유비쿼터스 환경에능동형 창고 상태관리를 위한 보안 프로토콜 설계

-A Design of Security Protocol for Active Warehouse Condition Management System based on Ubiquitous Environment-

전 영 준 *
John Young Jun
최 용 식 *
Choi Yong Sik
신 승 호 *
Shin Seung Ho
박 상 민 **
Park Sang Min

Abstract

RFID/USN is important infrastructure of the ubiquitous society. And so, It is various and practical research is attempted. These two base technology have physical characteristic and complement relationship. Like this relationship is applied Following example that is system research which manages warehouse stocks and conditions. First, We adhere RFID Tag at the Pallet of the warehouse and do identification goods. And then, It grasps the environment state information of stocks with sensor module which has Zigbee wireless communication function. From like this process RFID Tag information and jop-control command of sensor node also it is exposed to air.

* 인천대학교 컴퓨터공학과
** 인천대학교 산업경영공학과 교수
2006년 11월접수; 2006년 12월 수정본 접수; 2006년 12월 게재확정

Therefore, We control sensor node in USN/RFID environment through the mobile device. And system design for the security Apply of the process is main purpose of this paper's. We propose the condition and function of the mobile device to the secondary. And We define the relation of the sensor node with RFID to be arranged to a warehouse. Finally, This paper is designed to find a trade-off of the following viewpoints. First, We offer suitable sensor-control information to a actual manager. Second, We offer RFID tag security approach to control the action of the sensor. Third, It increases the survivability of sensor node form.
Keywords : RFID, USN, Security Protocol

1. 서 론

유비쿼터스 센서 네트워크는 광범위하게 설치되어 있는 유무선 네트워크 인프라에서 상황 인식을 위해 다양한 센서들을 장착한 형태를 말한다. 관련된 용어로 WSN(Wireless Sensor Network, WSN) 는 국내에서 USN(Ubiquitous Sensor Network) 이라는 용어로 많이 사용되고 있다. 센싱된 정보를 이용하여 응용서비스를 제공하는 예로 지능형 물류관리 시스템과 시큐리티, 침입 탐지, 군사, 방재 시스템 등을 들 수 있다. 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[1].

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 기억공간과 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[2].

USN/RFID 기술이 응용의 예로 물류 집하장이나 수출입 항의 경우 창고에 보관된 다양한 제품 상태 관리를 들 수 있다. 보관되는 제품들에 따라 온도, 습도, 압력, 빛 등의 상태정보가 제품의 품질을 좌우하는 경우가 있으며 이에 따라 제품의 출고시기와 유통기간이 변경되기도 한다[3]. 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 유지가 가능하다. 이에 유형의 시스템 구성을 세분화 하면 다음과 같다. 센싱 대상이 되는 특정 환경이나 물품 등의 객체, 그리고 센싱 정보가 최종적으로 수집되고 기록되는 서버, 마지막으로 센서와 물품관리를 위해 현장 관리자가 사용하는 이동형 단말장치이다. 이러한 시스템 구성은 기본적으로 다음과 같이 나눌 수 있다. 우선 특정 주기마다 자동적으로 물품의 상태정보를 수집하는 단계가 첫 번째이다. 다음으로

이동형 장비를 통해 물품을 배치하거나 특정 센서의 정보를 취득하기 위해 수동적으로 명령을 내리는 과정이다. 개선된 수동관리 체계에서 현장 관리자는 보안코드를 습득하고 인증코드를 받아 지정된 센서가 원하는 동작을 수행하도록 명령한다. 본 논문은 유비쿼터스 환경에서 RFID/USN 기술을 사용하고, 창고의 상태정보를 관리하는 시스템을 구성 한다. 또한 상태정보 습득 과정의 보안 프로토콜을 구성한다. 보안 프로토콜은 다음의 운용단계로 구분된다. 첫째 입고시 전처리 과정, 둘째 상태정보 습득 단계, 셋째 출고시 후처리 과정이다. 논문의 구성은 2장에서 RFID/USN 기반 기술들과 능동형 창고관리 시스템에 대해 개략적으로 설명하고 보안 취약점에 대해 설명 한다. 그리고 나서 적용될 수 있는 보안프로토콜에 대해 설명한다. 3장에서는 보안프로토콜이 적용된 능동형 창고 상태 관리 시스템을 설계한다. 그리고 시스템 구성을 3가지 요소로 나누어 설명한다. 마지막으로 보안이 적용된 능동형 창고 상태 관리의 전체 프로세스를 입고/출고 및 상태 정보 수집 단계로 나누어 설명한다. 4장에서는 결론 및 향후 연구 방향을 제시하는 것으로 정리한다.

2. 관련 연구

2.1 RFID 기반 기술

2003년 10월 설립된 EPCGlobal은 Savant(미들웨어), 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, 칩에있는메모리를 통해 태그 식별을 위한 EPC 코드가 저장된다. (그림 1)은 RFID 시스템의 일반적인 구성을 나타낸다. RFID 시스템은 전자기파 무선 시스템으로 분류되며, 다른 무선 서비스들의 충돌을 피하기 위해서 적절한 동작 주파수가 필요하게 된다[2]. 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[2]. EPC 코드는 기존의 바코드 관리기관에서 제안한 RFID용 코드체계이며, 64비트, 96비트, 256비트의 상품번호 체계를 기반으로 한다. Savant는 PML 쿼리에 대하여 다양한 서비스를 제공하기 위해 미들웨어의 기능을 수행한다. PML은 XML을 기반으로 EPCs와 관련된 Report 기능과 구조화된 쿼리 지원을 목표로 한다.

