센서노드 접근을 위해 RFID 를 지역 키로 사용하는 이동형 단말장치상의 개선된 보안 프로토콜 설계

Design improved security protocol on mobile device for sensor node access using RFID local key

전영준*, YoungJun John, 최용식*, YongSik Choi, 박상현*, SangHyun Park , 한 수*, Soo Han and 신승호*, SeungHo Shin
*인천대학교 컴퓨터공학과

요약 RFID 와 sensor network 의 두 기반 기술은 독특한 물리적 특정을 가지며 상호 보완적인 관계를 가지고 있다. 이러한 관계는 창고 안 물품의 상태파악과 입출 재고를 관리하는 형태로 응용된다. 창고 내 물품 보관 단위인 파렛트(Pallet) 에 RFID 태그를 부착하여 입/출고시의 물품을 식별한다. 그리고 Zigbee 무선 통신기능을 가진 센서 모듈에 의해 물품의 환경 상태 정보를 파악한다. 이후 현장 관리자나 소비자들은 이동형 단말장치를 통해 현장에서 다양한 USN 상의 정보들과 상호작용 한다. 이 과정에서 이동형 단말장치를 통한 RFID tag 정보와 센서 노드의 접근이 공중파 상에 노출 된다. 이러한 센서 노드 접근을 보호하기 위해 추가적인 칩 설계 등의 비용 지불로 기밀 노출에 대처할 수 있다. 이에 대한 대안으로 인프라형태로 놓여진 RFID tag 와 단말장치에 탑재될 RFID 리더를 활용해 더 적은 비용으로 보안 서비스를 받고자 한다. 그래서 유비쿼터스 환경에서 센서 노드에 대한 접근을 제어하기 위해 RFID tag 를 지역키(local key) 처럼 사용한다. 또한 이 과정에 보안이 적용된 프로토콜을 설계 하는 것이 본 논문의 주된 목표이다.

핵심어: RFID, sensor network, USN, 이동형 단말장치, 보안 프로토콜

1. 서론

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. RF 태그는 반도체 칩과 안테나로 구성되며, 칩에는 특정 정보를 저장하고, 트랜스폰더의 요청에 의해 자신의 정보를 전달한다[1,2].

USN에서 핵심 단말인 센서노드와 RFID의 RF tag는 각각의 영역에서 고유한 특징을 가지고 있다. RF Tag는 센서노드에 비해 매우 저렴하며, 별도의 전원 없이 운용이 가능하다. 센서 노드는 부착된 센싱 장비에 의해 실시간의 환경정보를 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 시간 동안 센서노드의 프로세서를 통해 자료를 처리하고 통신한 후 노드를 sleep 하는 운용전략을 취하게 된다.

USN/RFID 기술이 응용의 예로 물류 집하장이나 수출입항의 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 제어하기나 필요한 정보를 현장에서 취득하기 위한 과정이 공중파 상에 노출된다. 그러므로 대상의 수준에 알맞은 보안 서비스가 고려되어야 한다[4,5].

센싱정보를 수집하는 일반적인 시스템 운용은 특정 주기마다 주변환경의 상태정보를 수집하는 것이다. 또한 센서에 정해진 임계 값과 환경 정보를 비교하여 알람과 같은 이벤트를 생성한다. 그 외에 이동형 장비를 통해 원격지에서 특정 센서의 정보를 취득하기 위해 수동적으로 명령을 내리는 과정을 고려해 볼 수 있다. 이 과정은 원격지에서의 수동관리 체계에서 현장 관리자가 보안코드를 습득하여 인증코드를 받아 지정된 센서가 원하는 동작을 수행하도록 명령하는 형태로 확장해 볼 수 있다. 그러나 제한된 자원만이 허용되는 이동형 장비에 추가적인 보안장치를 부착하거나 설계하는 것은 비용 면에서 부담이 될 수 있다. 본 논문에서는 이동형 단말장치에 RFID 리더를 부착하여 RFID 태그정보를 수신한다. 그리고 수신 받은 태그 정보를 센서 노드를 제어하기 위한 인증키처럼 사용한다. 이를 위해 RFID 지역 키 (RFID local

key) 개념을 제안하여 활용한다.

