情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

RFID/USN 보안 연구대상 및 향후 추세

김 동 성*, 박 종 서*

요 약

유비쿼터스 컴퓨팅은 향후 USN(Ubiquitous Sensor Network) 환경에서 구현될 것으로 예상되며, 유비쿼터스 컴퓨팅에서 RFID(Radio Frequency Identification)기술 기반의 응용 서비스들이 가장 먼저 활성화될 분야로 전망된다. RFID 분야에서의 보안은 RFID의 태그로 인한 프라이버시 침해가 가장 큰 문제점으로 인식되고 있으며, 기술적, 법적·제도적으로 개인의 프라이버시를 보장하기 위한 노력들이 진행 중이다. USN에서의 보안은 센서노드의 자원의 제약으로 인해 기존의 전통적인 보안과는 다른 관점에서의 접근이 필요하며, 키분배 및 관리, 안전한 라우팅 방법론, 센서네트워크에 대한 공격에 대한 안전한 네트워크 구축 등이 이슈들이다. 본 논문에서는 RFID와 USN의 보안 연구 대상에 대해서 살펴보고 이들에 대한 향후 연구 방향을 소개한다.

Ⅰ. 서 론

최근 유비쿼터스 컴퓨팅(Ubiquitous Computing)이라는 용어가 광범위하게 사용되고 있다. 유비쿼터스 컴퓨팅의 개념은 1988년 Xerox사의 마크와이저에 의해 "사용하기 쉬운 컴퓨터 연구"를 통해 처음으로 도출되었다. 유비쿼터스 컴퓨팅은 무수히 많은 마이크로 컴퓨터(칩)들이 가전제품, 건물, 도로, 의복과 같은 피조물은 물론 동·식물에 이르기까지 모든 일상사물과 환경에 식재되고 이들이 네트워크로 상호 유기적으로 연결되어 인간의 삶을 도와주는 신 개념의 컴퓨팅 환경을 말한다[3]. 유비쿼터스 컴퓨팅의 지향점은 5C(Computing, Communication, Connectivity, Contents, Calm)의 5Any(Anytime, Anywhere, Any-network, Any-device, Anyservice)화로 집약되며, 유비쿼터스 컴퓨팅의 조건은 모든 컴퓨터는 서로 연결되어야 하고, 이용자 눈에 보이지 않아야 하고, 언제 어디서나 사용가능해야 하며, 현실세계의 사물과 환경 속으로 스며들며 일상생활에 통합되어야 한다는 것이다. 유비쿼터스 컴퓨팅은 미국에서는 퍼베이시브 컴퓨팅(pervasive computing), 유럽에서는 Disappearing Computer 혹은 ambient computer, 일본에서는 Ubiquitous Network, 그리고 국내에서 유비쿼터스 센서 네트워크(Ubiquitous Sensor Netowk, 이하 USN)라는 명으로 추진되고 있다. 유비쿼터스 컴퓨팅을 달성하기 위한 관련기술로는 MEMS(Micro Elector Mechanical System, 미세전자기계시스템), 유무선 통합 IPv6기반의 BcN기술, RFID(Radio Frequency Identification, 주파수인식시스템) 등을 들 수 있다. 유비쿼터스 컴퓨팅 기술은 먼저 인식정보를 제공하는 RFID를 중심으로 발전하고 이에 감지 기능이 추가되고 이들 간의 네트워크가 구축되는 USN의 형태로 발전될 전망이며, 이러한 네트워크를 RFID/USN라고 할 수 있다[4]. RFID/USN은 필요한 모든 것(곳)에 RFID를 부착하고 이를 통하여 사물의 인식정보를 기본으로 주변의 환경정보(온도, 습도, 오염정보, 균열정보 등)까지 탐지하여 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 것을 말하는 것으로 궁극적으로 모든 사물에 컴퓨팅 및 통신기능을 부여하여 유비쿼터스 환경을 구현하기 위한 것이다. 향후 RFID/USN의 이용은 칩의 가격, 크기, 성능 등 센서 기술의 발전에 따라서 적용이 확산되면서 단계적으로 발전할 것으로 예상된다. RFID 태그가 소형화,

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터의 육성지원사업의 연구결과로 수행되었습니다.
* 한국항공대학교 컴퓨터공학과 네트워크보안연구실 ({dskim, jspark}@hau.ac.kr)
한국정보보호학회 조기경보시스템연구회 WG17 "유비쿼터스 센서 네트웍 보안" 운영자

