

## 보안을 고려한 RFID/USN 기반의

### 능동형 창고 상태 관리 시스템

전영준<sup>○</sup>, 최용식, 박상현, 한 수, 신승호  
인천대학교 컴퓨터공학과

{0961144<sup>○</sup>, mars, tank1862, puckktan, shin0354}@incheon.ac.kr

#### Active Warehouse Condition Management System based on RFID/USN Security

Young-Jun John<sup>○</sup>, Yong-Sik Choi, Sang-Hyun Park, Soo Han and Seung-Ho Shin  
Department of Computer Science & Engineering, University of Incheon

#### 요 약

RFID/USN은 유비쿼터스 사회의 중요한 기반 인프라로서 고려되고 있다. 또한 다양한 연구를 통해 실용적인 접목이 시도되고 있다. 특히 물류 시스템에서 물류의 입출 재고와 상태 관리를 위한 연구가 진행 중에 있으며 이는 물류 보관 단위인 팔레트(Pallet)에 RFID 태그를 부착하여 입/출고시의 물류를 식별하고, Zigbee 무선 통신기능을 가진 센서 모듈에 의해 물류의 환경 상태 정보를 파악하는 형태로 이루어진다. 본 논문은 RFID/USN 기반의 창고 상태 관리 시스템에서 상태정보 습득 과정의 보안적용을 위한 시스템을 구성을 주된 목적으로 한다. 부가적으로 상태정보 습득에 사용되는 이동형 단말장치의 기능에 대해서 제안한다. 창고 내에 배치되는 RFID와 센서노드간의 적용 관계 또한 정의한다. 결과적으로 본 논문은 의사판단의 주체인 현장 관리자에 적절한 제어 정보의 제공과 센서의 동작을 제어하기 위한 RFID tag 보안 접근, 그리고 센서 노드 자체의 생존성이라는 세 가지 관점의 절충점을 찾기 위한 시도로서 설계하였다.

#### 1. 서 론

WSN(Wireless Sensor Network, WSN)은 국내에서 USN(Ubiquitous Sensor Network)이라는 용어로 많이 사용되고 있다. 유비쿼터스 센서 네트워크는 광범위하게 설치되어 있는 유무선 네트워크 인프라에서 상황 인식을 위한 다양한 센서들을 장착한 형태를 말한다. 센싱된 정보를 이용하여 응용서비스를 제공하는 예로 지능형 물류관리 시스템과 시큐리티, 침입 탐지, 군사, 방재 시스템 등을 들 수 있다[1]. RFID 기술은 이진 정보를 보관하고 있는 RF 태그와 트랜스폰더 형태로 구성된다. RF 태그는 반도체 칩과 안테나로 구성되며, 칩에는 특정 정보를 저장하고, 트랜스폰더의 요청에 의해 자신의 정보를 전달한다[2][3].

USN에서 핵심 단말인 센서노드와 RFID의 RF tag는 각각의 영역에서 고유한 특징을 가지고 있다. RF Tag는 센서 노드에 비해 매우 저렴하며, 별도의 전원 없이 운용이 가능하다. 센서 노드는 부착된 센싱 장비에 의해 실시간의 환경 정보를 제공하며 RF tag에 비해 기억력과 데이터 처리능력 면에서 월등히 앞선다. 이러한 대비되는 특징으로 인해 RF tag에 대해서는 자료의 처리(processing)보다 단순한 구조의 고속 RF 통신을 주목하게 한다. 센서노드에 대해서는 제한된 시간동안 센서노드의 프로세서를 통해 자료를 처리하고 통신한 후 노드를 sleep 하는 운용전략을 취하게 된다.

물류에서 USN/RFID 기술이 조합된 응용은 물류 집하장이나 수출입 항의 경우 창고에 보관된 다양한 제품의 관리를 말한다. 보관되는 제품들에 따라 온도, 습도, 압력, 빛 등의 상태정보가 제품의 품질을 좌우하는 경우가 있으며 이에 따라 제품의 출고시기와 유통기간이 변경되기도 한다. 이 과정에서 특정 센서의 동작을 제어하기 위해 보안이 적용되어 특정 사용자에게 정보를 제공할 필요가 있다.

