碩 士 學 位 論 文

저가형 RFID를 위한 최소한의 연산을 사용한 인증 프로토콜

高 麗 大 學 校 大 學 院

情 報 保 護 大 學 院

崔 東 熙

2004 年 7 月 日

李 東 勳 敎 授 指 導

碩 士 學 位 論 文

저가형 RFID를 위한 최소한의 연산을 사용한 인증 프로토콜

An Authentication Protocol using minimal computation for Low-cost RFID

이 論文을 工學碩士學位 論文으로 提出함

2004 年 7 月 日

高 麗 大 學 校

情 報 保 護 大 學 院

崔 東 熙

Copyright ⓒ Korea Univ. Library All Right Reserved.

崔東熙의 工學 碩士學位 論文
審査를 完了함

年 月 日

委員長 李 東 勳 印

委 員 李 玉 淵 印

委 員 林 鍾 仁 印

Copyright ⓒ Korea Univ. Library All Right Reserved.

요 약

우리에게 유비쿼터스 컴퓨팅 환경이 제공되면 우리가 느끼지 못할 정도로 다양한 서비스가 제공될 것이다. 스마트 태그로 불려지는 RFID기술은 가장 빨리 유비쿼터스 컴퓨팅 환경을 실현할 기술로 주목받고 있다. 무선 주파수 인식 (Radio Frequency Identification: RFID) 기술은 바코드 시스템과 마그네틱 카드시스템을 대체할 새로운 기술이다. RFID 태그는 주변 리더기의 요청에 의해 자신의 식별정보를 알려주는 작고 값싼 칩이다. 또한 저가형 RFID(Low-Cost RFID)가 본격적으로 사용하게 되는 수년 내에 개당 5센트 이하로 가격이 떨어지게 되어 보편적으로 사용될 것이다. 그 결과 보다 다양한 서비스가 우리에게 제공될 것이 예상된다. 하지만 다양한 서비스의 제공은 우리가 느끼지 못하는 사이 네트워크를 통해 수많은 개인정보가 떠다는 뜻이다. 그러나 저가형 RFID 태그는 계산능력이 부족하고 간단한 대칭키 연산(Symmetric-key Cryptographic Operation)조차도 불가능하다. 결국 근본적으로 보안에 취약하다. 그러나 본 논문에서는 RFID에서도 구현 가능한 최소한의 연산과 작은 재사용(rewritable) 메모리를 사용하여 프라이버시(privacy)의 보호와 인증이 가능 할 수 있도록 고려하였다. 또한 보다 현실적인 모델을 제시하였으며 RFID태그의 도청을 막음으로써 익명성을 제공하여 프라이버시를 보호하고, 몇 가지 능동적 공격 모델에 대해 안전한 프로토콜을 제안하였다.

Copyright ⓒ Korea Univ. Library All Right Reserved.

목 차

Copyright © Korea Univ. Library All Right Reserved.

Copyright ⓒ Korea Univ. Library All Right Reserved.

그림 목차

Copyright ⓒ Korea Univ. Library All Right Reserved.

표 목차

Copyright ⓒ Korea Univ. Library All Right Reserved.

I. 서론

1. 배경

“Ubiquitous(유비쿼터스)”라는 용어는 이제 먼 미래의 공상이 아니다. 정부의 USN 기본 계획에 따르면 앞으로 수년 내에 우리에게 다가올 것이다[1]. 우리에게 유비쿼터스 컴퓨팅 시대를 열어줄 첫 번째 도구로 무선 주파수 인식 (Radio Frequency Identification: RFID) 기술이 자주 거론되고 있다. RFID는 바코드를 대체할 새로운 저비용의 무선인식 메모리 태그이다. RFID는 짧은 거리에서 시리얼 번호나 고정된 인식번호(static identifier)를 전달 할 수 있는 마이크로 칩이다. 수동형 RFID는 저가형으로 주로 제작되며 리더기에 의해 질의(query)와 전원(power)을 받아서 작동되며 여러 분야에 고루 적용 될 수 있다. RFID 태그의 사용은 산업전반에서 특히 물류나 유통 분야에 있어 혁신적인 발전을 이룩할 것으로 기대되고 있다[2]. 그러나, 산업 전반에 걸 쳐 다양한 서비스를 제고하게 된다는 것은 소비자의 개인정보들이 어느 곳에나 존재한다는 것 자체가 바로 잠재적인 프라이버시 침해의 소지가 있다. 재고관리, 반품관리, 절도나 모조품 예방 등에 유용한 RFID태그의 사용은 반대로 고객에 대한 신용정보나 구매유형 등 프라이버시가 침해당하는 것이다. 앞으로 더더욱 급속히 발전할 무선이동통신 관련 기술의 발달로 RFID태그의 위치정보와 함께 물류, 거래, 보안 관련 정보를 이용한 서비스는 더더욱 확대될 것이다. 그러나 이러한 서비스의 확대 속에 개인의 사생활이나 회사의 기밀에 대한 프라이버시의 침해가 심각하게 우려된다. 실제로 이러한 우려를 베네통의 경우를 예로 들어 알 수 있다[3].

2.유비쿼터스(Ubiquitous)와 RFID

유비쿼터스는 ‘어느 곳에나 존재한다.’는 의미를 가지고 1988년 우리에게 소개되었다[4]. 미국의 Mark Weiser가 처음 제안하였으며 앞으로 우리의 기술이 고도로 발달된 미래 사회를 지칭하는 말이기도 하다. 현재 우리 사회는 컴퓨터를 다룰 줄 아는 사람만이 정보의 바다를 향유 할 수 있지만 유비쿼터스 컴퓨팅의 세상에서는 우리는 일상생활에서 컴퓨터를 사용하는지도 인식하지 못하는 상태

Copyright ⓒ Korea Univ. Library All Right Reserved.