지능화되는 반면에 가격은 수 센트로 저가화가 실현되면 다양하게 활용될 것으로 전망된다. RFID에 통신 기능이 부가되고 점차 주위 환경을 감지하는 센싱 기능이 부가되어 능동적으로 정보를 처리하는 지능형 초소형 네트워크 센서로 발전할 것이다. 현재의 고정된 개체 인식코드 획득수준에서 2007년경 다기능 태그에 의한 상황인지 처리수준으로 진화하고, 2010년 이후에는 개체 간 통신기능을 갖춘 USN으로 발전할 것이다. RFID/USN에서 언제 어디서나 사람, 사물, 다양한 콘텐츠의 이용과 더불어, 의식하지 못하는 사이에 개인정보는 물론 상황정보까지 누군가에 의해서 정보를 실시간 수집, 이용될 수 있기 때문에 개인의 프라이버시 침해 문제와 정보보안의 확보에 대한 대책이 시급한 실정이다. 현재 센서 네트워크 자체가 아직 미성숙 단계이기에 RFID/USN 환경에서 공격의 형태나 공격자를 추정하기 쉽지 않지만, 유무선 통합 환경에서 센서들을 통하여 장소와 시간에 관계없이 동작하는 센서 네트워크 환경에서의 공격이 현재의 공격보다 광범위하게 발생할 것으로 예상된다[23]. 공격 침해 대상도 기존의 전통적인 네트워크 환경에서는 컴퓨터의 저장된 정보 또는 통신 정보였다면, USN 환경에서는 개인의 모든 정보뿐만 아니라 사물, 신체의 정보까지를 포함한다. 공격 범위 면에서 기존의 공격들이 개인의 컴퓨터 혹은 컴퓨터 네트워크를 공격한 반면 USN 환경에서는 개인의 사적인 모든 공간이 공격의 범위가 된다. 따라서 공격 범위는 확대되고 또한 센서에 의해서 대상이 노출되어 있으므로 공격이 보다 용이하고 그 피해 규모는 확대되고 치명적일 것으로 전망된다. 그러므로 RFID/USN에서의 정보보호 기술은 매우 중요하다.

현재 RFID는 왕성하게 그 응용 범위를 넓혀가고 있지만, USN은 아직 미성숙한 단계이기 때문에 본 논문에서는 RFID/USN 보안에 대하여 RFID보안과 USN 보안에 대해서 각각 기술한다. RFID보안 분야에서는 리더와 태그 사이의 보안 기술, 이들을 지원하는 백엔드 시스템의 보안 문제에 대하여 살펴보고 향후 연구 방향을 제시한다. 한편 USN 보안 분야에서는 센서노드 사이의 안전한 키 관리, 안전한 라우팅 방법, 안전한 데이터 통합, 그리고 공격에 대한 예방 및 방어에 대한 연구를 간략히 소개하고 향후 연구 방향을 전망한다.

본 논문은 다음과 같이 구성되어 있다. Ⅱ장에서는 RFID 보안에 대해서 살펴보고, Ⅲ장에서는 USN 보안에 대해서 살펴본다. Ⅳ장에서는 결론을 내린다.

Ⅱ. RFID 보안

1. RFID 보안 제약사항과 취약점

RFID란 마이크로 칩을 내장한 태그, 라벨, 카드 등에 저장된 데이터를 무선 주파수를 이용하여 리더(Reader)기에서 자동 인식하는 기술을 말한다. 이러한 기술은 칩의 저장 능력과 인식능력이 향상되면서 유비쿼터스 환경에서 필수적인 기술로 유비쿼터스 컴퓨팅 기술을 실생활에 가장 먼저 접목시킬 기술로 주목받고 있다. 그러나 RFID 기술은 물리적인 공격, 위조, 스푸핑, 도청, 트래픽 분석, 서비스거부공격 등에 대한 취약점들을 가지고 있다. 이러한 취약점들은 개인이나 조직의 심각한 보안과 프라이버시 문제를 야기할 수 있다. RFID 기술을 위한 컴퓨팅 환경은 일반적인 네트워크와 인터넷 환경과는 달리 많은 제약사항을 가진다. RFID 태그 가격은 5센트 이하로 구현되어야 하고 전송데이터의 크기와 판독 시간도 한정되어 있으며, 리더 장비나 백앤드 시스템은 성능과 자원 측면에서 한계를 가진다. 따라서 RFID에 대한 보안 대책도 태그와 리더, 백엔드 시스템의 제약사항을 고려하여 설계되고 구현되어야 한다. 본 논문에서는 RFID 시스템이 IPv6 BcN기반의 RFID 시스템의 구현 관점에서의 필요한 요소들에 대한 보안 제약조건과 보안 기술을 중심으로 소개하고 USN환경에서의 RFID 시스템의 보안 기술은 배제한다.

1.1 RFID의 제약 조건

5센트 이하의 저렴한 RFID 태그는 기본적으로 수동형 형태로 사용되며, 태그가 사용할 수 있는 전력, 처리 시간, 저장 공간 게이트 수 등의 자원을 제한한다[9]. CRYPREC 보고서에 의하면 대칭키 암호 알고리즘의 구현이 6~13K 게이트로 알려져 있으며 대칭키 기반의 해쉬 함수도 유사한 수의 게이트가 요구될 것으로 예상된다. 더 적은 게이트 수가 요구되는 Tiny Encryption Algorithm[21]은 저렴한 RFID 태그에 향후 사용될 가능성이 있으나 현재 사용하기에 비싸다. 공개키 암호를 사용하기 위해서는 NTRU 공개키 암호의 경우 약 2달러의 비용이 소요되는 것으로 예측되므로 RFID에 사용하기 어려운 실정이다.