따라서 입고되는 시점에 보관되는 제품의 이력을 관리하고 상태를 파악하여 창고물품의 전반적인 상황을 최적의 상태로 관리할 필요가 있는 것이다. 이런 이유로 제품의 이력정보를 확인할 수 있는 지능형 창고 시스템이 필요하다. 이에 따른 창고 관리 시스템의 주요 구성을 세분화 하면 다음과 같다. 센싱 대상이 되는 물품, 그리고 센싱 정보가 최종적으로 수집되고 기록되는 서버, 마지막으로 센서와 물품관리를 위해 현장 관리자가 사용하는 이동형 단말장치이다. 이러한 시스템 구성 과정에서 자동적으로 수집되는 물품의 상태정보와 이동형 장비를 통해 물품을 배치하거나 특정 센서의 정보를 취득하기 위해 명령을 내리는 과정을 분할한다. 현장 관리자는 보안코드를 습득하고 인증받아 특정 센서가 원하는 동작을 수행하도록 명령한다. 본 논문은 RFID/USN 기반의 창고 상태 관리 시스템에서 상태정보 습득 과정의 보안적용과 관리 시스템을 구성하는데 있다. 2장에서는 RFID/USN 기반 기술들과 적용될 수 있는 보안프로토콜에 대해 설명한다. 3장에서는 창고 관리시

시스템을 3가지 요소로 구분하여 설명하고, 상태 관리를 위한 RFID/USN 보안 적용 요소를 설계한다. 4장에서는 결론 및 향후 연구 방향을 제시하는 것으로 정리한다.

2. 관련 연구

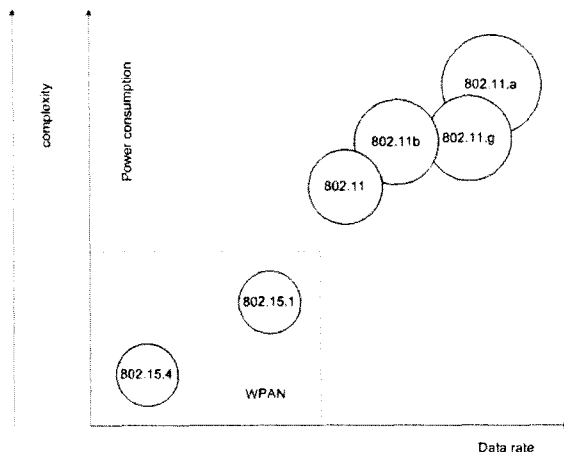
2.1 RFID 기반 기술

2003년 10월 설립된 EPCGlobal은 Savant(마들웨어), ONS(Object Name Service), PML(Physical Markup Language), 태그, 리더기, EPC(Electronic Product Code), EPCIS(EPC Information Service) 등의 기술을 기반으로 EPC 네트워크를 구성하기 위한 기술을 개발과 표준화를 추진 중에 있다. 태그는 반도체 칩과 안테나를 가지고 있으며, 칩에 있는 메모리를 통해 태그 식별을 위한 EPC 코드가 저장된다. RFID 시스템은 전자기파 무선 시스템으로 분류되며, 다른 무선 서비스들의 충돌을 피하기 위해서 적절한 동작 주파수가 필요하게 된다[4]. RFID를 위한 주파수 대역으로는 인식 거리가 짧은 135KHz 이하와 13.56MHz용 저주파 태그와 인식거리가 수 미터에 달하는 433.92MHz, 900MHz, 2.45GHz 등이 있다. 주변 지형지물, 제품정보, 주파수와 같은 환경에 따라 인식거리에 차이가 있다. <표 1>은 주파수 대역별 인식거리 및 적용분야를 나타낸다[5]. EPC 코드는 기존의 바코드 관리기관에서 제안한 RFID용 코드체계이며, 64비트, 96비트, 256비트의 상품번호 체계를 기반으로 한다. Savant는 PML 쿼리에 대하여 다양한 서비스를 제공하기 위해 마들웨어의 기능을 수행한다. PML은 XML을 기반으로 EPCs와 관련된 Report 기능과 구조화된 쿼리 지원을 목표로 한다.