<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

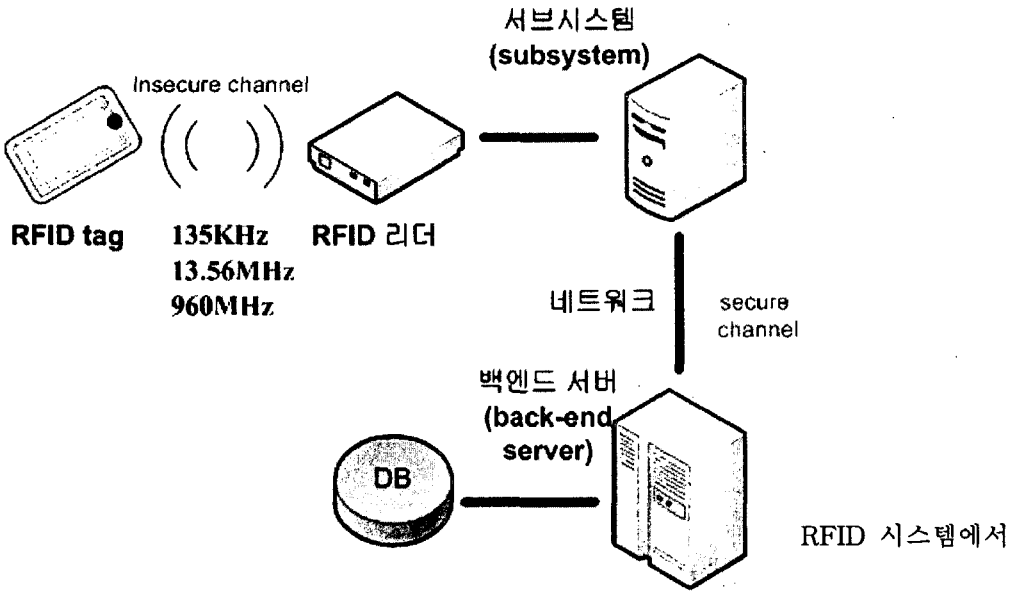
2.2 USN 기반 기술

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[4]. 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 슬에이브는 공동 마스터와 통신을 한다. Zigbee는 저전력, 저비용의 특징인 2.4GHz 기반의 가정용 무선 네트워크 규격으로 반경 30m 안에서 250kbps의 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 2) 은 WPAN과 WLAN에서 데이터 전송률, 전력의 소모량과 그 구현의 복잡도 등을 보여준다[5][6].

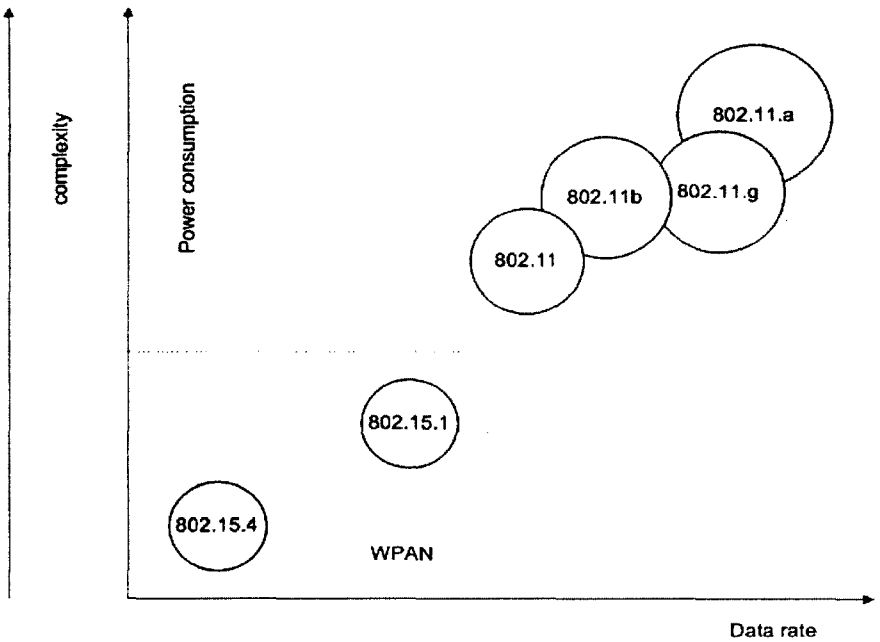
실제적인 센서 네트워크의 구현을 위해서 필요한 것은, 고속의 무선 네트워크 보다 낮은 복잡도의 회로와 저가격, 저 전력의 구성이다. 이를 통해 배터리로 몇 개월에서 수년까지 지속적인 생존이 가능하다.

2.3 RFID 프라이버시 보호 요소

다음과 같은 특성을 갖는다. 첫째 정보를 담고 있는 RF tag 와의 access 과정이 비접촉식이어서 외부 오염에 강하다. 둘째 RF tag 리더는 다수의 태그를 동시에 수신 가능하다. 셋째 RF tag 에 다양한 형태로 데이터를 기록 가능하다. 이러한 특성은 공중(air)을 매체로 이루어지는 관계로 다음과 같은 프라이버시 문제가 발생한다[7][8].



<그림 1> RFID 시스템의 일반적인 구성



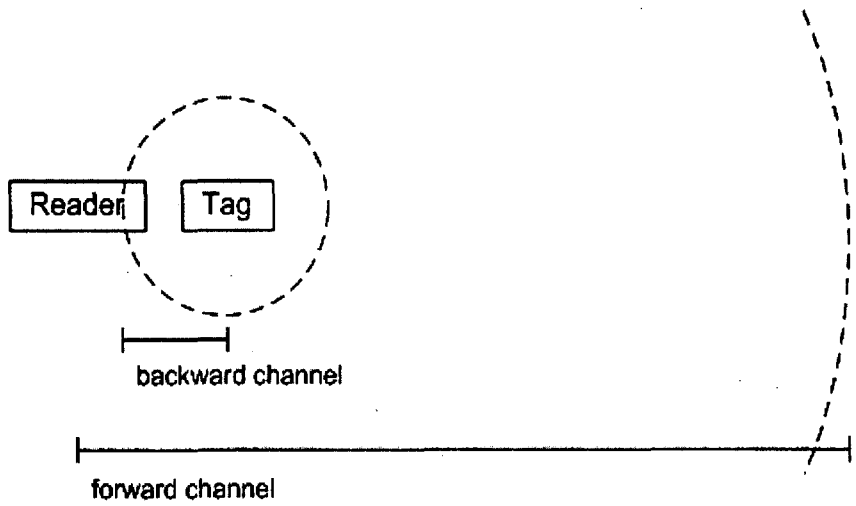
<그림 2> WLAN과 WPAN 표준 기술들의 동작환경

2.3.1 기밀성 (confidentiality)