1.2 리더-태그 보안 문제

리더-태그 사이의 보안 문제는 태그에 탑재될 수

있는 하드웨어 기술을 한계적인데 반해 태그의 정보는 스푸핑, 위조, 서비스 공격, 물리적인 공격 등을 시도하기 비교적 쉽기 때문에 야기된다[1]. 첫 번째, 스푸핑에 관련된 모델은 전후방 범위(Forward and Backward Range) 모델을 예로 들 수 있으며, 리더가 태그에게 질의를 보낼 수 있는 물리적 범위인 전방범위(Forward Range)가 태그가 리더에게 질의에 대한 응답을 보낼 수 있는 물리적 범위인 Backward range보다 작기 때문에 발생한다. 도청자가 전방범위(Forward Range)안에 있을 때 RFID의 리더는 태그의 정보를 계속 전송하게 되며 도청자는 이를 성공적으로 도청할 수 있게 된다. 두 번째, 재쓰기 가능한 태그(Re-Writable Tag)에 의한 문제로, 가령 EEPROM을 채택한 태그는 악의적인 공격자에 의해 변경되거나 위조될 가능성이 존재한다. 세 번째, 서비스 거부 공격에 의한 문제로, 무의미한 태그를 임의적으로 생성하여 질의를 송신하는 태그가 있을 경우에 리더가 정당한 태그에게 서비스를 제공하지 못할 위험성을 가진다. 네 번째, RFID 태그에 대하여 물리적인 공격을 가할 때의 문제이다. 전기자기적인 전파방해 혹은 쇼크를 주어 태그를 파괴하는 공격 등이 그 예이다.

1.3 백엔드 시스템 보안 문제

백엔드 시스템에 관한 보안문제는 RFID 기술을 구현하기 위한 태그와 리더가 사용하는 네트워크와 정보 자원들에 관한 취약점으로 인해 기인한다. 백엔드 시스템이 기존의 전통적인 네트워크 기반에서 구성된다는 기존의 네트워크와 인터넷의 취약점을 가지게 되며, RFID 기술이 능동형 태그 기술과 통신 기술의 진화로 지능화된다면 USN의 보안 취약점을 가지게 될 것이다. 현재 RFID 기술에 대한 백엔드 시스템은 기존의 유무선 네트워크 기술을 사용하며, 다양한 리더를 지원하는 미들웨어, RFID의 정보를 제공하는 ONS(Object Name Service)서버와 상품의 제품 정보를 저장하는 PML(Physical Markup Language) 서버를 필요로 한다. 유비쿼터스 컴퓨팅 환경을 구축하기 위하여 차세대 핵심 기술인 RFID 기술을 기반으로 하는 스마트 객체를 활용하는 다양한 응용 서비스를 조기에 구축하기 위해서는 스마트 객체와 응용 서비스를 이음새 없이 연결하는 미들웨어가 요구된다. ONS서버와 PML서버에 대한 보안 문제는 자격조건이 없는 호스트로부터 올바르지 않은 정보를 수용하거나 사용할 때 발생한다. 또한 이들 서버의 처리용량이 한정되어 있기 때문에 서비스 거부 공격을 이들 서버에 실행할 경우에 RFID 시스템은 타격을 받을 수 있다. 보다 심각한 문제로는 이들 ONS서버와 PML서버의 데이터베이스에 저장된 정보가 유출될 경우에 발생한다.

2. RFID 보안 기술

RFID의 보안 대책은 크게 리더와 태그 사이의 보안과 이것들을 지원하기 위한 백엔드 시스템의 보안으로 나누어 볼 수 있다.

2.1 리더-태그 보안 방안

최근의 RFID에 대한 보안 대책은 대부분 리더와 태그 사이의 보안 기술에 초점이 맞추어져 있다. 현재 제안된 기술을 인증 및 접근 제어, 도청 방지, 그리고 정보 차단의 3가지 분야로 분류하여 간략히 소개한다[7].

첫째, 인증 및 접근 제어 기술은 해쉬 기반(Hash-Based) 접근 제어나 랜덤(Randomized) 접근 제어 방법론을 제안하였다[22]. 해쉬 기반 접근 제어 방법은 태그를 잠그고 풀기 위하여, 리더가 랜덤한 키를 해쉬하여 데이터베이스에 저장하고 이를 태그의 메타 ID로 사용한다. 랜덤 접근 제어 방법에서 태그는 메타 ID뿐만 아니라 난수 R을 사용하여 보안성을 높일 수 있지만, 리더가 자신이 잠갔던 태그가 많을수록 태그를 해제하는데 걸리는 시간이 늘어난다는 단점을 가진다.