2.2 USN 기반 기술

유비쿼터스 센서 네트워크는 WLAN을 위한 IEEE 802.11과 WPAN을 위한 IEEE 802.15의 규약이 있다. IEEE 802.15.1에 Bluetooth가 정의되고 있으며, Zigbee는 802.15.4에 표준이 정의된다[6]. Bluetooth는 피코넷(Piconets)과 스캐터넷(Scatternets)으로 구분된다. 피코넷은 공동 마스터와 함께 동작하는 슬레이브 집합이다. 피코넷 상의 모든 장치들은 마스터의 주파수 호핑 순번과 시간에 따른다. 한 피코넷 내의 슬레이브 수는 7개로 제한하고, 각 슬레이브는 공동 마스터와 통신을 한다.

의 속도로 255대의 기기들을 연결할 수 있다. 이와같은 구성을 통해 대용량의 데이터 전달이 요구되지 않고, 긴 배터리 수명 보장된다. 또한 일정 거리 이상의 전송 영역의 확보가 필요한 곳에 사용 가능하다. 일반적으로 무선네트워크에서 데이터 송수신부분의 전력 소모량이 가장 크다. 그러나 Zigbee는 통신시 50mW로 전력 소모하는데, 이는 UWB의 200mW, WLAN의 1W에 비해 매우 낮은 소모량이다. (그림 1)은 WPAN과 WLAN에서 데이터 전송률, 전력의 소모량과 그 구현의 복잡도 등을 보여준다[7].



(그림 1) WLAN과 WPAN 표준 기술들의 동작환경

실제적인 센서 네트워크의 구현을 위해서 필요한 것은, 고속의 무선 네트워크 보다 낮은 복잡도의 회로와 저가격, 저 전력의 구성이다. 이를 통해 배터리로 몇 개월에서 수년까지 지속적인 생존이 가능하다.

2.3 센서 네트워크 운영체제

센서 노드는 마이크로 컨트롤러가 내장된 소형 컴퓨터 시스템에 온 보드 된 센서 모듈이다. 또한 센싱 기능과 센서 노드간의 통신을 위한 운영체제로 조합된다. TinyOS는 U.C. Berkeley대학을 중심으로 한 NEST

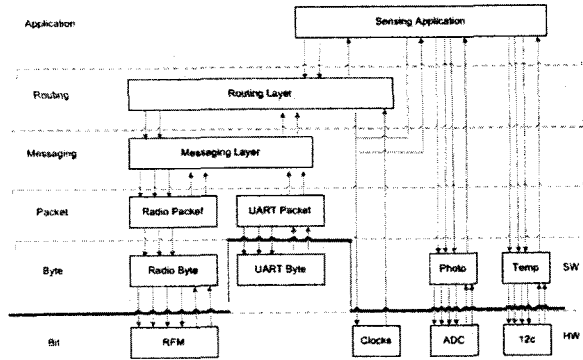
<표 1> 주파수별 특징

주파수	인식거리	적용분야
125-135kHz	< 10cm	Rental Item, Auto Immobilizers, Animal Tracking
13.56MHz	10-70cm	Rental Item, Auto Immobilizers, Security/Access Control, Smart Card
433.92MHz	< 100m	Container Management, e-Seal
860-960MHz	> 1m	Asset Management, Yard Management, Baggage Tracking, Toll Collection
2.45GHz	< 1m	Asset Management, Supply Chain Management, Toll Collection

Zigbee는 저전력, 저비용의 특징인 2.4GHz 기반의 가정용 무선 네트워크 규격으로 반경 30m 내에서 250kbps

(Network Embedded Software Technology) 프로젝트에서 개발한 센서 네트워크 노드 전용의 OS이다.

TinyOS와 같은 센서 노드 OS의 기본적인 요구사항은 다음과 같다. 우선 적은 코드 크기, 효과적인 자원(Resource)관리, 그리고 저 전력 소모, 마지막으로 통신을 위한 Ad Hoc 센서 네트워크 프로토콜이다. TinyOS는 4KByte 미만의 매우 작은 실행 이미지를 처리하는 OS로 주로 NesC 언어로 개발된다.