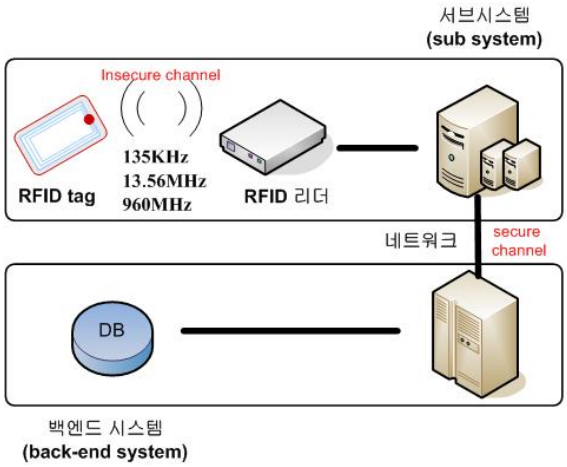
2. 관련연구

2.1 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, Zigbee 는 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. 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[7,8]. 실제적인 센서 네트워크의 구현을 위해서 필요한 것은 고속의 무선 네트워크 보다 낮은 복잡도의 회로와 저가격의 저전력의 구성이다. 이를 통해 배터리로 몇 개월에서 수년까지 지속적인 생존이 가능하다.

2.2 RFID 기반 기술

RFID 시스템에서 다음과 같은 특성을 갖는다. 첫째 정보를 담고 있는 RF tag 와의 access 과정이 비접촉식 이어서 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 개인 프라이버시 문제가 발생한다[4,5].



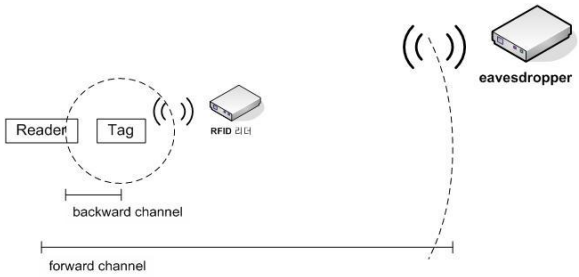
(그림 1) RFID 시스템의 일반적인 구성

(그림 1) 은 일반적인 RFID 시스템의 구성을 보여 주고 있다. 유선망 기반의 네트워크와 비교해 본다면 RFID 태그와 태그 리더간의 통신이 특정 주파수대의 통신에 기반하는 것과 이 과정에 유선망에 준하는 보안알고리즘을 적용하는 것이 쉽지 않다는 것이 차이이다.

2.3 RFID 프라이버시 보호 요소

2.3.1 기밀성 (confidentiality)

(그림 2)는 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.



(그림 2) RFID 와 tag 간의 정보 누출

2.3.2불구분성 (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.

2.3.3전방 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 과정에서의Spoofing은 방지하지 못하지만 탐지가 가능하다. 이 방식은 해시 함수만을 요구하는 단순한 구조이다. 그래서 저비용으로 구현

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

(그림 3) Hash Lock의 Unlocking 프로토콜

(그림 3)은 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[4][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[10]. Hash Lock 방식은 인가받지 않은 Reader기가 Tag를 읽는 것을 방지 할 수 있으며 Hash Function만을 요구하므로 저비용으로 구현가능하다. (그림 4) 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.

Tag는 자신의 비밀 키를 이용하여 생성된 metaID를 Reader에 보내고 Reader는 해당되는 키(k)를 만들어내 Tag에 보낸다. 이때 Tag는 Reader로부터 보내진 키(k)를 해시값과 자신의 metaID에 비교하여, 그 값이 동일하면 자신의 ID를 전송한다.

(그림 4) Hash Lock과 PKI 방법을 이용한 프로토콜

(그림 4)는 다음의 단계를 거쳐 Tag 를 인증한다.