둘째, 도청 방지 기술 분야에서는 고요한 트리워킹(Silent Tree-walking)이나 랜덤 트리워킹(Randomized Tree-walking) 같은 방법이 제안되었다. 또한 비밀키 암호화 방식을 사용하여 암호화된 데이터를 전송하는 방법과 공개키 암호화 방식을 사용하여 암호화된 정보를 태그에 기록하는 재암호화(Re-encryption) 방법이 있다[13]. 이 기술은 태그가 리더에게 보내는 데이터는 도청자가 직접 들을 수 없다는 점에 착안하여 리더가 태그의 정보를 부르지만 태그가 리더에게 보낸 마지막 데이터와 리더가 태그에게 보내고 싶은 데이터를 XOR연산하는 방식을 사용한다. 랜덤 트리워킹은 고요한 트리워킹과 유사한 방식으로 태그가 난수를 생성하여 이를 리더에 보내고 이를 기초로 하여 탐색을 시도하는 방식이다. 재암호화 방식은 Elgamal 공개키 암호화 방식을 사용하여 암호화한 고유번호를 태그에 덮어쓰는 방식으로 이루어진다.

셋째, 정보 차단을 위하여 물리적인 방법으로 킬 태그(kill tag) 방법이나 패러데이 우리(Faraday Cage), 방해전파 방법(Active Jamming), 차단자 태그(Blocker Tag)를 사용하는 방법들이 제안되었다[14]. 킬

태그 방법은 재사용이 불필요한 분야에서 사용이 가능하며, 태그가 8비트의 패스워드와 킬(kill)명령을 받을 경우 그 태그가 비활성화 되게 된다. 패러데이 우리는 무선 주파수가 침투하지 못하도록 금속성의 그물이나 박막을 입히는 방법이며, 방해전파 방법은 리더가 태그의 정보를 읽지 못하도록 방해신호를 보내는 물건을 소비자가 소지하는 방식이다. 차단자 태그는 리더의 모든 질의에 '그렇다' 혹은 '아니다'라는 일관적인 응답만 하는 태그들로, 보안 구역(Privacy zone)을 만들어서 차단자 태그와 동일한 시작 비트를 갖는 태그들을 안전하게 보호할 수 있다.

2.2 백엔드 시스템 보안 방안

이전 절에서 주로 리더와 태그 사이의 보안 기술들을 살펴보았다. 본 절에는 백엔드 시스템의 보안 방안에 대해서 소개한다. 현재 미들웨어, ONS 서버, PML 서버 등 백엔드 시스템을 보호하기 위한 기술의 제안이 미흡한 실정이다. 안전한 RFID 시스템을 구축하기 위해서 각 구성 요소별로 보안 방안이 필요하다. 첫째, 리더에서 RFID 태그를 통한 서비스 공격을 탐지하고 방어하는 연구가 필요하다. 둘째 미들웨어는 각 구성요소와 안전한 통신채널을 제공하여야 하며, 서비스 거부 공격 등의 공격을 탐지하고 차단하는 기술이 필요하다. 또한 ONS 서버는 ONS 질의의 보호가 필요하다. 끝으로, PML서버에서는 제품 정보 검색을 위한 접근제어 기술이 필요하다. 요약하면, 백엔드 시스템 보안 방안은 백엔드 시스템의 구성요소에 대한 보안 방안과 백엔드 시스템간의 안전한 통신 채널 확보 및 서비스 거부 공격에 대한 방어대책이 필요하다. 백엔드 시스템 구성요소에 대해서는 DNS와 XML 관련 보안 기술이 사용될 것으로 예상되며, DNS의 보안과 관련해서는 DNSSEC이 기술이 ONS서버에 적용될 수 있을 것으로 보이며, XML의 경우는 W3C의 XML signature, XML encryption 등과 OASIS의 SAML, XACML 등의 기술이 적용가능하리라 본다[21]. 백엔드 시스템간의 통신에서는 기존의 인터넷 보안 기술이 적용될 수 있을 것으로 예상되며, IPSec이나 SSL/TLS 같은 암호 기반의 안전한 통신 채널 보장 기술과 안전한 라우팅 기술 등을 적용할 수 있을 것으로 예상된다.

3. RFID 보안 연구 방향

RFID 보안기술에서 리더와 태그 보안 향후 연구 방향은 크게 2가지로 요약해볼 수 있다[22].

리더와 태그 사이에서의 보안 연구 방향은 첫 번째, 안전한 RFID 프로토콜의 개발이다. 새로운 RFID 프로토콜은 도청, 고장 유도 해석(fault induction), 전력 해석(power analysis)에 강하도록 설계시 고려되어야 한다. 인증 및 접근 제어 방식은 긴 범위의 도청에 대해서는 보안성을 제공하지만 가까이에 있는 도청자들과 고장 유도 방법에 여전히 취약하다.

두 번째, 하드웨어 기반의 보안 기술의 개발이다. RFID 시스템의 보안은 하드웨어 기반의 효율적인 해쉬 함수, 대칭키 암호화, 메시지 인증, 난수 생성기 등의 지속적인 발전이 매우 중요하다. 저가격의 하드웨어 해쉬 함수로는 셀룰러 오토마타(cellular automata)와 비선형 피드백 쉬프트 레지스터(nonlinear feedback shift register)를 들 수 있다. 향후 공개키 암호화 방식을 지원하는 초경량의 암호화 알고리즘이 개발되어야 할 것이다.