(그림 2) 컴포넌트 기반의 TinyOS 응용 예

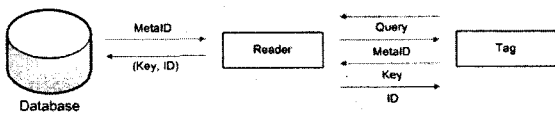
S-MAC은 센서 네트워크의 대표적인 MAC 프로토콜로써 센서 네트워크 응용프로그램에서 특별한 센싱 이벤트가 발생하지 않을 때 휴지(Idle)상태에 들어간다. 또한 낮은 전송속도로 인해 전송할 패킷을 여러 작은 단위로 나누어 전송하는 특징을 가진다.

본 논문에서는 TinyOS를 센서 노드들을 위한 운영체제로 사용한다. TinyOS는 코어 운영체제 외에 센서 네트워크용 소형 데이터베이스인 TinyDB와 태스크 툴킷 등을 제공하고 있다.

2.4 RFID 보안 프로토콜

2.4.1 Hash lock 방식

Hash Lock 방식은 일 방향 해시 함수의 역함수 계산 어려움에 기반하고 있으며 인가받지 않은 Reader가 Tag를 읽는 것을 방지하는데 응용될 수 있다. 이 과정에서의 Spoofing은 방지하지 못하지만 탐지가 가능하다. 이 방식은 해시 함수만을 요구하는 단순한 구조이다. 그래서 저비용으로 구현될 수 있으나, metalD가 고정된 후 별도의 변경을 하지 않아 공격자는 metalD를 이용하여 해당 Tag의 위치를 추적할 수 있다.



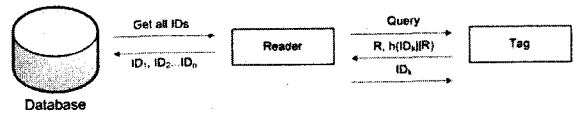
(그림 3) Hash Lock의 Unlocking 프로토콜

(그림 3)은 Reader가 Tag에게 metalD를 질의한 결과를 받아 DataBase에 전송하고 DataBase는 (metalD, Key)

의 일치 여부를 확인한다. 이후 Reader는 Tag에게 Key를 전송하며 Hash(key)와 metalD가 일치하면 잠긴 상태에서 빠져나온다[8].

2.4.2 Randomized hash lock 방식

Randomized hash lock 방식은 Hash lock 방식을 개선하여 고정된 metalD를 갖지 않는다. 난수 생성기를 사용하여 Tag 접근시 다른 값을 갖는다. 그러므로 이론적으로 Tag에 대한 추적이 가능하지 않다. 그러나 해시 함수와 난수가 동시에 생성되는 복잡도로 인해 저비용으로 구현하기 어렵다.

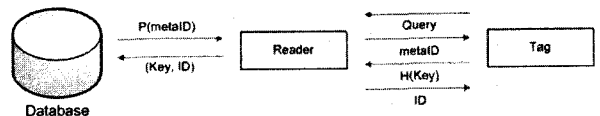


(그림 4) Randomized Hash Lock의 Unlocking 프로토콜

(그림 4)와 같이 Reader는 Tag에게 질의를 보낸다. Tag는 랜덤한 난수를 생성하고, hash(ID || R) 값을 계산한 후 Reader에게 전송한다. Reader는 hash(ID || R) == hash(ID || R)을 만족하는 ID를 찾으면 전송하고 잠긴 상태에서 빠져나온다[8].

2.4.3 Hash Lock과 PKI 방법을 이용한 인증 프로토콜

일방향 해시 함수의 역함수 계산 어려움에 기반을 둔 Hash Lock에 PKI방법을 적용하여 MetalD를 비밀 키로써 사용하는 개선된 형태로 <2.4.1> <2.4.2> 절의 개선된 형태이다[9]. Hash Lock 방식은 인가받지 않은 Reader기가 Tag를 읽는 것을 방지 할 수 있으며 Hash Function만을 요구하므로 저비용으로 구현가능하다. [그림 5]에서의 Reader는 미리 등록된 공개키(meta ID를 이용하여 생성된)로 Tag를 인증하고 metalD로 각 Tag의 유일한 키(k)를 생성하며 이에 해당하는 metalD = H(k)를 가지고 있다. 이 때 H()는 해시함수이다. Tag는 자신의 비밀키를 이용하여 생성된 metalD를 Reader에 보내고 Reader는 해당되는 키(k)를 만들어내 Tag에 보낸다. 이때 Tag는 Reader로부터 보내진 키(k)를 해시값과 자신의 metalD에 비교하여, 그 값이 동일하면 자신의 ID를 전송한다.