(1)Reader는 Tag에게 질의를 보낸다

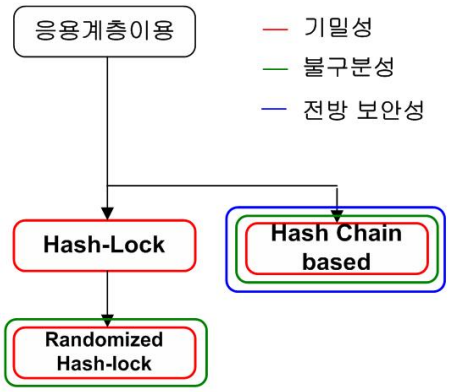
(2)Tag는 미리 생성된 비밀 키를 이용한 생성된 MetaID를 보낸다.

(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[10].

2.6 RFID Security Schemes

(그림 5)는 <2.4> 절의 RFID 프라이버시 요건에 맞추어 RFID 보안프로토콜의 관계를 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[4][11]. 이를 위해 Hash-Lock 에서 부족한 보안 요소를 새로운 칩설계나 속도 저하 없이 만족하기 위해 유선통신이나 이동형 단말장치의 wlan을 사용한다. 다시말해 RFID 통신 속도나 장비비용등의 trade-off 에 대응해 외부자원을 통해 해결하고자 한다.



(그림 5) RFID Security Schemes

3. 본론

3.1 이동형 단말장치 구성

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. 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 센서접근 제어는 공중(air interface) 을 통해 간접적으로 이루어진다. 그러므로 센서의 동작제어 명령에 대한 보안이 필요하다. (그림 6) 은 RFID tag 를 해당 지역의 센서노드 접근중에 관문에 해당하는 기본 컨셉이다.

3.1.1 이동형 단말장치

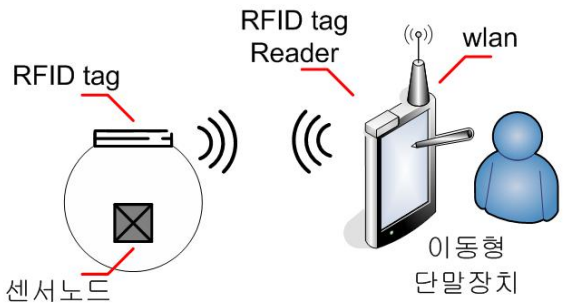
이동형 단말장치 자체의 구성은 RF tag로부터 정보를 수신할 수 있는 1.RF tag reader 모듈과 수신된 태그 정보를 분석할 정도의 2.cpu 파워, 마지막으로 분석된 결과를 서버군 으로 전송할 3.wireless lan 모듈로 구성된다. 본 논문의 설계에서는 별도로 tag 에 데이터를 기록하는 과정이 없으므로 단순히 태그로부터 데이터를 수신할 수 있는 정도면 충분하다.

3.1.2 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 암호화를 위해 추가적인 tag 설계는 가정하지 않는다. 범용의 tag로도 운용 가능하며, 전파 차폐된 공간에서 write 되는 정도면 충분하다.

3.1.3 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.



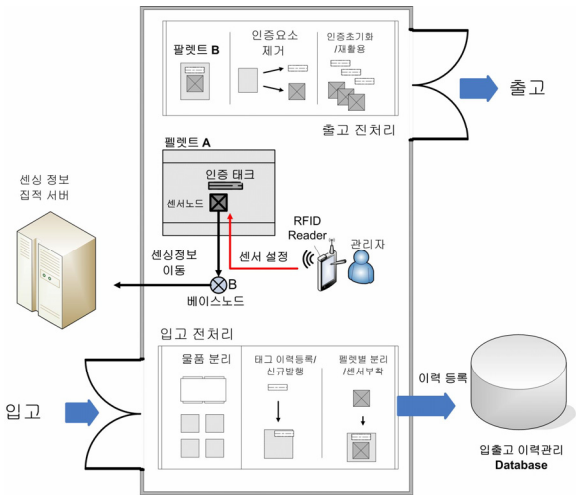
(그림 6) 이동형 단말장치 와 센서/RF tag 연계 컨셉

3.2 적용 시나리오

3.2.1 창고 상태관리

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[3].