백엔드 시스템 측면에서의 연구는 리더와 태그 보안보다 연구 진행도가 늦은 편이다. USN 환경이 아니라 전통적인 네트워크 환경 상에서 RFID 시스템을 구현하는 측면에서만 고려할 때 두 가지 정도로 요약해 볼 수 있다. 첫 번째 ONS 서버와 PML 서버 등 백엔드 시스템 구성 요소에 대한 보안 기술이 DNSSEC과 XML보안 기술의 발전과 더불어 연구되어야 할 것으로 전망된다. 둘째, 미들웨어 측면에서 우선적으로 태그와 리더에 대한 인증 및 접근 제어 기술을 제공해야 하며, 향후 기밀성을 포함한 다양한 보안 서비스 모델을 지원하여야 할 것이다. 또한 불법적인 리더와 불법적인 태그를 감지하는 기술이 연구되어야 할 것이며, 비정상 유해 트래픽을 탐지하고 차단하는 기술도 진행되어야 할 것으로 예상된다. 향후 USN 환경으로 기반 환경이 변형 될 경우에는 USN의 보안 기술과 RFID 기술이 결합되어 좀 더 복잡한 형태의 구성이 될 것이며, 전력과 자원의 제한적인 요소가 세밀하게 고려되는 기술이 설계 및 구현되어야 할 것으로 보인다.

한편, RFID에 대한 보안 기술은 RFID 태그와 리더로 인한 개인의 프라이버시 침해와 관련되어 있다. 이러한 문제는 사용자의 프라이버시를 보호하기 위한 법적, 제도적 측면의 고려가 시도되고 있으며[제 4차 빅브라더 보고서, RFID와 프라이버시], 기술적인 방법과 함께 같이 개선되어야 할 것으로 사료된다.

Ⅲ. USN 보안

실세계에 대규모의 센서 네트워크를 도입하는데 몇

가지 장애물이 존재한다. 이 장에서는 USN 특징들에 대해서 간략히 살펴보고, USN의 보안 취약점에 대한 기존 보안 기술의 연구 결과와 향후 연구 방향을 소개한다.

1. USN 보안 문제점

USN 환경에서의 보안 문제는 기기들이 무선으로 데이터를 송수신하는 특성과 각 기기들의 컴퓨팅 능력과 전력 관리 등의 문제를 가지고 있으므로 전통적인 네트워크의 보안 문제보다 복잡하며 이들 구성 장비에 대한 공격은 쉬운 반면 이러한 공격에 대한 방어를 수행하는 작업은 기존의 방법보다 더 어려울 것으로 전망된다. 또한 USN 환경에서는 센서들이 생활의 곳곳에 널리 퍼져 있기 때문에 개인 정보보호, 시스템 혼란 방지, 확장성, 보안 등이 장기적 이슈가 될 문제점이 노출되고 있다.

USN은 기존의 무선 네트워크와 다음과 같은 차이점들을 가진다[6]. 첫째, USN의 센서 노드의 수가 애드혹(Ad-hoc) 네트워크에서 사용하는 노드 수의 수배가 될 수 있으며, 둘째, 센서 노드는 밀집되어 분포가 되며, 셋째, 센서 노드의 오동작(Failure) 을 허용하며, 넷째, 센서 네트워크의 토폴로지는 매우 수시로 변화를 하며, 다섯째, 센서 노드는 브로드캐스트(broadcast) 통신 환경을 사용하며, 여섯째, 전력, 컴퓨팅 능력과 그리고 메모리의 용량이 제한적이며, 일곱째, 센서의 개수와 오버헤드 때문에 센서 노드는 글로벌 인식자(ID)를 갖지 않아야 한다. 센서 네트워크의 이러한 특성들을 고려하지 않고, 보안 문제를 해결하려면, 컴퓨팅 문제가 발생되어 노드와 네트워크 전체에 심각한 부하를 주게 된다. 따라서 USN에 적합하게 구현된 알고리즘, 키 분배 및 인증 프로토콜의 개발이 현실적으로 가장 필요하다.

2. USN 보안 기술

이번 절에서는 USN에서의 보안 기술 분야를 크게 4가지로 나누어 보고 현재 제안된 기술들을 간략히 소개한다.

2.1 암호화 알고리즘

USN 환경에서는 AES, DES, SEED 등 대칭키 방식의 국제표준 암호알고리즘의 사용이 부적합하다. 저전력 계산 환경(Smart Dust, RFID)에 적합한 해쉬 함수의 개발이 필요하다. UMAC의 경우, WPI (Worcester Polytechnic Institute) 대학의 Cryptography and Information Security Lab.에서 2004년 구현 결과가 제시되었다. 한편, 공개키 알고리즘의 하드웨어 구현이 필요한 사항이다. 2004년 Rabin, NTRU, ECC등의 공개키 알고리즘에 대한 구현 결과 제시하였고, NTRU의 경우 20μW의 저전력에 3000개의 게이트만 필요하므로, 경량화된 센서 노드에 탑재 가능하다고 알려져 있다.