(그림 5) 인증 프로토콜

- (1)Reader는 Tag에게 질의를 보낸다
- (2)Tag는 미리 생성된 비밀 키를 이용한 생성된 MetalD

를 보낸다.

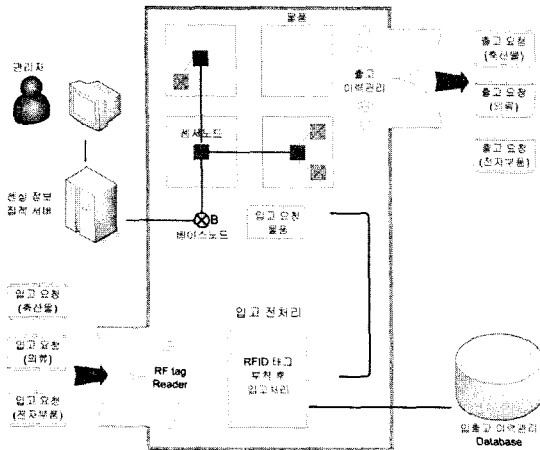
(3) Reader는 P(meta ID) 인증키를 생성한다.

Reader는 Data Base에서 값을 조사하고 일치하면 Key와 ID를 Tag에게 전송한다. metaID는 PKI와 관련하여 사용할 수 있는 장치들에 대하여 단일 접속이 가능하며 다중 요소 인증을 사용하여 지역 환경에서 접속가능하다[9].

### 2.5 물류 시스템 상의 RFID/USN 적용

RFID/USN환경의 실용적인 적용으로 물류 시스템에 대해 많은 시도들이 이루어지고 있다. (그림 6)은 물류를 보관하기 위한 창고 운영 예시로써 유사한 제품군이 창고에 입고되거나 비슷한 특징을 다양한 제품들이 창고에 배치되는 것을 가정한다. 일반적으로 창고에 보관되는 물품들은 다양한 이유로 인해 보관되는 기간에 차이가 있으며 최적의 상태를 유지하기 위한 환경 또한 다르다. 이러한 차이로 인해 제품의 유통기간이나 적절한 출하시기는 물품의 질을 유지하는 변수로써 작용한다.

환경변수로는 창고 내에서 보관되는 위치나 빛, 온도, 습도, 먼지 등을 들 수 있다. 그러므로 물품의 입고시 물품의 종류와 보관되는 장소에 따른 최적의 환경을 설정하고, 보관 이력을 관리하여 물품의 이상 징후 발생시 관리자가 알 수 있도록 경고와 로그정보가 생성되어야 한다[10].



(그림 6) RFID/USN 적용하의 창고관리 운용

### 3. 능동형 창고 상태 관리 시스템

대형 설비 등의 장비이력을 관리하기 위한 기존의 유선 설비에서 고가의 기민한 장비에 센서를 부착한 형태는 오래전부터 구축되어 왔다. 능동형 창고 상태 관리 시스템은 특수 장비에서 일반 재고나 물품으로 대상을 전환하고 유선의 전력을 공급 받는 센서에서 무선통신을 수행하는 저 전력 센서로 대상이 대체된다. 그래서 특수 환경의 작업지 보다는 일반적인 물류창고를 대상으로 고

려된다. 이러한 물류 창고 파렛트에 RFID 태그 외에 추가적으로 저 전력(Low Power)을 기반으로 하는 근거리 무선 네트워크 통신 장치인 센서노드를 부착한다. 센서노드는 배터리로 작동되며, 보관되어지는 물품의 상태를 파악할 수 있도록 다양한 센싱 기능(온도, 습도, 조도, 압력 등)을 가지고 있다[10].

