유비쿼터스 환경에서의 능동형 창고 상태관리를 위한 보안 시스템 설계

일자 : 2006년 11월 8일

발표자 : 전영준

개요 (1)

목차
-개요
-RFID 시스템
-RFID 프라이버시
-보안프로토콜
-창고상태관리
-보안적용
-참고문헌

- **RFID/ USN 기반의 창고 상태 관리 시스템에서 상태정보 습득 과정의 보안적용을 위한 시스템 구성**
  - 3가지 이슈
    - 의사판단의 주체인 현장 관리자에 적절한 제어 정보의 제공함
    - 센서의 동작을 제어하기 위한 RFID tag 보안 접근
    - 센서 노드 자체의 생존성 이라는 세 가지 관점의 절충점을 찾기 위한 시도로서 설계하였다

개요 (2)

- **유비쿼터스 센서 네트워크**
  - 광범위하게 설치되어 있는 유무선 네트워크 인프라에서 상황 인식을 위한 다양한 센서들을 장착한 형태를 말함.

- **물류에서 USN/RFID 기술의 응용**
  - 물류 집하장이나 수출입 항의 경우 창고에 보관된 다양한 제품의 관리를 말함
  - 관리해야 할 센싱 정보들
    - 보관되는 제품들에 따라 온도, 습도, 압력, 빛 등
    - 상태정보가 제품의 품질을 좌우하는 경우.
    - 제품상태에 의해 출고시기와 유통기간이 변경되기도 함.

USN 기반 기술

- **Zigbee**
  - 특징
    - 저전력/저비용의 특징인 2.4GHz 기반의 가정용 무선 네트워크 규격임
    - 반경 30m 네에서 250kbps의 속도로 255대의 기기들을 연결 가능함.
  - 이슈
    - 대용량의 데이터 전달이 요구되지 않는 환경에서 긴 배터리 수명 보장됨.
    - *일정 거리 이상의 전송 영역의 확보가 필요한 곳에 사용 가능하다.*
    - *일반적으로 무선네트워크에서 데이터 송수신부분의 전력 소모량이 가장 크다.*

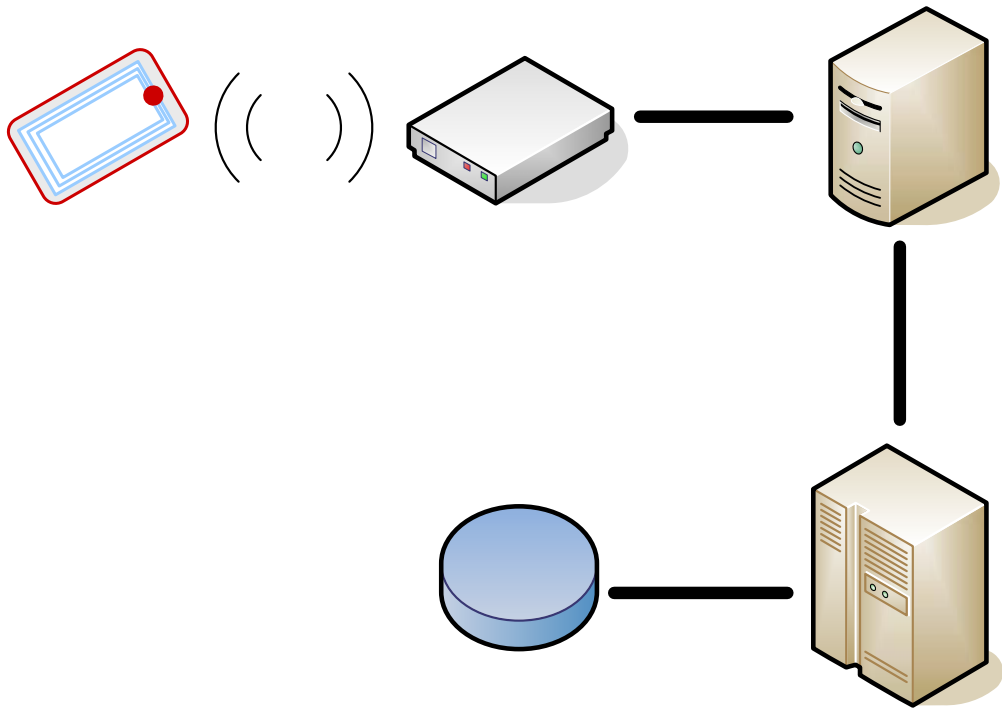
RFID 시스템 개요 (1)

- **RFID 시스템의 장점**
  - 비접촉식으로 오염에 강함
  - 여러 개의 태그 해독 가능
  - 다양한 형태의 데이터 기록 가능

- **RFID 기술은 이진 정보를 보관하고 있는 RF 태그와 트랜스폰더 형태로 구성됨.**
  - RF 태그는 반도체 칩과 안테나로 구성됨
    - 칩: 특정 데이터를 저장.
    - 트랜스폰더: 데이터 전송.
  - 태그는 반도체 칩과 안테나를 가지고 있으며, 칩에 있는 메모리를 통해 태그 식별을 위한 EPC 코드가 저장된다.