2.2 키 관리

USN에서는 노드가 신뢰받은 인증기관을 통해 인증을 받는 형식이 아니기 때문에, 멀티 홉 방식에 의해 라우팅을 수행할 경우 악의적인 중간 노드에 의해 데이터의 무결성 및 기밀성 문제가 발생할 수 있다. 특히, 매체를 신뢰할 수 없는 상황에서 암호를 사용하므로, 암호키에 크게 의존하게 된다. 또한, USN은 모든 노드들이 분산되어 있고, 어떠한 고정된 기반구조도 없으며, 모든 노드가 공평하게 역할을 나누어 갖는다는 특징을 갖는다. 한편으로, 보안 문제가 확실히 해결되다보면, 컴퓨팅 문제가 발생되어, 노드와 네트워크 전체에 심각한 부하를 주게 되므로, USN에 적합하게 구현된 알고리즘, 키 분배 및 인증 프로토콜의 개발이 현실적으로 가장 필요하다. 즉, 키 사이에 신뢰할 수 있는 관계를 형성하고, 이를 USN 전반에 분배하는 것이 주요 관심 사항이라 할 수 있다. 즉, USN환경에서의 센서 노드와 노드 사이에 안전한 통신채널을 구축하는 것이 가장 큰 이슈이다. 가장 먼저 제안되었던 보안 프로토콜은 SPIN으로 SNEP(Sensor Network Encryption Protocol)과 μTESLA로 구성되며 기존의 무선랜의 액세스 포인트와 유사한 역할을 하는 베이스 스테이션(base station)이 있는 것으로 가정한다[22]. 그러나 최근의 경향은 USN환경에서는 베이스 스테이션을 포함하지 않는다는 것을 가정한다. 최근의 제안되었던 프로토콜은 EG (Eschenauer-Gligor) 프로토콜[12], Random pair-wise scheme CPS[10], Polynomial-based scheme LN[15], Grid-based key predistri-bution[16] 등이 제안되었다. 이러한 키 관리 스킴은 대칭키 풀을 선택하고 무작위로 키를 선택하여 센서 노드에 할당하고 두개의 노드는 자신의 대칭키 풀을 탐색하여 상대방이 같은 공통키를 소유하고 있으면 이 키를 세션키로 사용하는 방식을 사용한다. 센서 노드가 악의적인 센서노드에 의해 침해당했을 경우(node capture)에

도 복원력(resilience)을 가지느냐가 중요한 평가 항목으로 사용되고 있다.

2.3 라우팅 보안

USN의 라우팅 프로토콜의 보안은 초기 설계시에 크게 고려되지 않았다. 안전한 라우팅을 지원하기 위해서는 메시지에 대한 무결성, 인증, 가용성을 보장하여야 하며, 토폴로지 변화에 능동적으로 대처해야 하며, 저전력 라우팅 알고리즘 필요하다. 또한 시빌 공격(sybil attack)[17], 웜홀 공격(wormhole attack)[18] 등 다양한 공격에 대응 가능하여야 한다. 시빌 공격은 한 노드가 다중의 식별자를 가지는 것으로, 대책은 주파수 대역 검사, random key predistrib ution scheme을 사용한 노드 인증, 다른 외부의 서버를 이용한 센서노드의 등록방법, 그리고 위치에 대한 거리 식별을 이용한 방법 등이 있다. 웜홀 공격은 USN을 구성하는 센서 노드를 훼손하여 모든 트래픽이 그 노드로 통과하도록 만드는 싱크홀(sinkhole)을 통하여 트래픽을 가중시킴으로써 안전한 라우팅을 방해하는 방법이다. 앞으로 이외의 다른 USN에 대한 공격 방법이 등장할 것으로 예상되며, 라우팅에 있어서 안전한 환경이 더욱 중요한 이슈가 될 것이다.

한편 라우팅 분야에서 센서 네트워크의 에너지 소비 문제와 신뢰성 있는 데이터 전송의 두 가지 성능상의 문제를 해결해야 한다[5]. 센서 노드의 전체 소모 전력의 20-60%를 무선 통신에 사용하는 RF모듈이 차지하고 있다. 따라서 센서 노드와 센서 네트워크의 평균 작동 시간을 연장하기 위하여 저전력 통신 방법이 필요하다. 신뢰성 있는 데이터 전송 문제에 관해서는, 센서 노드에 장착된 소형 RF모듈은 약 50%의 높은 패킷 에러율을 가지며 이는 센서 네트워크의 유용성을 심각하게 떨어드릴 뿐만 아니라 불필요하게 통신 에너지를 낭비하게 한다. 이 두 가지 문제점을 해결하기 위하여 연결층에서 ARQ를 사용하여 완전한 전송을 보장하지만 하나의 패킷을 전달하는데 많은 에너지를 소모하는 RMST(Reliable Data Transport in Sensor Networks)와 이를 개선하기 위해서 이벤트 기반의 통신에너지를 줄일 수 있는 부분적인 신뢰성 전송 규약인 ESTR(Event-to-Sink Reliable Transport in Wireless Sensor Networks)가 제안되었다. 데이터 전송의 신뢰성을 향상하면서 에너지 소모를 줄이는 연구가 계속 진행중에 있다.

