고 있다[6].

RFID 보안

RFID는 그 편리함에도 불구하고 개인 정보나 보안에 대해 취약한 것이 사실이다. 바코드 시스템과 비교하여 시야가림에 대한 문제가 없어졌지만 그 시야가림의 문제로 인하여 RFID의 택은 항상 읽혀질 준비를 하고 있는 것도 사실이다. 또한 개인 정보에 관한 문제이다. 만약, 옷(물론 속옷도 포함해서)에 붙인 택이 악의적인 사람의 물음에 자신의 고유 번호를 가르쳐 준다면 이는 심각한 사회 문제가 될 것이다. 확실하지는 않지만 사람에게 RFID택을 부여한다고 가정해보자. RFID택에는 너무 많은 정보가

들어 있을 것이고 사적인 정보란 더 이상 존재하지 않을 수도 있다. 이러한 보안 문제를 고려한다면 RFID시스템에서 택에 부여하는 정보의 양은 충분히 고려하여 결정하여야 한다.

불행하게도 택에는 자체적인 네트워킹 기능이 있어 신뢰할 수 있는 CA(Certificate Authority) 같은 곳에 접속하여 리더가 믿을 수 있는지 알아낼 방법이 없다. 고기능 시스템의 경우 나름대로의 인증과 암호화 시스템을 탑재할 수 있지만 그렇지 않을 경우 택은 어떠한 리더의 요구에도 응답하게 된다. 그래서 가장 보편적인 해결 방안들은 택과 리더가 주고받는 신호를 도청하는 것을 막아 보고자 하는 데에 있다.

센서 네트워크 보안

무선 센서 네트워크는 가까운 미래에 널리 사용되어질 수 있는 기술로서 기술이 구체화되어 지고 있고 센서 네트워크 상에서 보안에 대한 필요성이 대두되어 이에 대한 연구가 활발해지고 있다. 센서 네트워크의 보안 요구사항으로서 첫째, 데이터의 비밀성을 들 수 있다. 센서 네트워크 환경의 많은 응용에서 민감한 데이터 교류가 노드 간에 빈번하게 이루어진다. 따라서 허가된 노드 이외의 민감한 정보를 볼 수 없도록 해야 하며 이것은 비밀 키로 데이터를 암호화한 상태에서 데이터 교류가 이루어져야 한다. 즉 데이터의 비밀성을 보장해야 한다. 둘째, 데이터 인증이다. 메시지 인증은 많은 응용의 센서 네트워크에서 중요한 보안 요구사항이다. 공격자는 쉽게 메시지를 삽입할 수 있기 때문에 수신자는 정책방향 결정 과정에서 사용되는 데이터가 원래 작성자로부터 온 것인지를 확인해야 한다. 양단간 통신인 경우 데이터 인증은 순수한 대칭 키 메커니즘을 통해 이루어질 수 있다. 송신자와 수신자는 모든 데이터 통신에 대한 메시지 인증 코드(MAC) 값을 생성하기 위한 비밀 키를 공유한다. 정확한 MAC 값이 수신되어질 경우 수신자는 송신자에 의해 보내진 메시지의 진위를 검증하게 된다. 그러나 브로드캐스팅 통신 방법에서 공유되는 비밀 키는 모든 수신자들과 송신자간에 공유되어야 하며 수신자를 가장해서 MAC 값을 생성할 수

있는 단점을 갖는다. 따라서 일반적으로 공개 키 방식을 통한 브로드캐스팅 통신을 해야 한다. 그러나 공개 키 방식은 실제적인 컴퓨팅 파워나 자원 소요가 크게 일어남으로 이러한 문제점을 해결하기 위한 방식으로 단방향 함수 키 Chain 매커니즘과 키 지연 공개 방식에 대한 기술을 제안한다. 셋째, 데이터 무결성이다. 통신상에서 데이터 무결성은 수신자가 수신한 데이터의 위조 또는 변조 여부를 확인하는 것으로 Security Protocols for Sensor Network(SPINS)에서는 데이터 인증을 통한 데이터 무결성을 보장한다. 넷째, 데이터 최신성이다. 데이터 최신성은 예전에 보낸 데이터에 대한 재사용을 방지하기 위한 기술로서 가장 최근에 보낸 데이터임을 보장하는 보안 서비스이다[7].

IEEE 802.11 Wireless LAN 보안 매커니즘

현재 가장 많이 사용하고 있는 802.11b 무선랜은 처음부터 보안에 큰 관심을 두지 않았다. 또한 공중망에서의 활용을 전제로 설계되지 않았던 것이 사실이다. 예를 들면, 무선랜은 브로드캐스팅 특성으로 인하여 도청 등 무선 데이터 프라이버시에 대한 취약성이 예상되었음에도 불구하고, 동적인 키 분배 방법이 없거나, 취약한 무결성 알고리즘을 사용하여 데이터 프라이버시를 제공하지 못한다는 점이다.

IEEE 802.11i(Enhanced MAC security) Task Group은 최근 무선랜 인프라 망과 Ad Hoc 망에 적용할 수 있는 새로운 형태의 보안 아키텍처인 Robust Security Network(RSN)를 제안하고 표준화를 완료했다. RSN은 다수의 액세스 포인트가 연결된 핫스팟에서 802.1x 기반 가입자 인증을 통한 네트워크 접속제어, 보안 세션 관리, 패킷당 키 관리, 그리고 새로운 암호 알고리즘 도입을 통한 무선접속 구간 보안을 강화하는데 이용된다.

III. 외국의 항공보안 적용 사례

앞에서 언급한바와 같이 9/11 사건 이후에 항공보안이 강화되면서 국제 사회에서는 이 무선

검색시스템을 이미 적용하고 있으며 더 나은 기술을 개발하고 있다.