RFID 시스템 개요 (2)

- 일반적인 RFID 시스템 구성



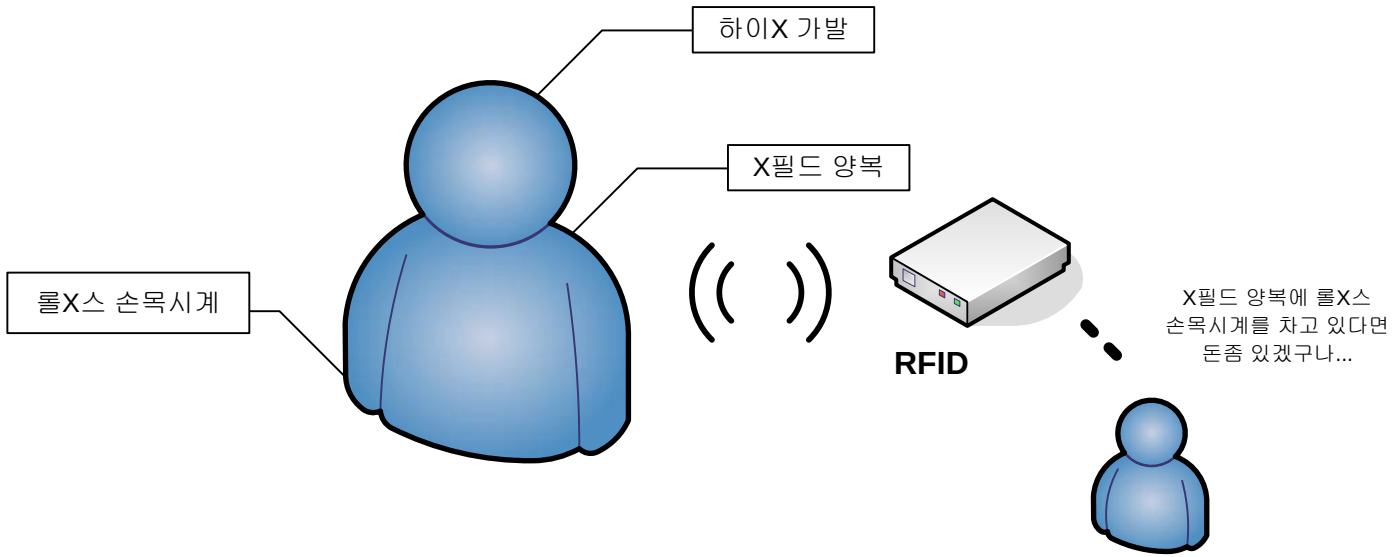
Insecure

RFID 시스템에서의 보안 취약성 (물류/유통망)

- **프라이버시 침해**
  - 태그가 삽입된 물품의 구매자(소유자)의 사생활 정보 유출
  - 소유자의 실시간 위치 추적
- **위변조 문제**
  - 고가 물품의 태그에 대한 위변조
    - 명품
    - 고액권
  - 중요 물품의 태그에 대한 위변조
    - Passport
    - 출입증

RFID 프라이버시 침해

- **정보 유출(Information leakage)**
  - 태그가 삽입된 물품의 구매자(소유자)의 사생활 정보 유출
- **위치 추적(location Tracking)**
  - 소유자에 대한 실시간 위치 추적으로 인한 location privacy 침해



프라이버시 보호 요소 [1]

- **RFID시스템에서의 프라이버시 보호를 위한 필수 보안 요건**
  - 기밀성 (confidentiality)
    - 통신내용에 대한 기밀 유지

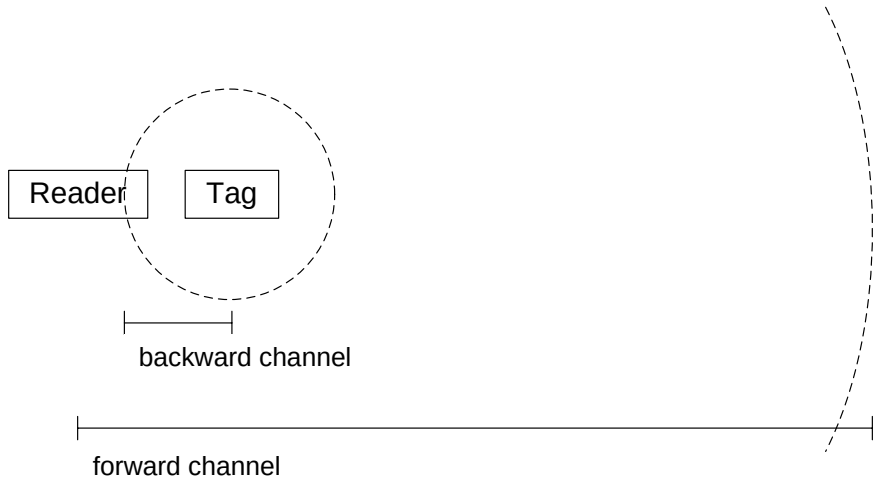
      → **정보 유출 방지**
  - 불구분성 (indistinguishability)
    - 태그의 송신 정보(출력값)가 동일하거나 예측 가능해서는 안됨

      → **위치 추적 방지**
  - 전방 보안성 (forward security)
    - 태그가 물리적 공격을 당해서 현재의 비밀 정보가 드러나더라도 과거의 출력값을 계산해 낼 수 없어야 함