2.4 기타 이슈

기존의 역할 기반 접근제어(Role-Based Access Control: RBAC)에서 접근 결정은 개개인의 사용자들이 조직원으로서 요구되는 역할에 근거하여 이루어진다. 그러나 기존의 역할 기반 접근 제어 모델로는 상황에 따르는 접근 제어를 수행할 수 없다. 보안의 강화와 사용자의 상황에 따른 유연한 정보 접근을 위하여 상황 정보를 접근제어에 이용하는 연구가 진행되고 있다[2]. 역할 기반 접근 제어 결정의 제약사항을 제약사항으로 이용하는 xoRBAC[19] 모델, 접근 제어 결정에 사용자 역할, 객체 역할, 환경 역할을 사용함으로써 기존 역할 기반 접근 제어를 확장한 GRBAC (Generalized Role Based Access Control) 모델[11] 등이 제안되었다.

센서 네트워크의 미들웨어의 측면에서는 크게 보안과 감내 관리의 문제로 요약해 볼 수 있다. 먼저 보안 측면에서 센서 네트워크의 초소형 노드들은 대부분 메모리 관리부가 없기 때문에 신뢰할 수 없는 의심스러운 코드가 수행되지 않도록 미들웨어 플랫폼에 추가적인 보안 기능이 요구된다. 장애 관리 측면에서는 네트워크의 신뢰도와 가용이 센서 네트워크가 사용하는 무선 환경보다 더 낮기 때문에 통신 실패가 훨씬 자주 발생하므로 장애 극복 기능을 가져야 한다.

3. USN 보안 연구 방향

현재 USN의 보안은 기존의 네트워크와 인터넷 보안 기술의 제약사항을 고려하여 변형하고 적용하는 형태가 대부분이다. 예를 들어 암호 기술 분야에서는 암호 알고리즘을 저전력화, 경량화, 하드웨어화를 시도하고 있다. 또한 기존의 ad-hoc 네트워크 기술을 기반으로 하여 이동형 센서 노드들에 대한 보안을 적용하려고 하고 있는 실정이다. USN 보안에 있어서 한계적인 자원의 전력 소비의 제약사항은 보안 기술을 적용하기에 가장 큰 걸림돌이다. 이러한 제약사항 하에서 USN의 환경에 적합한 암호 알고리즘을 새로 개발하고 프로토콜을 개발하는 것은 쉽지 않지만, USN이 성숙되기 전에 보안에 대한 기술을 발전시키는 것을 선행되어야 할 것이다. 앞 절에서 언급하였던 이슈들 중에서 가장 먼저 해결해야 할 문제는 키를 교환하는 것이다. 앞서 기술한 암호화 알고리즘의 적용, 안전한 라우팅 등은 세션 키를 먼저 공유하는 문제가 해결되어야 적용이 용이하며 그 안전성을 보장할 수 있다. 따라서 브로드캐스팅 방식으로 키를 안전하게 사

전 분배하는 연구가 매우 중요하며 현재 연구 중인 분야에서 많은 비중을 차지하고 있다. 아직 USN의 환경이 충분히 성숙하지 않았기 때문에 현재 발생가능한 공격의 수는 그렇게 많지 않지만, 기존의 전통적인 네트워크보다 악의적인 공격자에 의해 노출되는 정도는 큰 반면에 공격에 대한 보안 대책은 센서 노드들 간의 인증과 암호화에 치우진 면이 많다. 향후 공격에 대하여 탐지하고 감내하는 연구가 더욱 진행되어야 할 것으로 전망된다.

Ⅳ. 결 론

본 논문에서는 RFID/USN의 현재 보안 연구 상황과 향후 연구 방향에 대하여 각각 기술하였다. RFID 보안에 있어서는 리더와 태그 사이의 보안, 백엔드 시스템에 대한 보안으로 나누어 간략히 소개하였다. 또한 향후 RFID 시스템의 기반 네트워크로 사용되어질 USN의 보안 문제와 현재 연구 동향 그리고 향후 연구 방향을 살펴보았다. 그러나 RFID/USN의 정보보호는 현재 USN의 미성숙한 단계에서는 가시적으로 정의하기 어렵다. 현재 RFID기술을 이용한 많은 응용 분야들이 등장하고 있으며, 향후 RFID에 대한 보안과 프라이버시는 매우 중요한 기술이다. 한편 무선 네트워크 기술과 더불어 센서 네트워크 기술이 더욱 성숙되면 USN 보안 기술의 중요성 또한 증대될 것으로 보며 각 보안 분야에서 협력을 통한 기술 개발이 더욱 필요하리라 전망된다.

Ⅴ. WG 17 소개

한국조기경보포럼의 WG 17는 RFID/USN 보안 기술과 관련한 분과이다. 이 분과에서는 RFID 태그와 리더, 백엔드 시스템에 대한 보안 기술을 분석하고, 안전한 RFID시스템의 도입을 위한 보안 기술을 제시하는 것을 주목적으로 한다. 한편, 향후 RFID의 백본망으로 사용될 것으로 예상되는 USN의 취약점과 이에 대한 보안 기술을 논의하고 이를 해결하기 위한 방안을 연구한다.