<그림 3>은 데이터의 전송이 air interface 형태로 이루어져 식별 정보가 그대로 노출된다. 그러므로 통신내용에 대한 기밀이 유지되어야 한다. 또한 취득 정보를 해석할 수 없어야 한다. Forward Range은 리더가 태그에게 질의를 보낼 수 있는 물리적 범위이다. 그리고 Backward Range는 태그가 리더에게 질의에 대한 응답을 보낼 수 있는 물리적 범위 이다. 도청자가 Forward Range안에 있을 때 이진 탐색 기법을 사용하는 RFID 시스템의 리더는 태그에서 태그의 정보를 계속 전송하게 되고 도청자는 이를 성공적으로 도청 가능하다.

2.3.2 불구분성 (indistinguishability)

습득된 태그의 송신 정보(출력값)가 동일하거나 예측 가능해서는 안 된다. 특정 태그 정보가 동일할 때 태그 리더를 통해 태그의 위치를 역추적 가능하다. 그러므로 태그 접근시 출력 값을 매회 변동시키는 방법처럼 미래의 출력값이 예측 불가능해야만 한다.



<그림 3> RFID 와 tag 간의 정보 누출

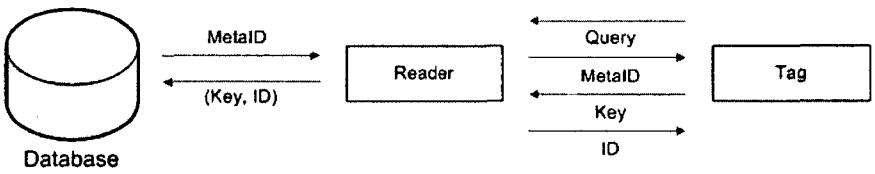
2.3.3 전방 보안성 (forward security)

태그는 저가의 하드웨어이기 때문에 물리적인 공격 가능성을 배제할 수 없다. 그러므로 태그에 대한 물리적 공격 시 내부의 정보가 노출되더라도 과거의 출력 값을 계산해 낼 수 없어야 한다.

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, metaID가 고정된 후 별도의 변경을 하지 않아 공격자는 metaID를 이용하여 해당 Tag의 위치를 추적할 수 있다.

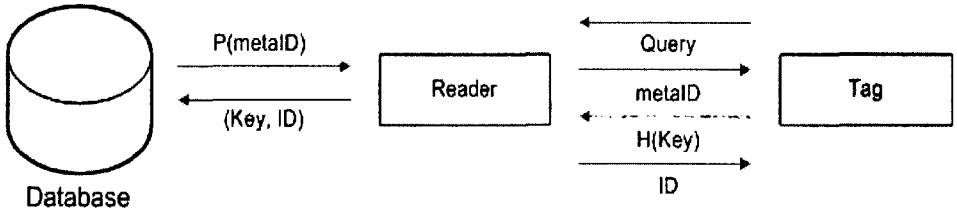


<그림 4> Hash Lock의 Unlocking 프로토콜

<그림 4> Reader가 Tag에게 metaID를 질의한 결과를 받아 DataBase에 전송하고 DataBase는 (metaID, Key)의 일치 여부를 확인한다. 이후 Reader는 Tag에게 Key를 전송하며 Hash(key)와 metaID가 일치하면 잠긴 상태에서 빠져나온다[7][9].

2.4.2 Hash Lock과 PKI 방법을 이용한 인증 프로토콜

일방향 해시 함수의 역함수 계산 어려움에 기반을 둔 Hash Lock에 PKI방법을 적용하여 MetaID를 비밀 키로써 사용하는 개선된 형태로 <2.4.1> 절의 개선된 형태이다[11]. 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 metaID로 각 Tag의 유일한 키(k)를 생성하며 이에 해당하는 metaID = H(k)를 가지고 있다. 이 때 H( )는 해시함수이다.



<그림 5> Hash Lock과 PKI 방법을 이용한 프로토콜

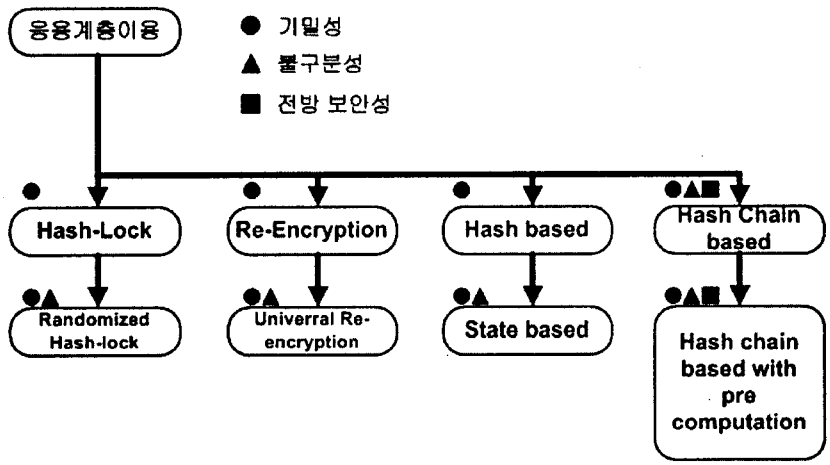
Tag는 자신의 비밀 키를 이용하여 생성된 metaID를 Reader에 보내고 Reader는 해당되는 키(k)를 만들어내 Tag에 보낸다. 이때 Tag는 Reader로부터 보내진 키(k)를 해시 값과 자신의 metaID에 비교하여, 그 값이 동일하면 자신의 ID를 전송한다. <그림 5>는 다음의 단계를 거쳐 Tag 를 인증한다.