(그림 7) RFID/USN 적용하의 창고관리 운용

대형 설비 등의 장비이력을 관리하기 위한 기존의 유선 설비에서 고가의 기민한 장비에 센서를 부착한 형태는 오래 전부터 구축되어 왔다. 지능화된 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 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[3].

3.2.2 유비쿼터스 매장

유비쿼터스 매장은 국제 표준으로 확정된 RFID 태그 형식인 EPC Gen2를 사용하여 RFID 리더기를 내장한 휴대폰으로 상품 정보를 확인하는 형태를 시작으로 다양한 적용모델이 검토되고 있다. RFID 를 활용한 모델 중 초기 단계는 전자 카달로그 시스템형태이다. RFID 리더기가 내장된 '스마트 선반' 에 RFID 칩이 부착된 상품을 선택하면 해당 상품의 정보를 매장의 디스플레이 장치에 표시해 소비자에게 다양한 정보를 전달한다. 이러한 정보에는 해당제품의 진열대 위치, 가격 정보등을 들 수 있다.

3.2.3 시나리오 분석

일반 소비자를 대상으로 한 매장과 물품의 상태를 관리해야 할 창고 상태 관리는 제공받아야 할 서비스의 수준과 상

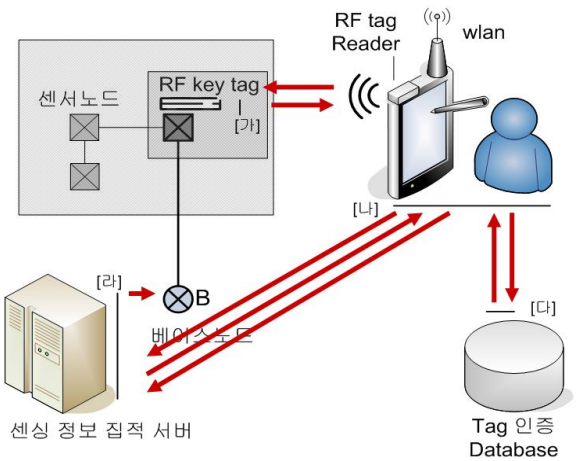
황에 차이가 있다. [표. 1] 은 이를 간략히 정리하여 나타내고 있다. 두 시나리오의 차이점은 사용자의 입장에서부터 출발한다. 일반 물류창고는 출입이 제한된 닫힌 공간에 해당한다. 또한 작업자는 센서의 이상징후 발견에 의한 대처나 센서의 상태 제어 등 일반적인 정보 열람보다 많은 제어 권한을 가지게 된다. 그러므로 닫힌 공간에서는 해당 센서를 정확히 제어하기 위해 명령어들을 주고 받는 행위에 집중해야 한다. 그리므로 혼선 없는 정확한 명령전달이 주된 목표이다. 이에 반해 매장에서는 수 많은 소비자들이 해당 지역의 센서나 RFID 태크 로부터 물품의 정보를 얻기 위해 접근을 요청하게 된다. 그러므로 출입에 특별한 제한이 없는 매장은 열려있는 공간처럼 다뤄지게 된다. 열려있는 매장 공간에서는 사용자들간의 통신에 기밀성을 유지하는 것이 주된 목표가 된다. 결과적으로 두 시나리오는 접근하는 목적에 따라 접근 절차에 차이를 두어야 함을 나타낸다.

[표 1] 시나리오 분석

	창고 상태관리	매장
사용자 권한수준	높음	낮음
지역 트랜잭션 량	적음	많음
사용자 접근목적	물품 상태관리	USN 정보취득
지역 작업 형태	센서 상태 제어	개인정보 보호

3.3 이동형 단말장치를 통한 보안 프로토콜 설계

(그림 8) 은 센서 노드에 접근하기 위해 RFID를 지역키처럼 사용하여 센서노드에 대한 접근 권한을 인증하는 과정을 보여준다. 이 과정은 (그림 8) 안에 나타낸 [가],[나],[다],[라] 의 네 구간으로 분리하여 고려해 볼 수 있다.