에서 수많은 컴퓨터가 연결되어 우리에게 서비스를 제공하는 인간 친화적이고 사용하기 쉬운 컴퓨터가 제공될 것이다. Mark Weiser는 유비쿼터스 컴퓨팅에 대해 다음의 4가지 판단기준을 제시하였다.[5]

1) 네트워크에 연결되지 않으면 유비쿼터스 컴퓨팅이 아니다.

2) 인간화된 인터페이스로써 눈에 띄지 말아야 한다.

3) 가상공간이 아닌 현실 세계의 어디서나 컴퓨터에 접근이 가능해야 한다.

4) 사용자 상황(장소, 장치, 시간, 온도, 날씨)에 따라 서비스가 변화되어야 한다.

언제나 어디서나 존재 한다는 의미를 가지고 위의 4가지 조건을 만족시키기 위해서는 네트워크와 통신 할 수 있는 단말 노드들이 우리의 주의에 편재(偏在)해 있어야 한다. 이런 세상을 열어줄 것으로 가장 주목받고 있는 기술이 바로 RFID이다[6].

무선 주파수 인식 (Radio Frequency Identification: RFID) 기술은 바코드 시스템과 마그네틱카드 시스템을 대체할 새로운 기술이다. 여러 가지 서비스, 구매, 유통, 재고 관리와 제조 및 자재 유통 등 RFID는 여러 가지 산업 전반에 걸쳐 바코드 혁명 이후 가장 혁신적인 변화를 가져올 것이다.[7]

RFID는 짧은 거리에서 시리얼 번호나 고정된 인식번호(static identifier)를 전달 할 수 있는 마이크로 칩이다. 수동형 RFID는 저가형으로 주로 제작되며 리더기에 의해 질의(query)와 전원(power)을 받아서 작동되며 여러 분야에 고루 적용될 수 있다.

앞으로 10년 안에 개당 5센트 이하 이면서 0.4cm*0.4cm의 크기를 가지며 종이에 프린트도 가능할 정도로 기술이 발전하여 상업적으로 이용 가능 할 것이다[13,14]. 이렇듯 기술의 발전이 가격 면에서나 크기 면에서도 급격한 발전을 이룩하게 되면 RFID의 사용 분야는 이루 말할 수 없을 정도로 그 범위를 넓혀 갈 것이다. 결국 RFID 태그는 바코드를 대체하여 어느 곳에나 존재하게 될 것이다. 이러한 변화는 설비와 소비재 등의 RFID가 들어간 물품들이 보다 스마트하고 지능적으로 변할 것이다.

Copyright ⓒ Korea Univ. Library All Right Reserved.

그러나, 소비자의 개인정보들이 어느 곳에나 존재한다는 것은 잠재적인 프라이버시의 침해 소지가 있다[15]. RFID 태그가 가진 정보를 누구에게나 알려준다는 것에서 유용할 수 있지만 반대로 누구나 RFID 태그를 읽을 수 있다는 점 때문에 물건을 운반하는 사람들에 의해 배송경로가 추적당할 수 있는 문제가 있다. 또한 베네통의 경우를 보면 사용자들은 자신들의 개인정보가 임의로 읽혀지는 것을 싫어한다[3]. 결국 정책적인 요인도 중요한 이슈가 된다. RFID태그의 사용은 많은 이점을 주지만 그만큼 그에 반하는 프라이버시의 문제가 존재하기 때문이다.

이러한 프라이버시의 문제는 어떤 리더기라도 RFID 태그의 정보를 읽을 수 있고, RFID 태그는 누가 질의(query)를 하건 자신의 정보를 알려준다는데 문제가 있다. 결국 태그와 리더기 사이의 프라이버시의 문제는 구조적으로 문제가 있으며 이는 태그와 리더기 사이에 인증을 통해 익명성을 제공함으로써 해결 될 수 있다.

RFID는 이미 수년 전에 개발되었지만 지난 몇 년간 저장 공간, 가격이나 기능면에서 빠르게 발전해 왔다. 그 결과 기본적인 연산(operation)이 가능해졌으며, 아직까지 적용되고 있는 무어의 법칙에 의하면 수년 내에 현재는 불가능해 보이는 암호학적 연산능력을 가진 개당 5센트 이하의 저가형 RFID 태그가 개발 될 것이다.

3.본 논문의 결과

저가형 RFID 태그는 계산능력이 부족하고 간단한 대칭키 연산(Symmetric key Cryptographic Operation) 조차 불가능하다. 결국 근본적으로 완벽한 보안요구사항을 만족시킬 수 없는 취약한 요소를 가지고 있다고 할 수 있다. 그러나 본 논문에서는 저가형 RFID에서도 구현 가능한 최소한의 연산과 약간의 재사용(rewritable) 메모리를 사용하여 사용자 프라이버시(privacy)의 보호가 가능하도록 고려하였다. RFID태그의 도청을 막고 인증함으로써 익명성을 제공하여 프라이버시를 보호하고, 제안한 능동적 공격 모델에 대해 안전하며 기존의 모델보다 현실적인 모델을 제안하였다. 또한 프로토콜의 안정성도 증가 시켰으며 수동적

Copyright ⓒ Korea Univ. Library All Right Reserved.

공격뿐만이 아니라 제안한 능동형 공격에 대해서도 안전한 프로토콜을 구성하였다.

II. RFID 시스템

1.RFID의 개요

RFID는 RF(Radio Frequency)를 이용해 트랜스폰더(Transponder: RFID태그)와 트랜시버(Transceiver: 리더기)가 서로 정보를 주고받는 방식이다. 예를 들어 태그가 붙어있는 상품을 골라 밖으로 나가려하면 입구에 설치된 리더기가 상품의 정보를 읽어 리더기와 연결된 애플리케이션(Application)이 상품을 구매한 사용자의 신용카드로 자동 결제하는 경우를 예로 들 수가 있다. 결국 RFID 태그의 정보를 이용하여 결재해야 하는데 이는 RFID 태그에 메모리칩이 내장되어있어 태그의 정보를 읽기/쓰기(Read/Write)함으로써 가능해 진다.RFID 태그의 종류는 크게 능동형 태그와 수동형 태그로 나눌 수 있으며, [표1]에 나와 있다[8].