(1) Reader는 Tag에게 질의를 보낸다
(2) Tag는 미리 생성된 비밀 키를 이용한 생성된 MetaID를 보낸다.
(3) Reader는 P(meta ID) 인증키를 생성한다.

Reader는 Data Base에서 값을 조사하고 일치하면 Key와 ID를 Tag에게 전송 한다. metaID는 PKI와 관련하여 사용할 수 있는 장치들에 대하여 단일 접속이 가능하며 다중 요소 인증을 사용하여 지역 환경에서 접속가능 하다[11].

2.5 RFID Security Schemes

<2.3> 절의 RFID 프라이버시 요건에 맞추어 RFID 보안프로토콜의 관계를 대략적으로 도식한 것으로 hash chain에 기반을 둔 형태는 안전도 면에서 가장 높다. 그러나 비용과 속도 측면에서는 hash-lock 에 기반을 둔 응용형태가 본 논문에서의 주요한 고려 대상이다[7][10]. 이에 대한 근거는 <3.1> 절 이후에 밝힌다.



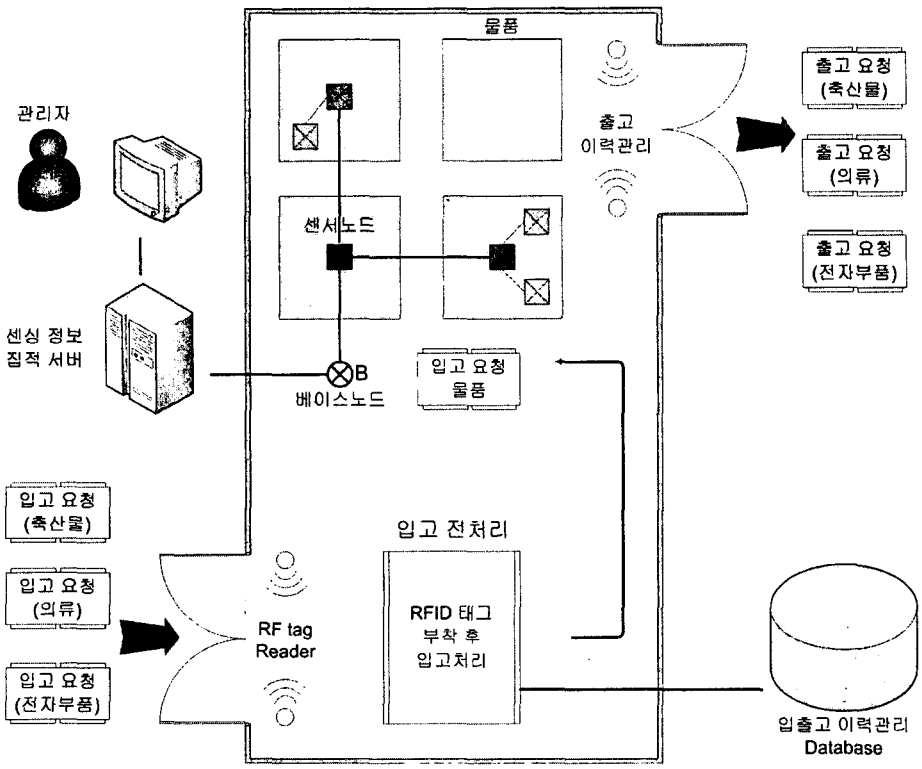
<그림 6> RFID Security Schemes

2.6 능동형 창고 관리 시스템

RFID/USN환경의 실용적인 적용으로 물류 시스템에 대해 많은 시도들이 이루어지고 있다. <그림 7>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 발생 시 관리자가 알 수 있도록 경고와 로그정보가 생성되어야 한다[12].

능동형 창고관리 시스템의 원형 모델은 특수 대형 설비 등의, 고가이면서 민감한 장비들을 관리하는 유선 센서 시스템이다. 이러한 고가의 기민한 장비에 센서를 부착한 형태는 필요에 의해 한정적으로 구축되어 왔다. 그러나 지능화된 창고 상태 관리 시스템의 대상은 특수 장비에서 일반 재고나 물품으로 대상을 전환하고 유선의 전력을 공급 받는 센서에서 무선통신을 수행하는 저 전력 센서로 대상이 대체된다. 그래서 특수 환경의 작업지보다는 일반적인 물류창고를 대상으로 고려된다. 이러한 물류 창고 파렛트에 RFID 태그 외에 추가적으로 저 전력(Low Power)을 기반으로 하는 근거리 무선 네트워크 통신 장치인 센서노드를 부착한다. 센서 노드는 배터리로 작동되며, 보관되어지는 물품의 상태를 파악할 수 있도록 다양한 센싱 기능(온도, 습도, 조도, 압력 등) 을 가지고 있다[12].