(그림 8) 이동형 단말장치를 통한 관계 도식

각 구간을 표로서 정리하면 [표 2] 와 같이 나타낼 수 있다.

[표 2] 프로토콜 구간 관계

	나	다	라
가	작업자~ 지역키	센서인증권한~ 지역키	명령수행지~ 지역키
나		인증대행소~작업자	인증권자~명령대행
다			인증대행소~명령행

(그림 9) 는 첫번째 시나리오인 창고 상태관리를 위한 절차를 나타내고 있다. 이는 아래와 같은 순서로 이루어 진다.

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

여기서 P(k{}) 는 PKI 방식을 말하여 공개키 K로 암호화한다. H( ) 는 hash 함수를 말한다.

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

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

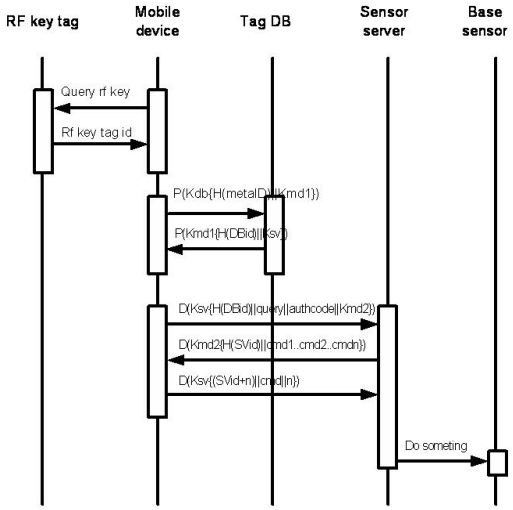
6). 서버는 이동 단말장치의 인증코드를 확인 한다. 인증코드는 RF tag 와 해당 센서가 연간관계에 있음을 나타내는 인증 역할을 수행한다.

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})



(그림 9) 이동형 장치를 통한 프로토콜 흐름도

8). 서버는 명령을 베이스 노드에 전달한다.

9). 센서노드의 지정된 라우팅 테이블을 통해 해당 명령을 수행한다.

10). 서버는 수행한 명령에 대한 결과코드 를 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 인가 받지 않는 명령을 이동형 장비로 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 어떤 식으로 역할을 분담할 수 있는지 보였다.

3. 결론

본 논문은 인프라로서 부착된 이동형 단말장치상의 RFID 리더를 활용해 평이한 장비구성으로 보안 서비스 제공에 목적이 있다. 논문의 근본적인 아이디어는 USN 의 기본 단말인 센서와 물류의 중심인 RFID tag , 각각의 물리적 특성을 구별하는 것에서 출발한다. 이 두 기반 기술이 상호보완적으로 운용될 경우 개별적인 운용될 경우에 비해 상대적으로 적은 비용으로도 적정한 수준의 보안 서비스를 제공 할 수 있다. 결과적으로 본 연구에서는 RFID 보안을 위해 복잡한 Hash( ) 기능을 수행하는 tag-chip 설계나 센서노드를 사용하기보다 기존의 저렴한 상용 장비를 활용하여 상호 연계 운용하는 방안을 제시하였다. RFID 시스템과 USN 센서노드, 그리고 이를 제어하기 위한 이동형 단말장치가 가장 빈번히 활용될만한 상황에서 도입 시 본 연구의 효과가 극대화 될 수 있다. 또한 시스템 구성에 평이한 상용제품에 기반을 둘 것으로 제한하였다.

참고문헌

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

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

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

[4]Ari Juels, “RFID Security and Privacy : A Research Survey,” IEEE Journal, vol 24, 2006

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

[6] 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.

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

[8] 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.

[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] 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.

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