#### 3.1 상세 시스템 구성 요소

본 절에서는 기존 시스템에서의 구성을[10] 세분화하여 3가지로 구분한다. 우선 정보수집의 목표가 되는 고정 위치의 다수 물품이 첫 번째 요소이다. 파렛트에 적재된 제품에 따라 물품이나 선반의 센서 노드를 배치하고 최적 환경을 원격으로 설정한다. 센서 노드는 각각의 센서들(온도, 습도, 조도)에 설정된 임계값을 벗어나는 경우 서버에 변경 사실을 알리게 된다. 두 번째로 물품의 정보가 집적되는 정보 집적 서버이다. 서버에서는 센서노드들이 보낸 데이터가 저장될 최종 목적지로써 다양한 마이닝 기법들에 의해 최종 사용자에게 자료의 분석된 결과를 보여주게 된다. 마지막 요소는 이동 단말 장치이다. 현장 관리자는 이동형 장비를 들고 센서의 데이터를 수집하거나 센서 데이터 생성시점을 지정하는 스위치 역할을 수행한다. 여기에서 이동형 장비는 파렛트단위로 창고 사이를 이동하는 물품이거나, 카트를 밀고 있는 소비자로서 변경해 볼 수 있으며, 본 논문에서는 PDA 단말기를 이용하여 재고 관리를 한다.

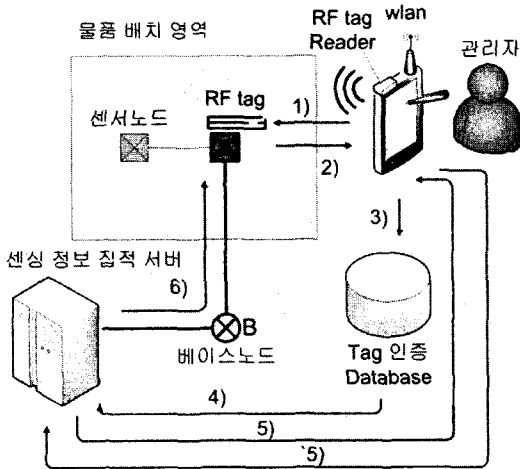
#### 3.2 이동형 단말장치 기능

기존 시스템에서는 물품과 서버군의 두 가지 요소를 기준으로 입고 프로세스 설계가 이루어졌다[10]. 본 논문에서는 추가적으로 이동형 단말장치를 마지막 세 번째 요소로 추가하였다. 이 세 번째 요소와 센서노드간의 보안 응용이 주된 내용으로 이동형 단말의 기능과 역할을 별도로 고려해야 하는 이유는 다음과 같다.

첫째, 센서에 의해 수집되는 정보가 자동화 처리가 가능하지 않거나 경보(alarm)에 의해 관리자가 원격지의 센서를 직접 조작해야 하는 경우이다. 다음으로 배터리에 의해 저 전력으로 운용되어야 하는 센서 노드의 경우 실시간 정보를 무작위로 생성하는 경우이다. 이 때 라우팅 경로상의 특정 센서노드가 집중적으로 사용될 수 있으며, 해당 노드의 생명주기가 극도로 낮아지게 되어 결과적으로 전체 센서 망을 단절시킬 위험이 있다. 이러한 위험을 피하기 위해 과부하가 예상되는 센서노드를 유선 전원 형태로 변환하거나 전체 센서망의 구성형태를 단순화시켜 특정 노드의 통신 집중 현상을 예방하는 방법이 있다. 그러나 보다 근본적인 해결책은 초기 설계부터 지속적으로 생산해야 할 센싱 데이터의 양을 최소화 하고 통신주기를 길게 정하는 방법이다. 다른 방법으로는 필요시에만 특정시점에서 센서의 동작을 수행하게 하는 것이다. 이와 같은 해결책들은 센서노드의 생존성이 실제 전력을 사용하는 통신행위에 있음을 고려한 것이다. 그러므로 센서가 배치된 곳이 전문 기술자의 관리가 필요한 경우 이동형 장비를 들고 이동하는 기술자/관리자에게 어떠한 형태로 정보를 제공하여 휴지(idle) 상태의 센서노드를 동작시킬지 고려되어야 한다.

3.3 RFID tag(RF tag)와 이동 단말간의 보안 운용

이동 단말기를 가진 관리자는 센서노드의 동작에 앞서 해당 센서노드의 키 역할을 수행하는 RFID tag와 통신을 수행하여 인증코드를 획득하여야 한다. (그림 7) 이를 위한 인증 과정을 보여 주고 있다.