<그림 7> RFID/USN 적용하의 창고관리 운용

3. 능동형 창고관리를 위한 보안 시스템 설계

3.1 상세 시스템 구성 요소

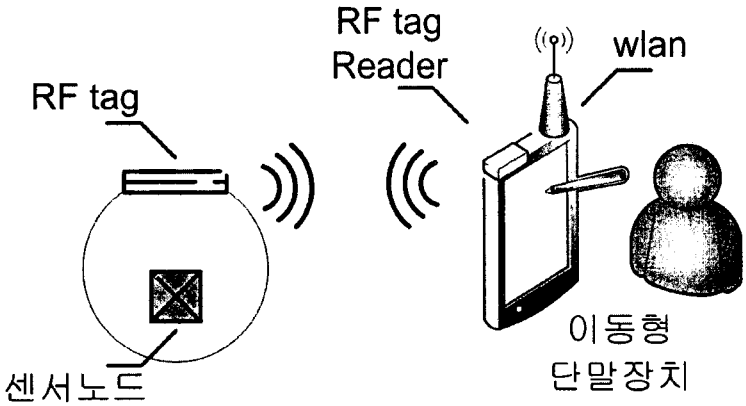
본 절에서는 기존 시스템에서의 구성을[12] 세분화하여 3가지로 구분한다. 우선 정보 수집의 목표가 되는 고정 위치의 환경정보/물품 등의 객체가 첫 번째 요소이다. 시나리오 에서는 파렛트에 적재된 제품에 따라 물품이나 선반의 센서 노드를 배치하고 최적 환경을 원격으로 설정한다. 센서 노드는 각각의 센서들 (온도, 습도, 조도)에 설정된 임계값을 벗어나는 경우 서버에 변경 사실을 알리게 된다. 두 번째로 물품의 정보가 집적되는 정보 집적 서버이다. 서버에서는 센서 노드들이 보낸 데이터가 저장될 최종 목적지로써 다양한 마이닝 기법들에 의해 최종 사용자에 자료의 분석된 결과를 보여주게 된다. 마지막 요소는 본 논문의 주요한 관심인 이동 단말 장치이다. 현장 관리자는 이동형 장비를 들고 센서의 데이터를 수집하거나 센서 데이터 생성시점을 지정하는 스위치 역활을 수행한다. 여기에서 이동형 장비는 파렛트 단위로 창고 사이를 이동하는 물품이거나, 카트를 밀고 있는 소비자로 변경 해 볼 수 있으며, 본 논문에서는 PDA 단말기를 이용하여 특정 지점에 배치된 센서의 동작이나 설정을 변경하는 것으로 가정한다.

3.2 이동형 단말장치 기능

자동화된 센서정보수집 시스템에서는 센서와 정보집적서버의 두 가지 요소를 기준으로 프로세스 설계가 이루어졌다[12]. 본 논문에서는 추가적으로 이동형 단말장치를 마지막 세 번째 요소로 추가 하였다. 이 세 번째 요소와 센서노드간의 보안 응용이 본 논문의 주된 내용으로 이동형 단말의 기능과 역할이 별도로 고려해야 하는 이유는 다음과 같다.

첫째, 센서에 의해 수집되는 정보의 유형이 자동화 처리가 가능하지 않은 예외적인 형태이거나 경보(alarm)에 의해 관리자가 원격지의 센서를 직접 조작해야 하는 경우이다. 둘째 배터리에 의해 저 전력으로 운용되어야 하는 센서 노드가 실시간 정보를 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 단순화 시켜 특정 노드의 통신 집중 현상을 예방하는 방법이 있다. 그러나 보다 근본적인 해결책은 초기 설계부터 지속적으로 생산해야할 센싱 데이터의 양을 최소화 하고 통신주기를 길게 정하는 방법이다. 다른 방법으로는 필요시에만 특정시점에서 센서의 동작을 수행하게 하는 것이다. 바로 이동형 단말장치를 통해 수동으로 명령을 받아 센싱 데이터를 생성하는 것이다. 이와 같은 방법들은 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. 이와 같은 이동형 단말장치를 통한 센서 동작의 제어는 공중을 통해 간접적으로 이루어진다. 그러므로 센서의 동작제어 명령에 대한 보안이 필요하다.



<그림 8> 이동형 단말장치 와 센서/RF tag 연계 컨셉

<그림 8> 은 이동형 단말장치 통해 센서노드를 동작시키기 위한 기본적인 컨셉이다. 우선 RFID 시스템에서 RF tag 와 zigbee 센서모듈 관계는 자물통에 잠겨있는 스위치의 관계로 가정해 볼 수 있다. 일반적인 상황에서 스위치를 누르기 위해서는 지정된 열쇠로 자물통을 열어야 한다. 물론 자물통은 누구든지 접근할 수 있다. 이러한 경우 열쇠에 대한 보안은 결국 스위치에 대한 보안을 대변한다. (그림 8)의 세부적인 구성과 목적은 다음과 같다.

3.2.1 이동형 단말장치

이동형 단말장치 자체의 구성은 RF tag로부터 정보를 수신할 수 있는 1.RF tag reader 모듈과 수신된 태그 정보를 분석할 정도의 2.cpu 파워, 마지막으로 분석된 결과를 서버군 으로 전송할 3.wireless lan 모듈로 구성된다. 본 논문의 설계에서는 별도로 tag 에 데이터를 기록하는 과정이 없으므로 단순히 태그로부터 데이터를 수신할 수 있는 정도면 충분하다.

3.2.2 RF tag

특정지역의 센서노드에 대한 동작 권한을 나타낼 수 있는 RF tag 이다. 이동형 단말장치의 태그 리더는 해당 태그를 읽어 암호화된 내용을 획득한다. 이 과정에서 암호와를 위해 추가적인 tag 설계는 가정하지 않는다. 범용의 tag로도 운용 가능하나 별도의 전파 차폐된 공간에서 write 되는 정도면 충분하다.

3.2.3 센서노드

최종적으로, 이동형 단말장치가 제어하고자 하는 대상이다. 센서 동작제어의 대상은 센싱 수집주기 변경, 라우팅 테이블 구성을 위한 탐색 출력, 통신 주기. sleep/wakeup 운용모드 등 센서의 생존성과 직결될 수 있는 요소들이다.

센서노드의 실제적인 동작 제어는 이동형 단말장치가 해당 지역의 자물통 역할을 수행하는 RF tag 의 정보를 분석해 상위 서버에 전달하는 것으로 시작한다. 센서노드는 이러한 정보를 토대로 센서 제어 서버가 해당 센서에 동작제어 명령을 전달하는 간접적인 방식으로 제어된다.