      → 과거 위치 정보**(location history)** 유출 방지

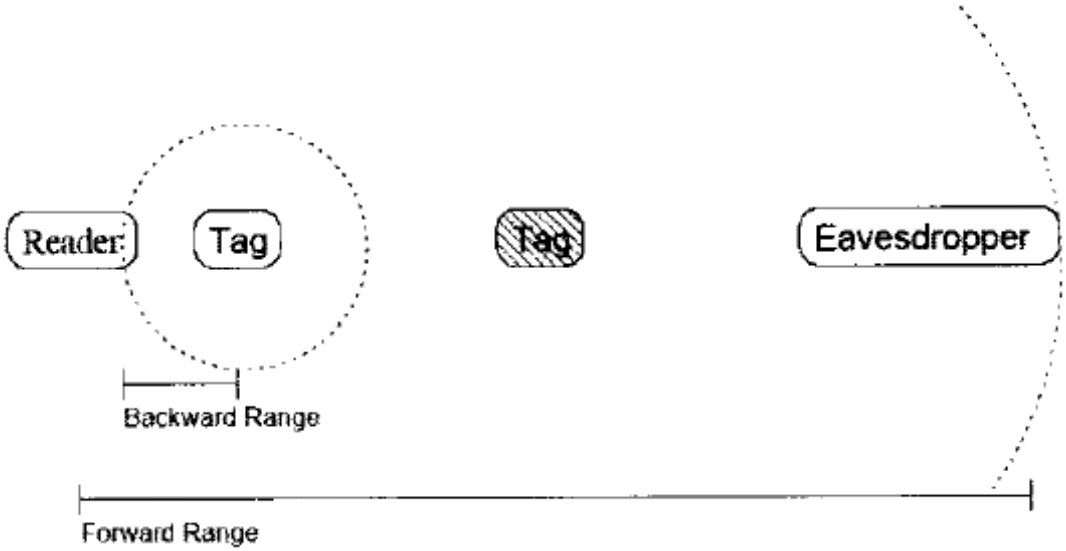
프라이버시 보호 요소 [1]

- **기밀성 (confidentiality)**
  - 태그–리더 간의 통신
    - air interface : 안전하지 못한 채널(insecure channel)이다
      - forward channel / backward channel
    - 식별 정보를 그대로 전송해서는 안됨 → *기밀성* 보장
      - 백엔드 서버 DB의 access code
      - 암호화



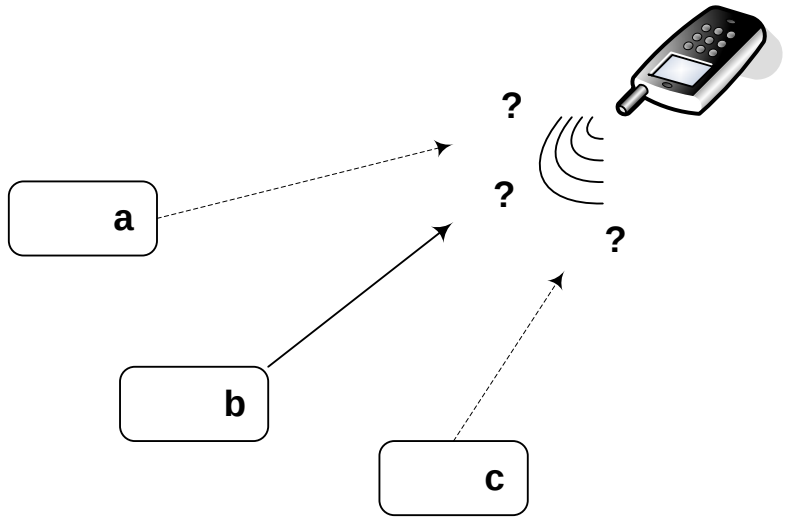
RFID 보안 문제 [2] (리더-태그 보안 문제)

- **리더-태그 보안 문제 : Forward and Backward Range**
  - Forward Range:
    - 리더가 태그에게 질의를 보낼 수 있는 물리적 범위
  - Backward Range:
    - 태그가 리더에게 질의에 대한 응답을 보낼 수 있는 물리적 범위
  - 도청자가 Forward Range안에 있을 때 이진 탐색 기법을 사용하는 RFID 시스템의 리더는 태그에서 태그의 정보를 계속 전송하게 되고 도청자는 이를 성공적으로 도청



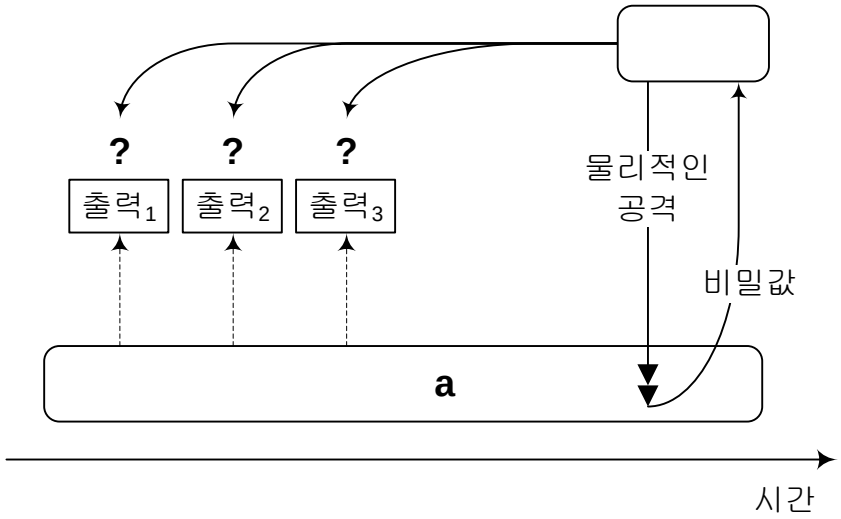
프라이버시 보호 요소 [2]

- **불구분성 (indistinguishability)**
  - 위치 추적
    - 위치 추적이 가능 하려면
      - 특정 태그를 다른 태그와 구분 가능해야 함
    - 위치 추적을 피하려면 → *불구분성* 보장
      - 태그의 출력값은 항상 달라야 하며, 난수와 구분이 불가능해야 한다
      - 미래의 출력값이 예측이 불가능해야만 한다



프라이버시 보호 요소 [2]