[표 1] RFID 태그 종류 및 특징.

	특징
수동형 태그	● 리더의 유도전류에 의해서 전원을 공급 ● 간단한 구조 ● 일반적으로 읽기전용 태그로 사용 ● 소형경량 ● 비용 저렴 ● 동작수명이 길다 ● 단거리 전송(인식) ● 데이터전송시간이 비제한적 ● 물류관리, 전자 상거래, 교통 분야, 전자물체감시(EAS) 시스템 에 응용
능동형 태그	● 태그 내부에 포함된 전원 또는 전지 사용 ● 보통 읽기/쓰기 형으로 사용 ● 장거리 전송(인식) ● 데이터 전송 시간이 제한적 ● 배터리에 의한 가격상승 ● 토목・건축분야, 의료분야, 레저 활동, 시설물 ● 수동형에 비해 고가의 비용 ● 수동형에 비해 센서 네트워크 같은 다양한 응용가능

Copyright © Korea Univ. Library All Right Reserved.

2.RFID 시스템의 구성[7,9,10]

RFID 시스템은 다음의 세가지 컴포넌트로 구성된다.

- **RFID 태그 또는 트랜스폰더(transponder)** : 식별정보를 가지고 다니며 리더기의 요청에 응답하여 정보를 준다..
- **RFID 태그 리더 또는 트랜시버(transceiver)** : 태그에 정보를 요청하며 태그에 데이터의 읽기/쓰기를 진행한다.
- **데이터베이스 (Data Base)** : 태그의 관련 정보를 저장하고 가공한다.

가. RFID 태그(Transponder)

RFID 태그는 일반적으로 밧데리의 내장유무에 따라 능동형 태그(Active Tag)와 수동형 태그(Passive Tag)로 나뉜다. 태그의 구조는 보통 수 미리미터(mm)에서 10cm반경의 감지거리를 갖는 디스크형태가 보통 사용되며 유리 트랜스폰더, 플라스틱 하우징 된 트랜스폰더, ISO69873 도구 손잡이용 트랜스폰더, 열쇠 고리 형 트랜스폰더, 스마트 라벨 등 태그의 사용 목적과 용도에 따라 형태가 다양하다.

Auto-ID 센터에서는 태그의 기능에 따라 [표2]와같이 다음의 4가지 클래스로 구분 지었다[11,12]

1) 클래스 0: 가장 기본적인 태그로 단지 EAS(electronic article surveillance: 개체식별기능)만 제공한다. 태그마다 유일한 식별정보를 가지는 것이 아니고 도서관이나 레코드점에서 상품의 품목을 알려주는데 주로 사용되고 도난방지 태그로도 사용된다. 아마 대부분 “Chipless”로 사용되고 로직을 포함하고 있지 않다.

2) 클래스 1: 태그마다 유일한 식별 코드를 가지고 있다. 읽기전용(read-only)이던지 한번만 쓰기가능(write-once/read-many: WROM)메모리를 가지고 있다. 일반적으로 수동형 태그가 주로 쓰이며, 준-수동형(semi-passive)이나 능동형(active)형도 사용 된다.

Copyright ⓒ Korea Univ. Library All Right Reserved.

3) 클래스 2: 읽기/쓰기(read/write)가 가능한 메모리를 가지고 있다. 그렇기 때문에 재사용이 가능하다. 일반적으로 수동형 태그가 주로 쓰이며, 준-수동형(semi-passive)이나 능동형(active)도 사용된다. 본 논문에서 주로 다루게 될 태그이다.

4) 클래스 3: 주변의 센서와 함께 붙어있다. 그래서 수동형 태그는 사용될 수 없으며 온도측정이나 속도, 방사능 등을 측정한 수치를 저장 할 수 있다. 센서기술과 결합하여 비-메모리(memoryless) 센서를 사용하는 것보다 훨씬 많은 분야에 활용 할 수 있다.

5) 클래스 4: ad-hoc 네트워크에서 다른 태그와 통신이 가능하다. 능동형(active) 태그가 사용되며 "smart-dust"라 불리는 유비쿼터스 컴퓨팅(Ubiquitous computing) 환경의 범주에 들어간다[19].

[표 2] 태그의 클래스별 기능 명세

클래스	태그 이름	메모리 종류	전원 공급형태	비고
0	도난 방지 태그	없다	수동형	물품 감시
1	EPC 태그	Read-Only	모든 종류	ID 확인 전용
2	EPC 태그	Read-Write	모든 종류	데이터 로깅
3	센서 태그	Read-Write	semi-passive /능동형	환경 센서
4	스마트 더스트	Read-Write	능동형	Ad-hoc 네트워크

나. 리더(transceiver)

RFID 리더는 RF를 통해 데이터를 전송할 뿐만 아니라, 수동형 태그에 RF 파장을 이용해 적은양의 에너지를 공급하여 태그를 활성화시키고 태그와 애플리케이션 사이의 데이터를 전송하는 역할을 한다. 리더기는 RFID에 비해 많은 연산능력과 메모리를 가지고 있어서 암호학적 연산의 수행도 가능하다. 데이터베이스(back-end database)와 안전한 채널로 태그와 통신을 하던지 서비스에 필요한 정보를 마스터-슬레이브(master-slave) 입장에서 주고받는다. 일반적으로 읽기(read) 기능만을 수행하며 쓰기(write) 기능을 수행하는

Copyright ⓒ Korea Univ. Library All Right Reserved.

리더기는 Interrogator라 부른다.