⊙ 연구 방향
- RFID/USN과 관련된 논문 및 최근 동향 연구
- 국내외 RFID 도입시 보안 기술의 사용방안 연구
- 국내외 USN의 보안 취약점 및 해결 방안 연구

⊙ 분과 운영
- 월 1~2회 온라인 및 오프라인 모임 실시
- 정규회원 중심 국내외 RFID/USN 보안 기술 발표 세미나 및 대안제시
- 비정규 회원의 자유로운 세미나 참여 및 토론

참 고 문 헌

[1] 강전일, 박주성, 양대헌, "RFID 시스템에서의 프라이버시 보호 기술", 한국정보보호학회학회지, 제14권 6호, pp. 28-36, 2004

[2] 변창우, 박석, 손상혁, "센서 네트워크 환경에서의 데이터 관리", 정보과학회지, 제 22권 제12호,pp. 31-40, 2004

[3] 한국전산원, "유비쿼터스 사회의 발전단계와 특성", NCA CIO Report, 04-16호

[4] 유승화, "RFID/USN 표준화 추진방향", TTA 저널, 제 94호, pp. 12-18

[5] 임근수, 김지홍, 고건, "센서 네트워크를 위한 저전력 통신 기법, 정보과학회지, 제 22권 제12호, 2004, pp. 21-30, 2004

[6] 임지형, 이병길, 김현곤, 정교일, 양대헌, "유비쿼터스 및 Ad Hoc 네트워크 망에서의 정보보호 분석", 한국정보통신연구진흥원(IITA)

[7] 정병호, "RFID/USN 환경에서의 정보보호", 제9회 정보보호심포지움, pp 447-463, 2004

[8] 제 4차 빅브라더 보고서, RFID와 프라이버시

[9] 주학수, "RFID 시스템의 보안 및 프라이버시 보호를 위한 기술 분석", IT리포트, 전자정보센터

[10] Haowen Chan, Adrian Perrig, Dawn Song, "Random Key Predistribution Schemes for Sensor Networks" In 2003 IEEE Symposium on Research in Security and Privacy

[11] M. Covington, M. Moyer, and M. Ahamad, "Generalized role-based access control for securing future applications", In 23rd National Information Systems Security Conference, Baltimore, MD, October 2000.

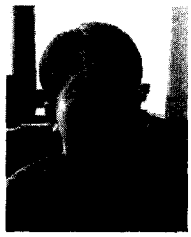
[12] Laurent Eschenauer and Virgil D. Gligor, "A keymanagement scheme for distributed sensor networks" In Proceedings of the 9th ACM Conference on

Computer and Communication Security, pages 41 - 47, November 2002.
[13] Ari Juels and Ravikanth Pappu, "Squealing Euros: Privacy Protection in RFID-Enalbed Banknotes", Financial Cryptography 2003, Springer-Verlag, 2003
[14] Ari Juels, Ronald L. Rivest, and Michael Szydlo, "The Block Tag: Selective Blocking of RFID Tags for Consumer Privacy", 8th ACM Conference on Computer and Communications Security, pp. 103-111, ACM Press, 2003
[15] D. Liu, P. Ning, K. Sun, "Efficient self-healing group key distribution with revocation capability", Proceedings of the 10th ACM conference on Computer and communication security, 2003.
[16] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks", The 10th ACM Conference on Computer and Communications Security, 2003.
[17] James Newsome, Elaine Shi, Dawn Song and Adrian Perrig, "The Sybil Attack in Sensor Networks : Analysis and Defenses", In Third International Symposium on Information Processingin Sensor Networks (IPSN 2004)
[18] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Packet Leashes: ADefense against Wormhole Attacks in Wireless Ad Hoc Networks", In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003.
[19] Neumann G, Strembeck M., "Design and implementation of a flexible RBAC-service in an object-oriented scripting language", Proceedings of the 8th ACM Conference on Computer and Communication Security, Philadelphia, PA, November 2001.
[20] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, "SPIN: Security Protocols for Sensor Networks", Wireless Networks Journal, 8(5):521-534, Sep 2002
[21] David J. Wheeler and Robert M. Needham, "TEA, a Tiny Encryption Algorithm", Technical report, Computer Laboratory, University of Cambridge, 1995.
[22] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", First International Conference on Security and Pervasive Computing, 2003
[23] 임종인, "유비쿼터스 네트워크 보안", 고려대학교 정보보호 대학원, 2004. 8 (http://www.secui.com/seminar/ IPS_ubiquitous.pdf)

〈著 者 紹 介〉

김 동 성 (Dong Seong Kim)
학생회원

2001년 2월 : 한국항공대학교 항공전자공학과 졸업
2003년 2월 : 한국항공대학교 컴퓨터공학과 석사
2003년 3월~현재 : 한국항공대학교 컴퓨터공학과 박사과정
〈관심분야〉 시스템 및 네트워크 보안, 인공지능, 데이터 마이닝



박 종 서 (Jong Sou Park)
정회원

1983년 : 한국항공대학교 항공통신공학과 졸업
1986년 : North Carolina State Univ. 석사
1994년 : Pennsylvania State Univ. 공학박사
1996년~현재 : 한국항공대학교 컴퓨터공학과 부교수
〈관심분야〉 시스템 및 네트워크 보안, 하드웨어디자인, 임베디드 시스템