- **전방 보안성 (forward security)**
  - 물리적인 공격
    - 태그는 저가의 하드웨어이기 때문에 물리적인 공격 가능성을 배제할 수 없다
      - laser-etching, …
    - 현재의 태그 내부의 비밀 값이 노출되어도 과거의 출력값을 계산할 수 없어야 한다 → *전방 보안성* 보장



RFID 보안 프로토콜 개요 [1]

Reader access 보안

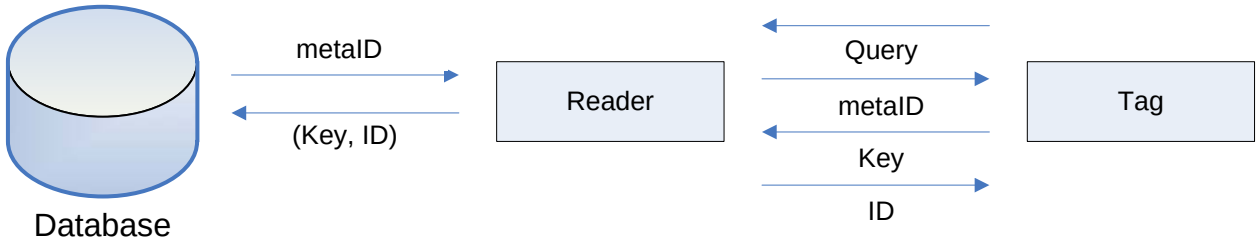
- 미리 등록된 공개키로 Tag를 인증
- meta ID로 각 Tag의 유일한 키(k)를 생성
- meta ID = H(k)로 키 확인

• Tag access 보안

1. 자신의 비밀키를 이용하여 생성된 meta ID 를 Reader에 전송.
2. Reader는 해당되는 키(k)를 만들어내고 Tag에 반송함
3. Reader로부터 받은 키(k)의 해쉬 값과 자신의 meta ID를 비교
4. 값이 동일하면 자신의 ID를 전송.

RFID 보안 프로토콜 [1]

- **Hash lock 방식**
  - 일방향 해시 함수의 역함수 계산이 어려움에 기반함.
  - 인가받지 않은 Reader기가 Tag를 읽는 것을 방지.
  - Spoofing은 방지하지 못하지만 탐지는 가능.
  - 해쉬 함수만을 요구하므로 저비용으로 구현 가능함.
  - meta ID가 고정되어 공격자는 meta ID를 이용하여 해당 Tag의 위치를 추적할 수 있는 문제가 발생함.



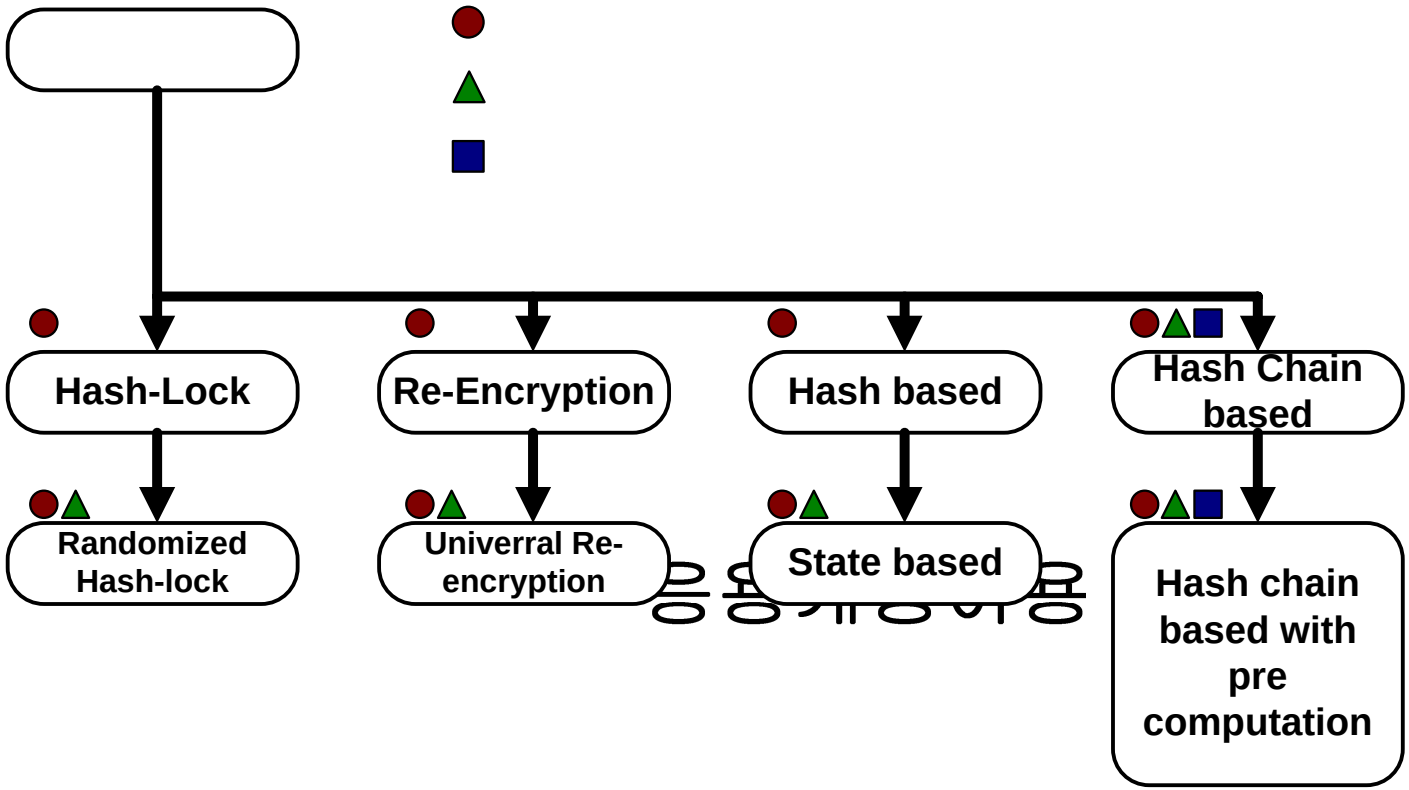
RFID 보안 프로토콜 [2]