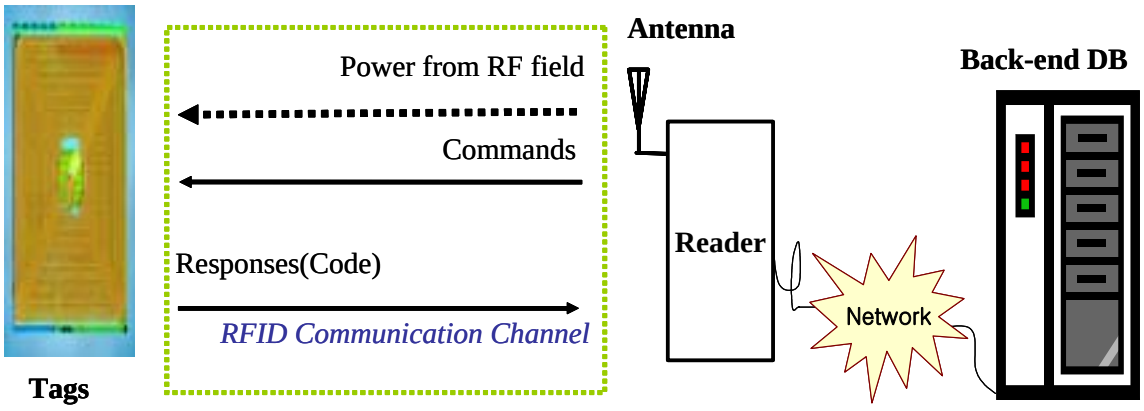
다. 애플리케이션 혹은 데이터베이스

(Application or Back-end database)

애플리케이션 혹은 데이터베이스라고 불리며, 리더기가 태그로부터 읽은 정보를 데이터베이스로 보내오면 데이터베이스는 태그정보를 분석하여 상품에 대한 정보를 얻던지, 태그의 위치를 추적하던지 아니면 키 관리 같은 인증을 한다든지 하는 등 적당한 서비스를 행한다. 때때로 RFID 시스템을 분석할 때 리더기와 데이터베이스를 하나로 보는 경우도 있으나, 태그는 리더기와 데이터베이스 사이에서 신뢰할 수 없다고 취급하는 경우가 보다 옳을 것이다. 현재는 구현된 예를 보면 데이터베이스가 한개만 존재하는 경우가 더 많으며 태그의 상품정보를 표시하거나 사용되고 있고 태그가 정당한 태그인지를 확인 하는 용도로 데이터베이스가 사용되는 경우가 많다. 데이터베이스는 난수로 구성된 ID를 가지고 있어서 ID와 실제 태그를 가리키는 값과 서로 매칭(matching)시켜주는 역할도 한다.

3. RFID 시스템의 작동

[그림 1] RFID 시스템 구성도



RFID시스템은 태그와 리더 그리고 태그로부터 읽어온 데이터를 처리할 수 있

Copyright © Korea Univ. Library All Right Reserved.

는 애플리케이션으로 구성된다. 태그와 리더기 사이의 RF통신을 통해서 읽기/쓰기 작업이 이루어진다. 처음 리더기가 태그에게 전원을 공급하면서 통신을 시도하면 리더기는 마스터가 되고 태그는 슬레이브가 되어 통신을 시작하게 된다. 마스터의 질의에 대해 슬레이브는 응답(response)하며 태그가 활성화되면 인증과정을 수행할 수 있다.

III.RFID와 프라이버시

1. RFID와 프라이버시(privacy)

저가의 RFID 태그 사용은 산업전반에서 특히 물류나 유통 분야에 있어 혁신적인 발전을 이룩할 것으로 기대되고 있다. 그러나, 소비자의 개인정보들이 어느 곳에나 존재한다는 것 자체가 바로 잠재적인 프라이버시 침해의 소지가 있는 뜻으로 받아들일 수 있다[13]. 재고관리, 반품관리, 절도나 모조품 예방 등에 유용한 RFID태그의 사용은 반대로 고객에 대한 신용정보나 구매유형 등 프라이버시 또한 노출 된다는 점을 지적 할 수 있다. 앞으로 더욱 급속히 발전할 무선이동통신 관련 기술의 발달로 RFID태그의 위치정보와 함께 물류, 거래, 보안 관련 정보를 이용한 서비스는 더더욱 확대될 것이 뻔하다. 그러나 이러한 서비스의 확대 속에 개인의사생활이나 나 회사의 정보들에 대한 프라이버시의 침해야 심각하게 우려된다. 실제로 이러한 우려를 베네통의 경우를 예로 들어 알 수 있다[3]. RFID의 사용자들은 자신들의 개인정보가 임의로 읽히는 것을 싫어하기 때문이다.

그러면 구체적인 프라이버시 침해요인에 대해 알아보겠다[14].

가. RFID 태그를 숨겨 놓을 수 있다..

RFID태그는 사용자가 모르게 사용자의 물건에 내장 될 수 있으며 RF는 지갑이나 쇼핑백, 서류 가방 등의 비금속 물체 속에서 자유롭게 주변의 리더기와 통신할 수 있다.

나. 오직 태그 자신만이 갖는 식별번호를 부여 받는다.

현재 연구 되고 있는 EPC코드 등을 통해 지구상 모든 물체 중 유일한 ID를

Copyright ⓒ Korea Univ. Library All Right Reserved.

부여받음으로써, 이 ID만 알면 물건의 소유주나 위치를 알아낼 수 있는 정보가 생기게 되어 구매자나 소유자를 추적 할 수 있게 된다.

다. 대량의 데이터 축적이 가능하다.

RFID 태그의 보편적인 사용은 대량의 태그별 정보를 저장하고 있어야 한다. 이러한 정보의 축적은 프라이버시 침해의 원인을 제공 할 수 있다.

라. RFID리더기를 숨겨 놓을 수 있다.