3.3 RFID tag(RF tag)와 이동형 단말장치를 보안 운용

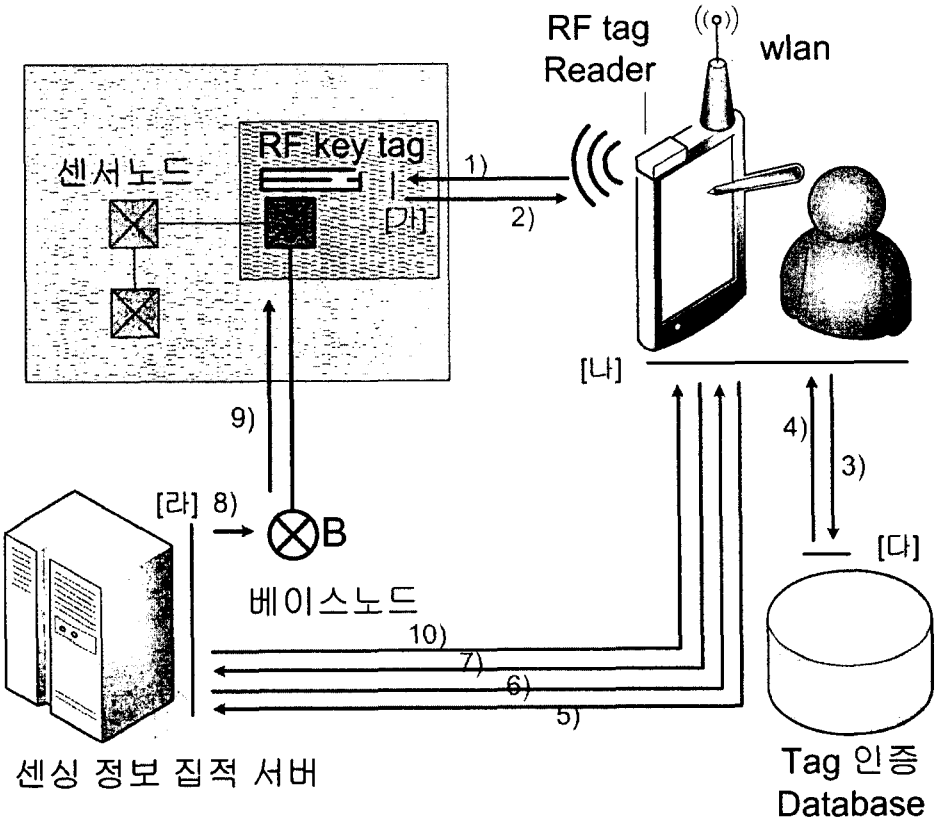
이동 단말기를 가진 관리자는 센서노드의 동작제어 에 앞서 해당 센서노드의 키 역할을 수행하는 RFID tag와 통신을 수행하여 인증코드를 획득하여야 한다. <그림 9> 이를 위한 인증 과정을 보여 주고 있다.

이 과정은 몇 가지 가정을 전재로 한다. 첫째, 해당지역의 키 tag 로부터 인증코드를 획득 가능한 이동 단말장치는 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 9)의 [가] [나] [다]의 단계는 [11]의 제안된 결과 기반으로 본 논문에서 추가 개량하였다. <2.4>절의 RFID 보안프로토콜을 기준으로 볼 때, [가] 는 RF tag 이고, [나] 는 RF 리더이며 [다]는 DB에 해당한다. [라] 는 센서정보가 집적되는 서버이며 대게 Base node 와 유선으로 연결되어 있다. 베이스 노드는 zigbee 통신을 수행하여 센서가 수집된 정보를 상위 서버로 전달하기 위한 노드이다. 통신 유형은 [가] 와 [나] 그리고 [나] 와 [다] 는 무선으로 통신하며 [다]와 [라] 그리고 [라] 와 base node 는 유선으로 연결되어 있다. <그림 9>의 보안운영 절차는 다음과 같다.

(1) RF reader를 통해 태그에 질의한다.
(2) RF tag 는 배치 전에 특정 지역에서 비밀 키를 이용해 write된 metaID를 보낸다.
(1),(2)의 과정은 별도의 암호와 과정이 없이 이루어진다.
(3) 이동형 단말장치는 다음의 과정을 수행하여 wlan 을 통해 DB에 발송한다.

P(Kdb{H(metaID)||Kmd1})
Kdb 는 DB 공개키, Kmd1 는 이동장비의 공개키



<그림 9> RF tag 를 이용한 센서노드의 동작제어

여기서 P(k{}) 는 PKI 방식을 말하여 공개키 K로 암호화한다. H( ) 는 hash 함수를 말한다. 불특정 무선 장비에 대해 암호와 서비스를 제공하기 위해 PKI 를 사용한 것이다. 만일 인가받지 않은 장비가 1) 2) 과정상에서 노출된 metaID를 획득한다고 해도 DB 에 H(metaID) 에 해당하는 값이 등록되어 있지 못하면 센서장비에 대한 인증 권한을 얻을 수 없다. 이를 위해 사전에 H(metaID)들에 대한 권한들이 DB 와 해당 이동형 단말장치 양측에 등록되어 있어야 한다.

(4) DB H(metaID) 에 해당하는 인증코드를 wlan 을 통해 단말장치에 다음의 과정을 수행한다.

P(Kmd1{H(DBid)||Ksv})
ksv 는 서버측 대칭키, DBid 는 DB 측의 임시 id

(4) 단계 이후는 서버 측과 대칭키 기반의 암호화 서비스로 직접 통신한다. DB에서 다른 암호화 서비스를 제공 받는 이유는 tag 에 대한 사용권한이 확실한 대상인 경우

불특정 다수에 대한 보안 접근이라기보다 특정 권한이 사전에 정의된 대상임으로 대상의 권한에 맞게 암호화 강도와 키 길이에 차등화를 주기 위해서 이다.

(5) 이동형 단말장비는 DB 로부터 건네받은 서버의 키로 대칭키 기반의 암호화를 수행하여 D(K{}) 노 나타내고, DB의 id 를 인자로 hash 함수 값과 서버에 대한 질의코드를 보낸다. 해당 이동장비의 인증코드를 발송한다.

D(Ksv{H(DBid)||query||authcode||Kmd2})
query 는 질의, authcode 는 인증코드, kms2 는 이동장비의 대칭키

(6) 서버는 이동 단말장치의 인증코드확인 한다. 인증코드는 RF tag 와 해당 센서가 연간관계에 있음을 나타내는 인증 역할을 수행한다. 6)의 단계까지 진행했다는 것은 해당 단말장비가 DB에 등록된 장비이며 센서노드를 동작시키기 위해 지역에 배치된 RF tag를 적법하게 접근하였음을 나타낸다. 그러므로 서버는 인증코드에 해당하는 동작 명령셋을 이동형 단발장치에 발송한다.