- **Randomized hash lock 방식**
  - Hash lock 방식의 개선안.
  - 고정된 meta ID를 갖게 하지 않기 위하여 난수 생성기를 통하여 접근할 때마다 Tag에서 다른 값을 가짐.
  - Tag에 대한 추적은 불가능
  - 해쉬 함수와 난수가 동시에 생성되어야 하므로 저비용으로 구현하기 어려움.

RFID 보안 프로토콜 [3]

- **Hash-chain 방식**
  - Randomized hash lock 방식의 문제점을 개선함.
    - Tag안의 정보가 노출되면 이전의 위치 정보가 추적되는 것을 방지함
    - 해쉬함수와 난수생성으로 인한 고비용을 개선함.
  - Tag안에서 해쉬 함수만으로 Tag정보의 보호가 가능함.
    - Tag의 위조 문제와 서버에서 Tag ID를 식별할 경우 해쉬 함수를 계속해서 반복, 수행함.
    - Randomized hash lock 방식보다 더 많은 연산이 요구되는 문제가 발생함.

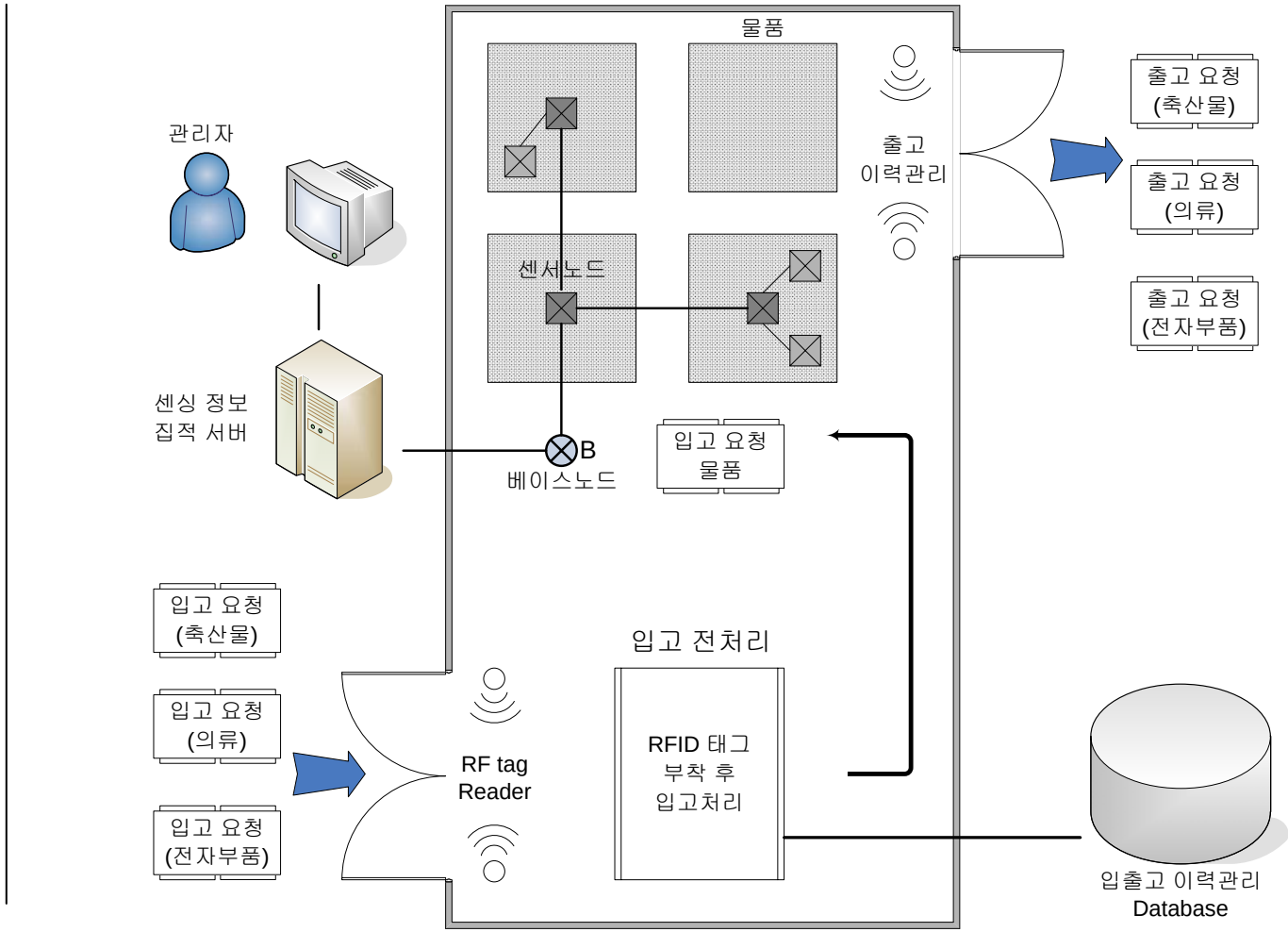
RFID Security Schemes



능동형 창고 상태 관리 시스템 (2)