그 적용 사례를 살펴보면 수화물 관리 시스템을 볼 때 수화물 체크인 카운터에서 RFID택을 발급받아 부착하고 수화물 이동 컨베이어에 RFID 리더를 설치하는 것은 물론 수화물 이동 관계자에게도 휴대용 리더를 지급하고 있다. 또한, 2000년 1월 미국의 BAE Automated Sys사는 이와같은 RFID label처리 시스템을 달라스 공항에 시범적으로 설치하여 99% 판독률을 기록하였는데 이는 레이저 스캐너에 의한 바코드 판독율의 50~86%와 비교하여 매우 높은 것이다. 감지거리는 1m이고 RF 택의 제조가는 25센트로 예상하고 있다. 유사한 시스템이 영국의 British항공에서 smart lavel로 일컫는 RFID luggage처리 시스템을 채택하여 luggage 손실율을 대폭 줄이고 탑승 수속 시간을 단축하였다[8].

또한 2004년 7월 5일, 미국의 델타항공이 미국 내 항공업계에선 처음으로 무선검색시스템 구축에 본격적으로 나섰다. 델타항공은 수화물 분실 사고를 없애기 위해 미 전역에 걸쳐 있는 자사 네트워크망에 향후 1500~2500 만\$를 투입, RFID시스템을 구축할 예정이라고 밝혔다. 델타는 시스템 구축이 끝나면 RFID택이 부착되는 공항 체크인 카운터에서도 수화물 추적이 가능하다고 한다. RFID택 리더는 체크인 카운터를 비롯하여 컨베이어 벨트, 공항 수화물 출입구 등 여러 장소에 설치된다. 델타는 RFID시스템 도입으로 연간 1억 \$의 경비 절감을 예상하고 있다. 앞서 델타는 올 초부터 아틀란타에서 잭슨빌 공항까지 가는 수화물에 RFID시스템을 시범적으로 사용하고 있는데 도입을 본격 선언한 곳은 델타가 처음인데 라스베가스 공항과 맥캐런인터내셔널 공항도 2004년 가을부터 RFID택을 도입할 예정이라고 한다. 국내의 경우, 한국공항공사는 공항에서의 신속·정확한 수하물 처리를 통해 비용절감과 공항 대외신인도를 높이기 위하여, 김포-제주 구간의 수화물에 RFID를 시범적으로 적용하고 있다. 이를 통하여 수화물 분실이나 바뀌는 것으로 방지하거나 수화물이 승객이 탄 여객기에 실리지 못하는 경우의 수도 줄일 수 있다. 현재 수하물 사고율 지수는 3.25건/1,000명인데 이를

1.25천/1,000명으로 줄인다는 방침이다[9].

IV. 결 론

지금까지 항공보안 무선검색시스템의 요소 기술에 대해 살펴보았다. 그 결과 확실한 것은 앞으로 이 무선검색 시스템이 전 세계 항공 보안 분야뿐 만 아니라 다양한 산업분야에 걸쳐 혁신 기술의 하나로 자리매김할 것은 분명하다는 것이다. 본 논문에서는 이 기술을 항공 안전 및 보안 분야에 적용함으로써 안전하고 편리한 인간중심의 사회 구현을 기대할 수 있다고 본다. 그러기 위해서는 승객의 유동율을 향상시키는 방향으로 추진함은 물론 프라이버시 침해 문제 및 기술적, 제도적 문제점 등 여러 가지 측면에서의 해결해야 할 문제점들이 많이 남아 있다. 다가올 유비쿼터스 시대에 맞게 이러한 문제들을 해결함은 물론 독자적인 기술개발 사업도 적극 추진해 나가야 할 것이다. 해외 각국에서는 이미 해당 기술의 선점을 위해 많은 연구비를 투자하여 기술을 개발하고 있으며 우리도 U-Korea의 건설을 위해 이에 대한 대비가 필요할 것이다. 따라서 이 기술의 조기 활성화를 위해 문제점으로 지적된 사항들을 정부와 민간이 상호 협력과 보완을 통해 우선적으로 해결해야 할 것이며, 이를 위해서 정부 및 공공기관의 지원이 필수적이라 하겠다.

참고문헌

- [1] 하원규, 이미숙, 홍영교, "UIT 혁명 시대를 전망 한 BcN의 발전방향과 조건," Telecommunication Review 특집부록 통권 89호. 2004
- [2] 유비쿼터스 네트워크와 신사회 시스템, 일본 노무라연구소 보고서, 2003
- [3] National Research Council, Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers, National Academy Press, 2001
- [4] [aky02] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, " A Survey on Sessor Networks", communication Magazine IEEE. Vol. 40, no. 8, pp.102-114, Aug. 2002
- [5] [sai04] H. Saito and H. Miinimi, "Performance Issues and Network Design for Sensor Networks", IEICE Trans. On Commun., vol. E87-B, no. 2, pp. 294-301, Feb. 2004.
- [6] 임지형의 "유비쿼터스 및 Ad Hoc 네트워크 망에서의 정보보호 분석" 주간기술동향 2004.
- [7] Y, J, Zhao, R. Govindan, and D. Estrin, "Computing Aggregates for monitoring Wireless Sensor Networks", The First IEEE International Workshop on Sensor Network Protocol and Applications(SNPA' 30), Anchorage, AK, USA, May 11, 2003
- [8] 박승창 "RFID/USN 관련 국내외 기술 및 시장의 최근 동향 분석" 전자정보센터
- [9] 김완석, 'RFID 응용과 분류,' IITA ITFIND 주간기술동향 제1177호, 2004. 12. 21.