RFID시스템은 유비쿼터스의 관점에서 볼 때 우리의 생활에 눈에 띄지 않게 될 것이다. 리더기가 우리 눈에 보이지 않게 되면 누구나 태그의 정보를 읽을 수 있게 된다. 리더기는 바닥의 타일에 들어갈 수 있고, 카펫의 매트 속에 넣을 수 있고 또한 문고리에 숨길 수도 있다는 것이 이미 실험을 통해 밝혀졌다.

마. 개인의 추적이 가능하다.

개인의 신원이 유일한 식별 번호와 연결되기 때문에 누구나 읽을 수 있는 식별번호를 통해 개인의 위치를 추적 할 수 있다. 예를 들어 신발에 심어진 태그는 미아방지에 효과적일 수 있지만 반대로 신발을 신고 있는 사람을 추적할 수 있는 도구로 사용되어질 수 있다. 심지어 물품의 정보가 일반적인 것일 지라도 사람들이 신고 이동하는 그 물품을 추적함으로써 사용자가 정치적 집회에 참석했는지 여부를 알 수 있다.

위와 같은 소비자의 프라이버시 침해에 대한 우려에 대해 RFID를 도입하려는 사람들은 여러 가지 RFID의 한계를 설명함으로써 사용자들이 거론하는 프라이버시 문제를 해결할 수 있다고 한다. 그러나 이는 RFID가 기잔 근본적인 문제점들을 해결하는 것이 아니다. 결국 RFID와 리더기가 통신하는 내용은 무선랜(Wireless LAN: [15],[16])의 문제점과 같이 RF를 통해 전달되는 모든 내용은 도청 가능하다고 보아야 안전한 프로토콜을 제시 할 수 있을 것이다.

RFID 태그와 리더기가 통신 하는 내용이 도청 가능하기 때문에 태그의 유일한 ID는 적당한 리더기만 가지면 누구나 알 수 있다. 이렇게 되면 RF를 이용한 통신 상황에서 안전한 프로토콜을 통한 인증의 필요성이 대두 된다. 그러면서도 RFID태그가 가진 비좁은 메모리와 기본적인 암호학적 연산도 부족한 환경적 요

Copyright ⓒ Korea Univ. Library All Right Reserved.

인을 극복하고 태그의 인증을 성공적으로 해내야 하는 힘든 문제가 남게 된다.

2. 프라이버시의 보호

RFID에서 프라이버시의 노출 문제를 해결하려는 많은 방법이 제시되었다. 상품을 사고 계산대를 거쳐 갈 경우 “KILL”명령을 내림으로써 태그를 영원히 못쓰게 하는 방법이 사용 된다[17]. 이러한 방법은 RFID 프라이버시의 문제를 해결할 수 있는 방법으로 미국이나 일본에서 법제화하기 위해 추진 중에 있으며, 우리나라 에서도 프라이버시를 보호하기 위한 정책적인 연구를 수행중이다. 2004년 2월 미국 캘리포니아 주 상원위원 Debra Bowen은 RFID 기술 상용화와 관련한 소비자 생활 보호 등을 주장한 법안 Senate Bill을 제안하였다[28]. 일본 총무성에서는 소매점에서 결재 후 RFID태그를 떼어버릴 것을 권장하고 있다. 그러나 이와 같은 경우는 RFID태그의 초창기에나 사용될 수 있는 모델이며 앞으로 생겨날 수많은 RFID 응용 서비스에는 적합하지 않다. RFID태그는 활성화된 상태로 거리를 활보하고, 리더기 들은 이들을 읽어서 서비스를 제공 할 수 있도록 해야 되기 때문이다. 결국 RFID에서 근본적으로 프라이버시를 보호하기위한 방법이 필요하다는데 인식을 같이 하게 되었다.

프라이버시를 보호하기 위해 익명성(anonymity)은 반드시 제공되어야 할 조건이다. 익명성은 사용자가 자신의 ID(Identity)를 드러내지 않고 서비스나 리소스를 사용하는 것을 보장하는 것이다[23].

태그와 리더기의 통신정보는 무선을 통하기 때문에 약간의 장비만 있으면 누구나 엿들을 수 있다. 태그가 통신 할 때의 정보는 인증의 주체들을 빼고는 아무도 알아서는 안 된다. 결국 통신하는 내용을 보고는 사용자의 ID관련 정보를 알 수 없어야 된다는 뜻이다. 이와 같은 성질을 제공하기 위해 인증 및 암호화가 수행되어져야 한다. 수동형/저가형 RFID환경에서는 메모리만 들어있는 태그의 환경에서 암호학적 연산이 불가능하다. 이런 문제를 해결하기 위해 나온 방법이 스마트 RFID 태그 (Smart RFID-tag)를 이용하는 방법이다. 스마트 RFID는 RFID 태그에 게이트(gate)를 심어서 암호학적인 방법(Cryptographic Method)을 이용하는 것이다. 그러나 여기서도 고비용의 연산을 하는 것이 현재로서는 비용측면에

Copyright © Korea Univ. Library All Right Reserved.

서 볼 때 실현되기 힘들다.

3. 프라이버시 요구사항

현재 CASPIAN[14]에서 태그 정보의 유출과 태그의 추적(tracking) 행위에 대한 문제를 가장 크게 지적하고 있다. 또한 무선 랜에서 가능한 Man-In-Middle 공격, 재생공격(Reply attack), 스푸핑(spooping) 공격과 서비스 거부 공격(DoS)이 가능 하다[10,16].

RFID의 프라이버시를 보호하기 위한 요구사항은 다음과 같다[30,31].

- 기밀성(Confidentiality)

기밀성은 수동적 공격으로부터 데이터를 보호하는 것이다. 정당한 권한을 가진 사용자만이 데이터의 내용을 확인 할 수 있어야 한다. 무선으로 주고받는 정보는 도청 가능하다. 비록 도청 가능하다 하더라도 데이터의 내용은 알 수 없어야 한다.