- **능동형 창고 상태 관리**
  - 입고되는 시점에 보관되는 제품의 이력을 관리하고 상태를 파악하여 창고물품의 전반적인 상황을 최적의 상태로 관리할 필요가 있음.
  - 구성
    - 센싱 대상이 되는 물품
    - 센싱 정보가 최정적으로 수집되고 기록되는 서버
    - 센서와 물품관리를 위해 현장 관리자가 사용하는 이동형 단말장치
  - 동작
    - 자동적으로 물품의 상태정보 수집
    - 이동형 장비를 통해 물품을 배치하거나 특정 센서의 정보를 취득하기 위해 센서에 명령 하달.
    - 현장 관리자는 보안코드를 습득하고 인증받아 특정센서가 원하는 동작을 수행하도록 명령

능동형 창고 상태 관리 시스템 (3)

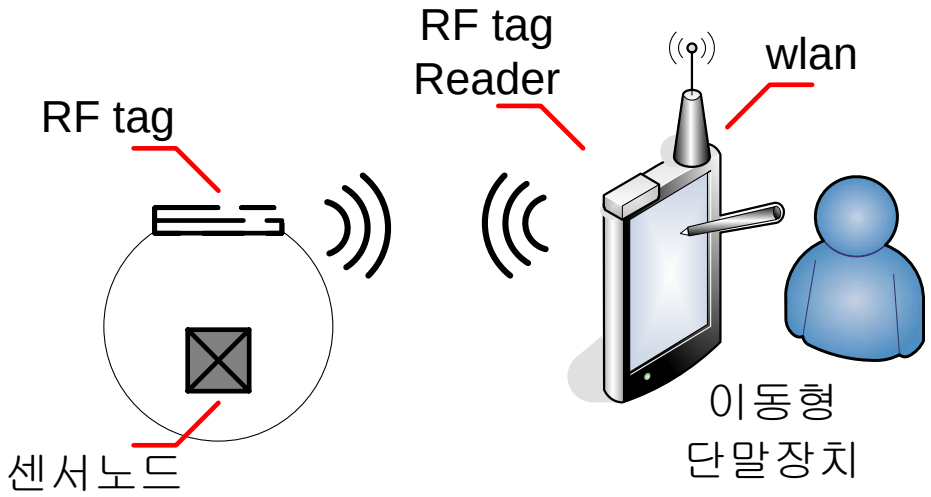


이동형 장비를 통한 창고 상태 관리.

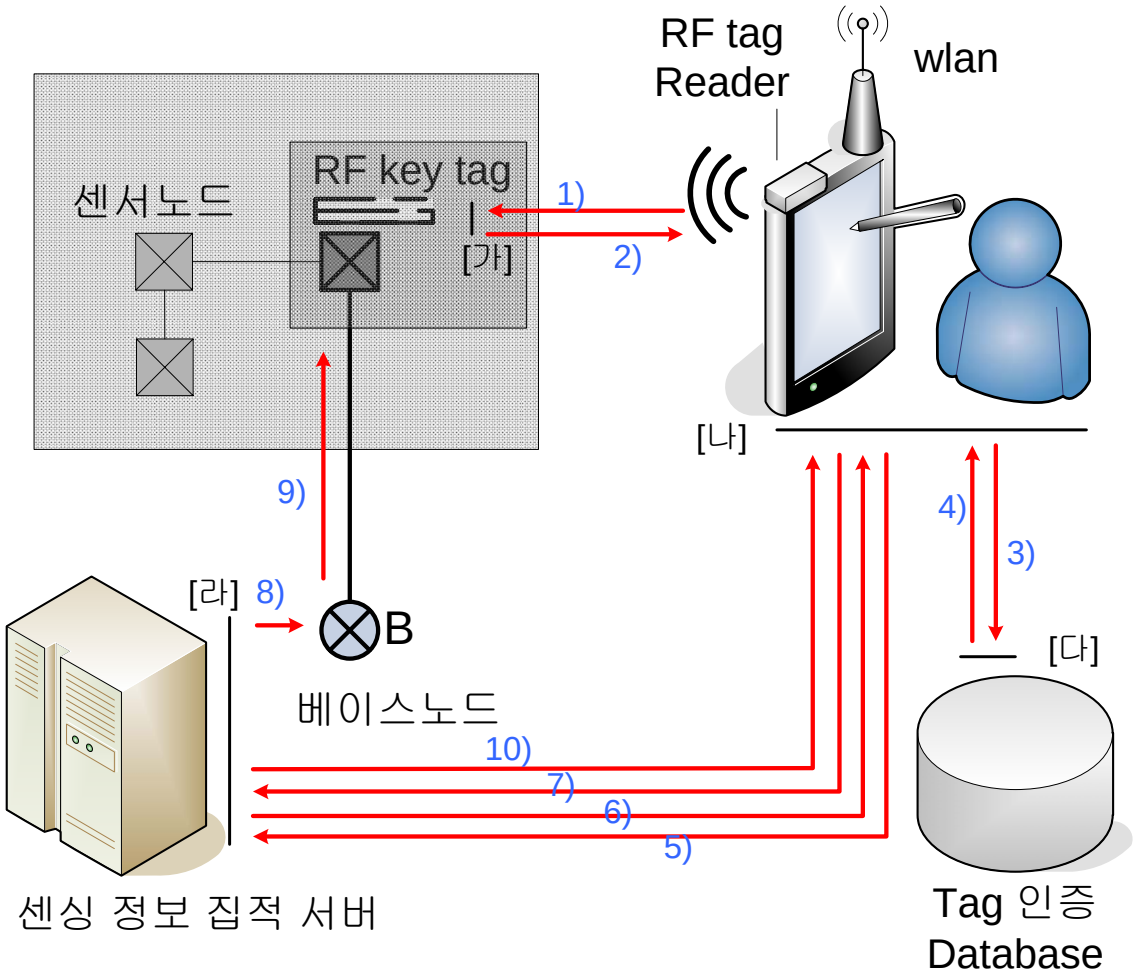
- **개선된 능동형 창고 상태관리 시스템**
  - 데이터 생성 센서와 서버군의 두 가지 요소를 기준으로 입출고 프로세스 설계가 이루어졌음.
  - 이동형 단말장치를 마지막 세 번째 요소로 추가함
  - *이동형 단말의 기능과 역할을 별도로 고려해야 하는 이유는?*
    - 센서에 의해 수집되는 정보가 자동화 처리가 가능하지 않은경우
    - 경보(alarm)에 의해 관리자가 원격지의 센서를 직접 조작해야 하는 경우.
    - 배터리에 의해 저 전력으로 운용되어야 하는 센서 노드