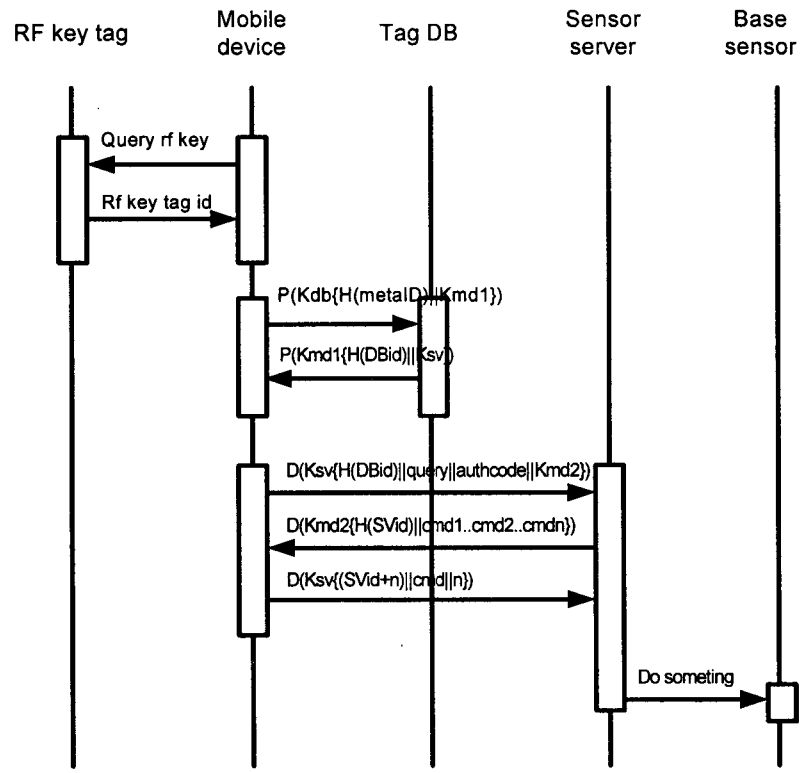
D(Kmd2{H(SVid)||cmd1..cmd2..cmdn})
SVid 는 서버의 임시 id, cmd 는 명령셋

(7) 이동형 단말장치는 수신 받은 명령들 중 하나를 선택하여 서버의 임시 id 에 특정 수열만큼 더한 후 서버에 발송한다..

D(Ksv{(SVid+n)||cmd||n})

(8) 서버는 명령을 베이스 노드에 전달한다.
(9) 센서노드의 지정된 라우팅 테이블을 통해 해당 명령을 수행한다. 8) 9)의 유선환경에 대한 부분은 고려하지 않았으며, 센서들 간의 통신과정 또한 본 논문에서는 제외하였다.
(10) 서버는 수행한 명령에 대한 결과코드를 반송한다.

이처럼 이동형 단말장치를 통해 해당 센서에 직접명령을 내리지 않고 고정 서버로부터 우회적인 명령을 내리는 이유는 다음과 같다. 이동형 단말이 가지는 일반 PC 와의 성능상의 차이가 첫째 이유이고, 둘째 인가받지 않는 명령을 이동형장비로 최대한 노출 시키지 않고자 함이다. 이러한 구성의 장점은 기존의 RFID 시스템이나 Zigbee 센서노드가 개별적으로 보안을 위해 필요한 장비 요건을 크게 낮추 면서도 적절한 보안수준을 제공한다는 데에 있다. 특별히 설계된 RF tag-chip 없이도 일반 상용제품을 통해서 운용 가능하다. 본 절에서는 보안 시스템 운용을 위해 RFID/USN 장비들이 어떤식으로 역활을 분담할 수 있는지 보였다.