- 무결성(Integrity)

무결성은 수신자 입장에서 송신자가 보낸 메시지가 제 삼자에 의해서 생성된 것인지 또는 변조된 것인지에 대해서 확인 가능해야 한다는 성질이다. 이 성질은 넓은 의미에서 통신상의 잡음에 의한 변조도 포함 가능하다. RFID 환경에서 메시지를 주고받는 것은 누구나 도청 가능하기 때문에 메시지를 변조하여 태그와 통신을 시도 할 수 있다. 그러므로 인가 받은 개체는 RFID가 전송하는 데이터가 변조 되었는지를 확인 할 수 있어야 한다.

- 익명성(Anonymity)

익명성은 이용자가 자신의 신원을 노출하지 않고 어떠한 자원이나 서비스를 이용할 수 있도록 하는 성질이다. 익명성은 송신하는 측의 익명성과 수신하는 측의 익명성 그리고 송수신자 사이의 링크(link)가 생기지 않게 하는 세가지로 구분한다. 무선 네트워크는 이동성을 제공해야 한다. 그러므로 태그의 위치 정보 또한 추적할 수 없어야 한다. RFID 환경에서는 태그가 태그의 정보를 무선으로 주고받으므로 항상 도청이 가능하다. 그래서 RFID 환경에서의 기밀성은 RFID

Copyright © Korea Univ. Library All Right Reserved.

태그에서 전송하는 데이터를 보고 인가받지 않은 사용자(리더)는 전송된 데이터에서 태그의 중요한 정보를 얻을 수 없어야 한다.

IV. RFID의 인증 프로토콜

처음 RFID를 개발 할 당시 RFID에서 프라이버시의 보호라는 측면 보다는 유용한 서비스의 제공에 초점을 맞춰 개발되었다. 그러나 다양하고 유용한 서비스의 제공은 반대로 소비자의 프라이버시의 침해소지가 있음이 드러나게 되었고, 처음에는 심각히 여기지 않았지만 서비스의 제공자보다 소비자들이 먼저 이의를 제기하고 집단적 행동(CASPIAN) 에 나서기 시작했다[14]. 서비스 제공자들은 프라이버시의 보호 방안을 제시 했으나 무두 충분한 프라이버시의 보호를 제공하지 못했다. 태그정보의 누출이 심각한 프라이버시의 침해가 되는 경우가 있음을 인정하고 이러한 경우가 생기지 않도록 익명성을 제공하게 되었다. 그 후 익명성 제공을 위해서는 인증의 주체들에게만 태그의 정보를 알려주는 기술이 필요 하다는 결론에 이르게 되었다. 암호화된 메시지를 통해 상호 인증을 함으로서 익명성을 제대로 제공 할 수 있게 되었다. 아래에 제시된 인증 방법은 비록 태그의 비용은 증가되었다는 단점이 있지만 보다 완벽한 익명성을 제공하기 위해서 필요한 어쩔 수 없는 선택이다.

인증용 태그 또한 처음에는 고정된 인증용 태그만 연구되다 도청, 복제 등의 위협요소가 존재함에 따라 태그가 ID 리스트를 가지고 하나씩 사용하는 방법이 연구 되었다. 그러나 이 방법 또한 리스트의 ID를 다 써버리면 재사용 된다는 점에서 문제점이 지적되었다. 결국 재사용 태그(Rewritable Tag)를 사용하여 태그의 ID를 업데이트 해주는 방법이 제시 되었다. 그러나 대칭키 연산이나 해쉬 연산을 사용한 인증은 아직까지 RFID의 비용과 구현적인 측면에서 볼 때 아직은 힘든 상황이다[10].

1.Broker-Tag 기법

Broker-Tag기법은 원래 태그의 충돌을 막기 위해 Tree-Walking Singulation 알고리즘을 확장 시킨 형태이다[10,24]. Tree-walking 알고리즘은 리더기의 한비트 질의(query)에 대해 돌아오는 한비트 응답(response)을 트리구조를 이용해 비

Copyright ⓒ Korea Univ. Library All Right Reserved.

교하는 방식으로 여러 개의 태그가 동시에 리더기와 통신할 때의 충돌 문제를 해결하는 방식이다. 여기서 태그의 구분은 태그마다 유일한 식별번호를 가지고 있기 때문에 가능하다[29]. Broker태그는 Tree-walking 기법을 이용하여 자신이 가진 비트의 반대 비트도 같이 보내 줌으로서 태그의 정보를 알려주지 않는 기법이다.

2.Re-encryption 기법

[24,26]에서 재-암호화(re-encryption)기법은 공개키 시스템으로 암호화된 태그 식별번호를 사용한 전자 화폐를 RFID 태그에 칩으로 만들어 집어넣어 프라이버시를 보호하는 방법을 제안하였다. 그 결과 태그마다 암호화된 정보가 매번 다른 값으로 재-암호화(re-encryption)되어 내보내지게 되어 unlinkability를 제공한다.

RFID의 여러 가지 제한된 연산환경 때문에 재-암호화(re-encryption) 연산은 외부의 에이전트(agent)가 해준다고 가정한다. 이 에이전트(Agent)는 은행과 소매점 사이에서 재-암호화(re-encryption)된 화폐들을 검증해준다.

이러한 프로토콜의 단점은 이러한 방법 자체가 자원을 많이 필요로 한다는 점이다(resource-intensive nature). 자원을 많이 필요로 한다는 것이 비용이 많이 든다는 의미를 가지고 있다. RFID태그가 재-암호화(re-encryption)를 할 수있는 공개키 연산이 불가능하고 현실적으로 구현하기 힘들 정도로 비용이 많이 든다. 또한 재-암호화(re-encryption)를 할 수 있는 에이전트(agent)들로 구성된 인프라가 구축되어야 하는 문제도 있다. 결국 재-암호화(re-encryption)를 하는데 따른 태그의 비용과 에이전트(agent)들로 구성된 인프라의 구축비용 문제로 인해 현실적으로 구축하기 힘들다.