(그림 7) RF tag 를 이용한 센서노드의 동작제어

이 과정에는 몇 가지 가정을 전제로 한다. 첫째, 해당지역의 키 tag 로부터 인증코드를 획득 가능한 이동 단말 장치는 센서노드의 동작 수행에 대한 사용권한이 사전에 등록되어야 한다. 둘째, 해당 키 tag 는 지역의 키 역할을 수행하기 위해 사전에 인증코드를 발급받아야 한다. 셋째, 키 태그와 인증코드 그리고 센서의 동작 명령이 사전에 등록되어야 한다. 이와 같은 가정을 기반으로 (그림 7) 의 1) 2) 과정 이후의 단계는 [9]의 제안된 결과를 본 논문에 맞게 추가 응용하였다.

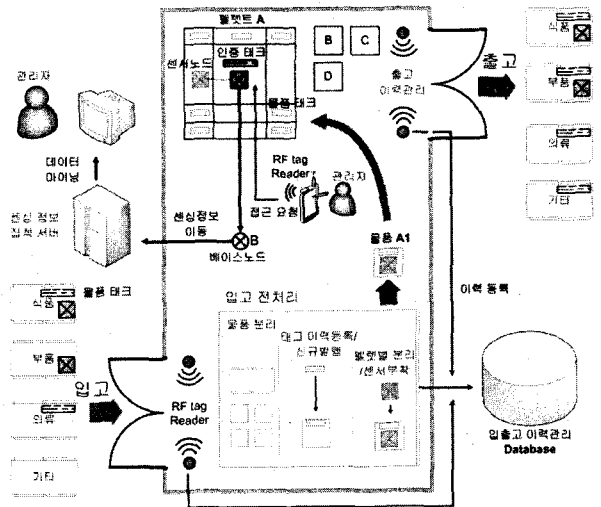
- 1) Reader 는 Tag 에 질의를 보낸다.
- 2) Tag 는 미리 생성된 비밀 키를 이용해 생성된 metalD를 보낸다.
- 3) Reader 는 P(Meta ID) 인증키를 생성하고 보안채널을 통해 서버의 DataBase에 전송한다.
- 4) DataBase에서의 조사된 값이 일치하면 해당 코드에 등록된 명령어 셋을 리더에 보내고
- 5) 리더는 수신된 명령어셋으로부터 원하는 센서노드의 동작을 선택하고 이를 서버에 전달한다.
- 6) 서버에서는 수신된 명령을 센서노드에 전달한다. 위의 과정에서 이동형 단말기에 센서모듈이 부착된 경우에는 6)의 과정을 이동형 단말이 대행하여 수행한다.

제안된 방법에서 1) 2) 의 과정은 metalD를 이용하여 공격할 수 있는 방법에 대하여 안전하고 인가 받지 않은 사용자의 접근을 방지하고 합법적인 reader 기의 의해서만 식별 가능함을 말한다. 3) 4) 5) 는 획득한 인증코드

를 서버에 전송하여 코드에 부과된 센서노드 사용 권한을 얻어 센서에 동작을 명령하는 과정을 나타내고 있다. 이처럼 이동형 단말장치를 통해 해당 센서에 직접명령을 내리지 않고 고정서버로부터 우회적인 명령을 내리는 이유는 다음과 같다. 이동형 단말이 가지는 일반 PC 와의 성능상의 차이가 첫째 이유이고, 둘째 인가받지 않은 명령을 이동형장비로 최대한 노출 시키지 않고자 함이다.