이동형 단말장치 구성

- **이동형 단말장치**
  - RF tag로부터 정보를 수신
  - wireless lan 모듈
- **RF tag**
  - 특정지역의 센서노드에 대한 동작 권한을 상징함
- **센서노드**
  - 이동형 단말장치가 제어하고자 하는 대상



RFID tag(RF tag)와 이동형 단말장치를 보안 운용 [1]



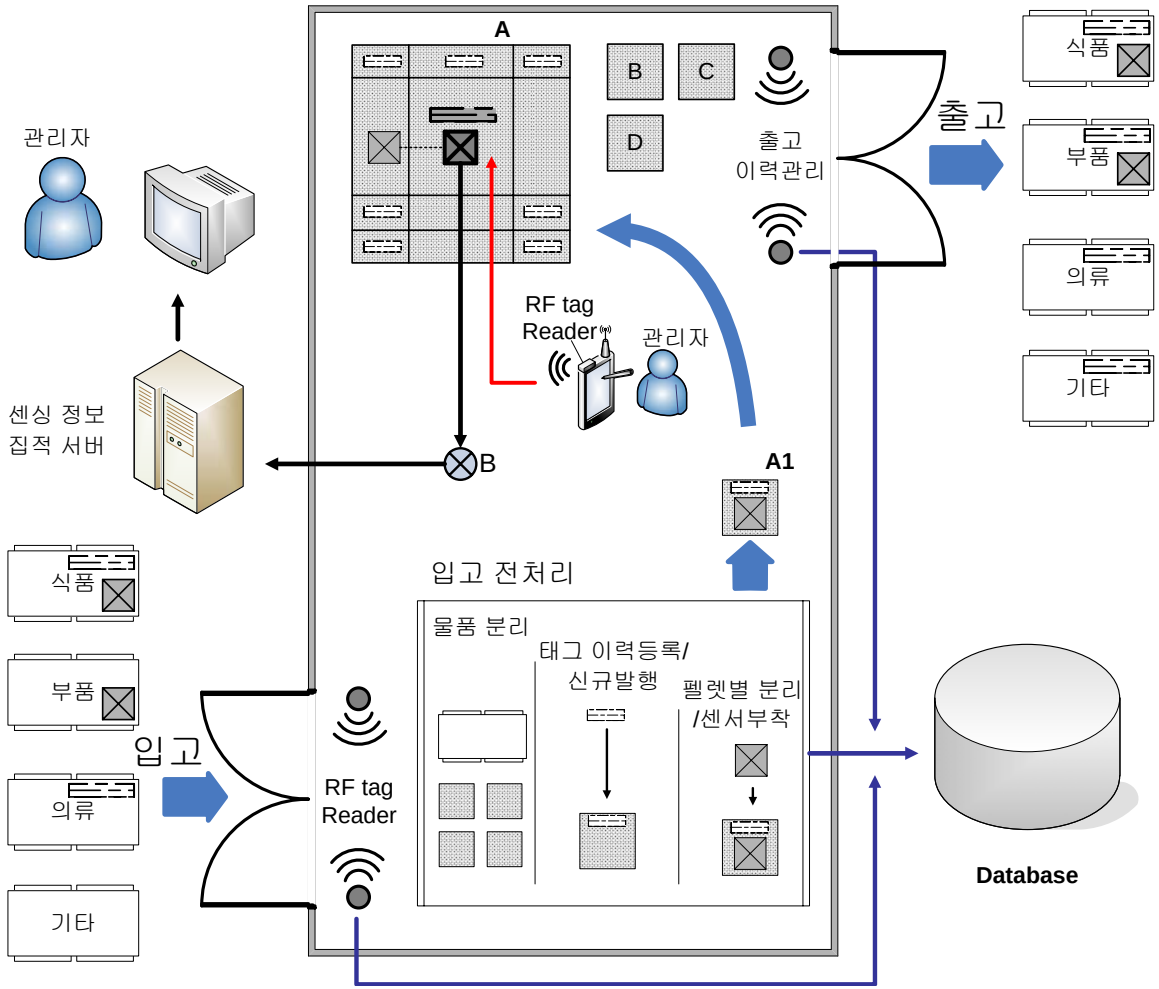
RFID tag(RF tag)와 이동형 단말장치를 보안 운용 [2]