Golle et al.[25]에 소비재에 부착할 수 있는 RFID의 프라이버시 보호 방안에 대한 자세한 설명과 함께 “universal re-encryption”을 제안 하였다. multiple public key를 사용하며, El Gamal Cryptosystem을 학장시키는 방식으로 공개키 교환(association)정보를 알지 못하고 재-암호화(re-encrypt)된 암호문을 이용하는 것이다. 그러나, Golle et al[25]의 스킴은 Juels과 Pappu[26]의 방법과 에이전트들로 구성된 인프라가 구성되어야 한다는 점에서 같은 문제점을 가지고 있다.

Copyright © Korea Univ. Library All Right Reserved.

3.Hash-Lock 기법

인증용 태그는 처음에 고정된 인증용 태그만 연구되다 도청, 복제 등의 위협요소가 존재함에 따라 태그가 ID 리스트를 가지고 하나씩 사용하는 방법이 연구되었다. 그러나 이 방법 또한 리스트의 ID를 모두 사용하면 ID가 재사용 된다는 점에서 문제점이 지적되었다. 결국 재사용 태그(Rewritable Tag)를 사용하여 태그의 ID를 업데이트 해주는 방법이 제시 되었다.

스마트 RFID 태그(Smart RFID-tag)와 암호학적인 방법을 이용하여 인증하는 방법으로 해쉬-락(Hash-Lock) 프로토콜이 제안되었다[10]. 이 프로토콜은 리더기의 질의(query)에 대해 태그는 ID를 해쉬 시킨 값을 응답(response)해주며 데이터베이스는 해쉬 값을 확인하고 리더기는 키와 ID를 받아서 키 값을 태그에게 주면 태그는 이 값을 확인하고 ID를 리더기에게 준다.

지금까지 암호학적 연산을 적용하지 않은 Broker-Tag를 제외하고는 Hash-Lock기법 , Re-encryption 기법, Hash-chain 기법과 같이 암호학적 기법을 사용하여 익명성을 제공하는 방법들에 대해 알아보았다. 이러한 프로토콜에서 사용된 공개키 연산이나 해쉬 연산을 사용한 인증은 아직까지 저가형 RFID가 가진 비용이나 구현가능성의 측면에서 볼 때 현재에 바로 적용하기 힘든 모델이다[10]. 현재에 바로 적용하기 힘들다는 문제를 해결하는 방법이 RSA security에서 제안되어 아래에 나와 있다.

4.Xor 기법

최근 RSA security에서 [18]을 제안하였다. Xor 연산을 이용하여 상호 인증을 수행하면서도 태그의 ID가 업데이트되는 프로토콜이다. Xor연산은 RFID에 적용가능한 연산(operation)으로 현실 세계에 바로 적용될 수 있는 모델을 제시한 것이다. 그러나 메모리의 양이나 리더기와 데이터베이스가 분리되지 않은 점과 모든 세션을 도청했을 경우 모든 정보가 드러난다는 점과 One-Time pad의 안전성에 기반 한 안전성 등이 아직은 해결해야 될 부분으로 남아있다. 이에 본 저자는

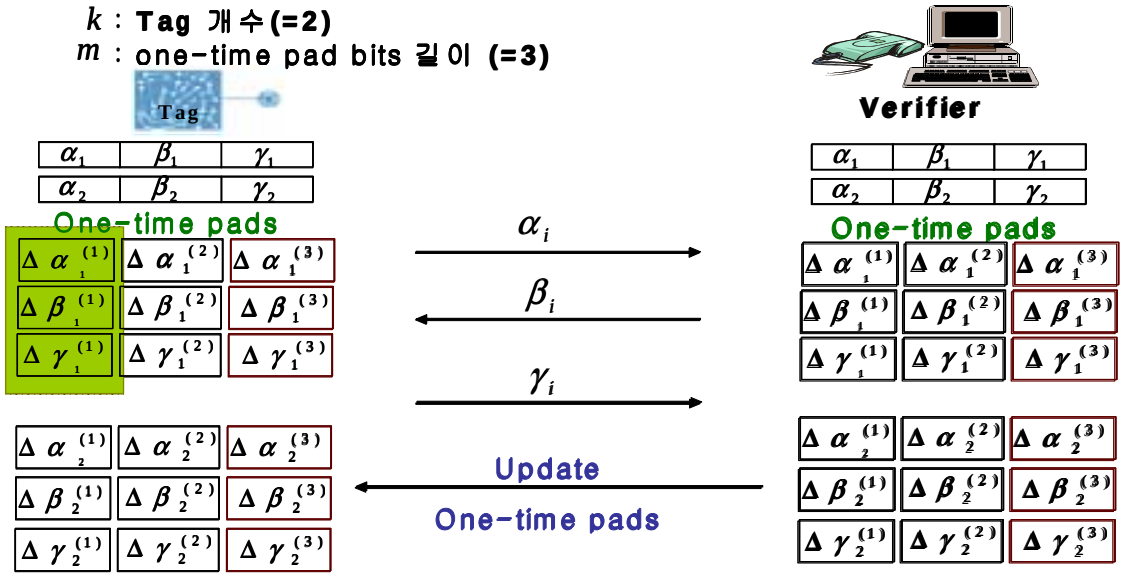
Copyright ⓒ Korea Univ. Library All Right Reserved.

이러한 문제점을 해결하고 보다 효율적으로 인증을 수행하는 프로토콜을 다음 장에 제시하였다.