3.4 보안이 고려된 입출고 흐름도

물품이 외부에서 입고되거나 창고 내에서 물품이 분할되는 경우와 같이 물품의 이력이 변동되면 해당 물품의 이력변동을 DB에 저장하게 된다. 외부에서 들어오는 경우 창고 입구에 설치된 RFID 리더기를 통해 자동으로 정보가 보관되며, 창고내 작업자에 의해 내부에서 이동되거나 분할될 경우 지정된 등록 장비를 통해 관련된 이력을 생성하는 과정을 거친다. 이후 물품이 배치된 후에는 특정 시점마다 센서노드에 의해 온도나 습도와 같은 환경정보가 수집되어 정보 집적 서버로 전송된다. 지정된 환경 값을 벗어나는 경우 서버에서 경고 메시지가 현장 관리자에 전달되는 형태로 물품의 이상 징후를 사전에 파악하고 대처하게 된다. 인가받은 현장 관리자는 이동 단말기를 통해 해당 센서노드의 동작 설정을 변경하여 변경된 물품에 대해 대처한다. 물품 중 창고 내의 온도와 적재 후 경과된 시간과 같은 환경정보에 매우 민감한 경우, 출고되거나 장소가 변경되어야 한다. 대개의 경우 환경정보의 변동은 물품의 질과 직결되는 결과로 이어진다. 이후 빈 파렛트의 센서 노드는 분리하거나 새로운 센서를 부착하여 재설정하는 형태로 재활용 된다. (그림 8) 은 이러한 과정에 대한 전체적인 흐름을 나타내고 있다.



(그림 8) 보안이 고려된 입출고 흐름도

#### 4. 결론

RFID/USN 은 유비쿼터스 사회의 중요한 기반 인프라로서 다양한 연구를 통한 실용적인 접목이 시도 되고 있다. 특히 물류의 입출 재고와 상태 관리를 위해 물품 보관 단위인 파렛트에 RFID 태그를 부착하여 물품을 식별하고 센서 모듈에 의해 물품의 환경 상태 정보를 파악한다. 본 논문은 RFID/ USN 기반의 창고 상태 관리 시스템에서 상태정보 습득 과정의 보안적용을 위한 시스템을 구성을 주된 목적으로 한다. 이 과정에서 이동형 단말장치의 기능에 대해서 제안하였고 또한 창고 내에 배치된 RF tag 와 센서 노드 그리고 이동형 단말장치와의 보안이 고려된 적용 관계 또한 정의하였다.

기존의 연구들과의 차별성은 자동화 가능한 범위에서의 수동제어에 주목한다는 점이다. 실제, 가장 가치 있고 중요한 부분은 자동화된 처리보다 현장 관리자의 의한 판단으로 이루어진다. 그러므로 의사판단의 주체인 현장 관리자에 적절한 제어 정보를 제공하기 위한 센서의 동작 기능과, 센서 노드의 동작을 제어하기 위한 RF tag 보안 접근, 마지막으로 센서 노드 자체의 생존성 사이의 절충점을 찾기 위한 시도로서 본 논문을 설계 제안하였다. 향후 설계된 시스템에 대한 구현을 통한 구체적인 성능평가 실험이 필요하다.

#### 5. 관련연구

- [1] 장병준, "RFID/USN 기술개발 동향," 한국정보과학회지, 23권, 2호, 2005.
- [2] 최재귀, 박지환, "효율적인 식별 기능을 가진 위조 불가 RFID Tag 가변 ID 방식," 한국정보처리학회 논문지 11권, 4호, pp. 447~454, 2004.
- [3] 장병준, 안선일, 이운덕, "RFID/USN 기술개발 동향," 한국정보과학회 학회지, 23권, 2호, pp.83~87, 2005.
- [4] "RFID Technical Education Seminar", RRC, University of Incheon, 2005.
- [5] S.H. Lee, W.D. Cho, B.C. Song, J.H. Kang, D.H. Kim, T.C. Chung, "IEEE 802.15.4: Sensor Network Technology," Journal of Electrical and Information Science, Vol.21, No.8, pp.93~102, 2003.
- [6] Zigbee Web Site: <http://www.zigbee.com>
- [7] J.A Gutierrez et al., "IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Network," IEEE Network, Vol. 15, No.5, pp.12~19, 2001.
- [8] 홍도원, 장구영, 박태준, 정교일, "유비쿼터스 환경을 위한 암호 기술 동향," 전자통신동향분석, 20권, 1호 pp.65~68, 2005.
- [9] Choi Yong Sik, Shin Seung Ho, "The Authentication Protocol using the Hash Lock and PKI IN Ubiquitous environment", ITC-CSCC, Vol.2 pp669~670, 2005
- [10] Lee Min Soon, Lee Ji Sun, Lee Byoung Soo, "Improved Active Warehouse State Control System based RFID/USN," APIS 5th, pp.235~39, 2006.