1. RF reader를 통해 태그에 질의
2. RF tag 는 배치 전에 특정 지역에서 비밀 키를 이용해 write된 metaID를 전송함.
3. 이동형 단말장치는 다음의 과정을 수행하여 wlan 을 통해 DB에 발송함
   - P(Kdb{H(metaID)||Kmd1}) : *Kdb 는 DB 공개키, Kmd1 는 이동장비의 공개키*
4. DB H(metaID) 에 해당하는 인증코드를 wlan 을 통해 단말장치에 다음의 과정을 수행함.
   - 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 전송함. 해당 이동장비의 인증코드를 발송함.
   - D(Ksv{H(DBid)||query||authcode||Kmd2}) : *query 는 질의, authcode 는 인증코드, kms2 는 이동장비의 대칭키*

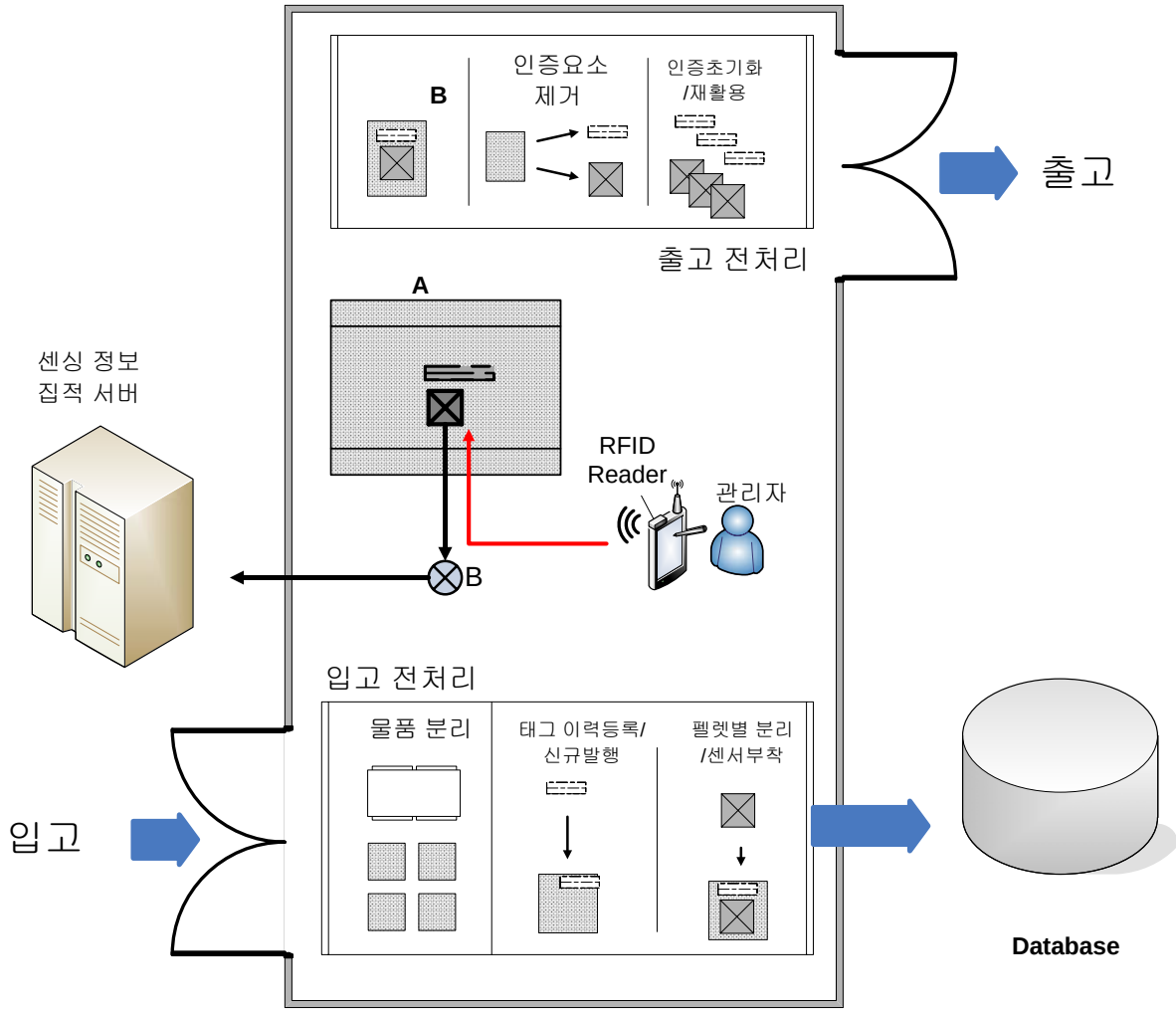
RFID tag(RF tag)와 이동형 단말장치를 보안 운용 [3]

1. 서버는 이동 단말장치의 인증코드확인 한다. 인증코드는 RF tag 와 해당 센서가 연간관계에 있음을 나타내는 인증 역할을 수행함.
   - D(Kmd2{H(SVid)||cmd1..cmd2..cmdn}) : *SVid 는 서버의 임시 id, cmd 는 명령셋*
2. 이동형 단말장치는 수신 받은 명령들 중 하나를 선택하여 서버의 임시 id 에 특정 수열만큼 더한 후 서버에 발송함.
   - D(Ksv{(SVid+n)||cmd||n})
3. 서버가 명령을 베이스 노드에 전달함.
4. 센서노드의 지정된 라우팅 테이블을 통해 해당 명령을 수행함.
5. 서버는 수행한 명령에 대한 결과코드 를 전송함

보안이 고려된 창고 상태관리 시스템



보안이 고려된 입출고 흐름도



팔

펠렛

참고문헌

- [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, 이윤덕, "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 Ubiqutious 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.