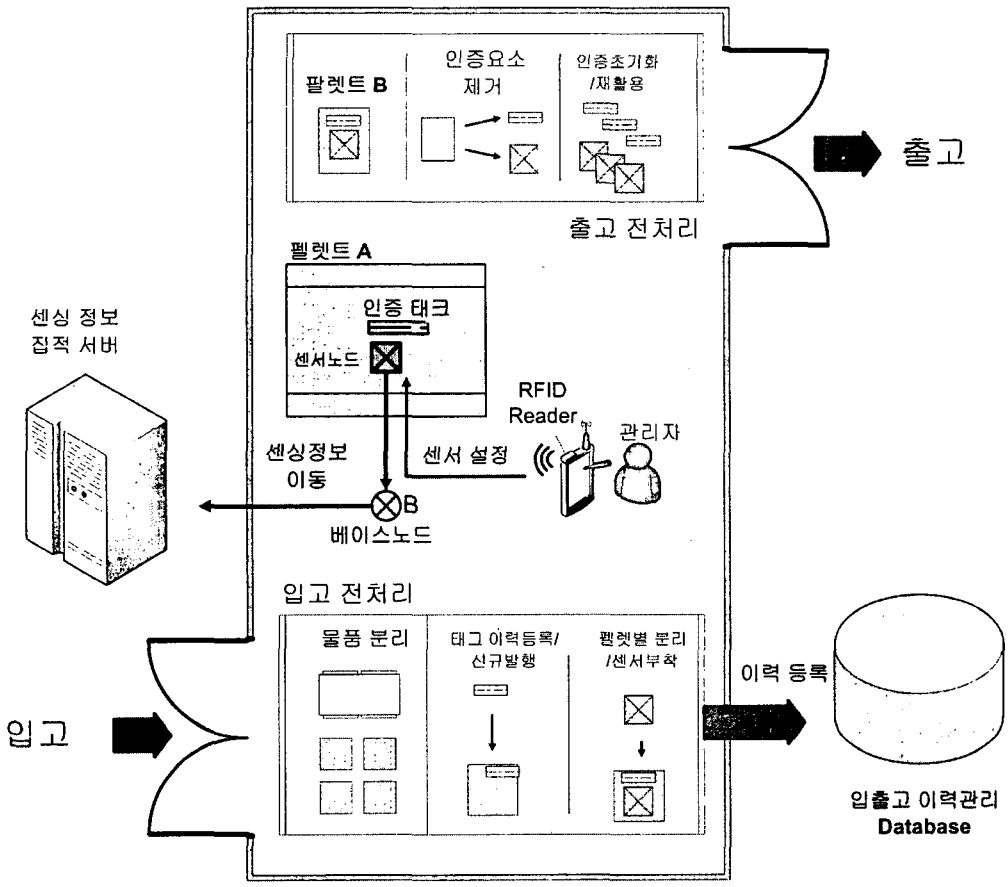


<그림 10> 이동형 단말장치 중심의 순차도

3.4 보안이 적용된 능동형 창고 상태 관리 시나리오

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 11> 은 이러한 과정의 전체적인 흐름을 나타내고 있다.



<그림 11> 보안이 고려된 RFID/USN기반의 능동형 창고 상태관리

4. 결 론

본 논문은 유비쿼터스 환경의 두 요소인 RFID/USN 기술을 사용한 능동형 창고 상태관리 시스템의 보안적용을 목표로 하였다. 이를 위해 이동형 단말장치를 현장에서 보안접근을 위한 중요한 구성품으로 정하고 센서와 이동형장비 그리고 데이터 서버의 관계와 프로토콜을 정의하였다.. 그래서 이동형 단말장치의 기능에 대해서 제안하였고 또한 물류창고의 시나리오를 통해 배치된 RF tag 와 센서 노드 그리고 이동형 단말장치간의 보안이 고려된 적용 관계 또한 정의하였다. 본 연구의 근본적인 아이디어는 USN 의 기본 단말인 센서와 물류의 중심인 RFID tag 이 각각의 물리적 특성이 있음을 인지함으로 써 출발한다. 이 두 기반 기술이 상호보완적으로 운용될 경우 개별적인 운용될 경우에 비해 상대적으로 적은 비용으로도 적정한 수준의 보안 서비스를 제공할 수 있다. 결과적으로 본 연구에서는 RFID 보안을 위해 복잡한 Hash( ) 기능을 수행하는 tag-chip 설계나 센서노드를 사용하기보다 기존의 저렴한 상용 장비를 활용하

여 상호 연계 운용하는 방안을 제시하였다. 물론 시나리오에서 보이듯이 RFID 시스템과 USN 센서노드, 그리고 이를 제어하기 위한 이동형 단말장치가 가장 빈번히 활용될 만한 상황에서 도입 시 본 연구의 효과가 극대화 될 수 있다. 또한 시스템 구성에 평이한 상용제품에 기반을 둘 것으로 제한하였다. 기존의 연구들과의 차별성은 가장 가치 있고 중요한 부분은 자동화된 처리보다 현장 관리자의 의한 판단으로 이루진다고 가정했다. 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.

5. 참 고 문 헌

[1] 장병준, 안선일, 이윤덕, "RFID/USN 기술개발 동향," 한국정보과학회 학회지, 23권, 2호, pp.83~87, 2005.

[2] Klaus Finkenzeller, "RFID Handbook" SE, John Wiley & Sons, 2003.

[3] "RFID Technical Education Seminar", RRC, University of Incheon, 2005.

[4] 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.

[5] Zigbee Web Site: http://www.zigbee.com

[6] 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.

[7] Ari Juels, "RFID Security and Privacy : A Research Survey," IEEE Journal, vol 24, 2006

[8] 홍도원, 장구영, 박태준, 정교일, "유비쿼터스 환경을 위한 암호 기술 동향," 전자통신동향분석, 20권, 1호 pp.65~68, 2005.

[9] Jianuhua Ma, Akito Nakamura, Runhe Huang, "A Random ID Update Scheme to Protect Location privacy in RFID-based Student Administraton Systems," IEEE Proceedings, 2005.

[10] 최재귀, 박지환, "효율적인 식별 기능을 가진 위조 불가 RFID Tag 가변 ID 방식," 한국정보처리학회 논문지 11권, 4호, pp. 447~454, 2004.

[11] Choi Yong Sik, Shin Seung Ho , "The Authentication Protocol using the Hash Lock and PKI IN Ubiqutious environment", ITC-CSCC, Vol.2 pp669~670, 2005.

[12] Lee Min Soon, Lee Ji Sun, Lee Byoung Soo, "Improved Active Warehouse State Control System based RFID/USN," APIS 5th, pp.235~39, 2006.

저 자 소 개

전 영 준 : 인천대학교에서 공학 학사 석사를 취득하였으며, 현재 인천대학교에서 컴퓨터공학과 박사과정 중. 관심분야는 RFID/USN, Security, 소프트웨어공학

최 용 식 : 인천대학교에서 공학학사 석사를 취득하였으며, 현재 인천대학교에서 컴퓨터공학과 박사광정 중. 관심분야는 컴퓨터 통신, 임베디드시스템, 암호학

신 승 호 : 경희대학교에서 전자공학과 공학사를 취득하였으며, 경희대학교에서 공학석사와 박사를 취득하였으며, 현재 인천대학교 컴퓨터공학과 교수로 재직중이다. 관심분야는 컴퓨터 통신, 신호처리, 암호학

박 상 민 : 한양대학교 산업공학과 공학사를 취득하였으며, 한양대학교에서 산업공학과 공학 석사와 박사를 취득하였으며, 현재 인천대학교 산업경영공학과 교수로 재직중이다. 관심분야는 e-Logistics

저 자 주 소

전 영 준 : 인천광역시 남구 간석 4동 616-25

최 용 식 : 경기도 부천시 소사구 송내동 300-13 동신 아트빌 402호

신 승 호 : 서울시 서대문구 남가좌동 173-18

박 상 민 : 서울시, 강남구 대치동 896-21