● Ari Juels의 프로토콜[18]

스마트 RFID를 이용한 방법들이 제안되었으나 이러한 방법들은 모두 많은 연산과 메모리를 요구한다. 결국 RFID의 저비용(Low-cost) 태그를 만들 낼 수 없다. 결국 RFID 태그의 연산을 최소화한 한 인증 프로토콜 필요하게 되어 RSA security에서는 Xor연산과 재사용 태그 (Rewritable Tag)를 사용한 프로토콜을 제안 하였다[18].

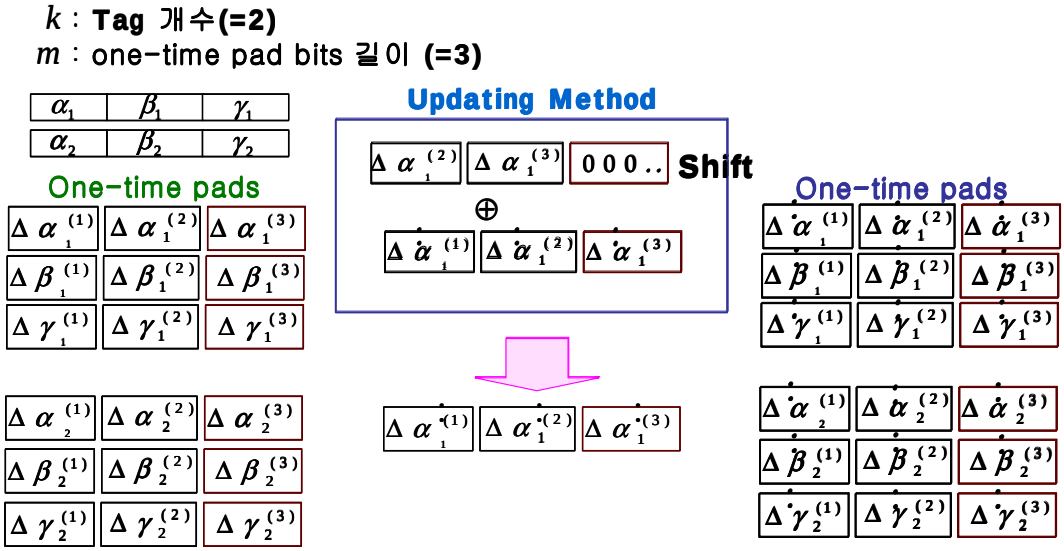
[그림 2] Ari Juels의 프로토콜 예제



[그림 2]에서 보는 바와 같이 제안된 프로토콜은 우선 태그가 가진 비밀 값 α를 verifier에게 보내면 verifier는 α를 보고 리스트에서 태그의 정보가 들어있는 테이블을 찾아 β를 응답(response)해 주고 태그는 γ를 verifier에게 응답 해주어 태그와 verifier사이에 상호 인증을 수행한다. 인증과정이 끝나면 verifier는 업데이트(update)테이블을 태그에게 보내어 업데이트한다[그림 3].

Copyright © Korea Univ. Library All Right Reserved.

[그림 3] Ari Juels의 업데이트 방법

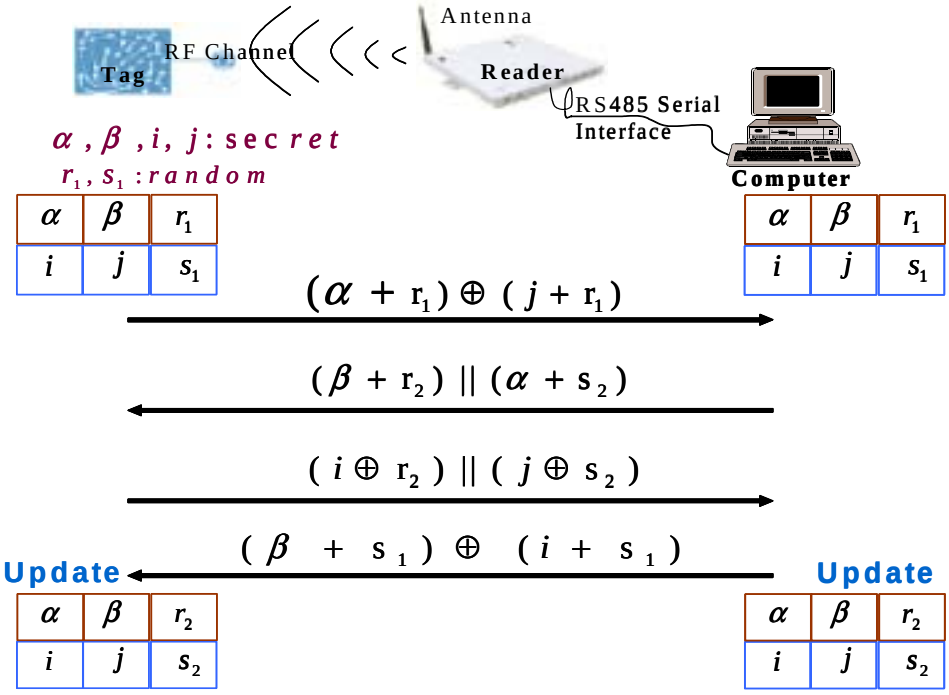


V. 프로토콜의 제안

저자가 제안한 프로토콜은 [18]에서와 같이 Xor연산만을 사용 하면서도 검증자(verifier)를 리더기와 데이터베이스로 구분하였다. 왜냐하면 [18]에서는 검증자가 One-time pad인 업데이트 테이블을 넘겨주는데 이는 실제로 리더기가 전달해 주기 때문이다. 데이터베이스는 인증서버(Authentication Server)의 역할을 함으로써 안전하다는 가정을 해도 무관하다. 그러나 데이터베이스와 떨어져서 많은 수가 존재하는 정당한 리더기는 악의적으로 변할 수도 있다. 누군가 리더기의 프로그램을 고칠 수도 있기 때문이다. 또한 리더기는 무선으로 데이터베이스와 통신할 가능성도 높다. 결국 태그가 주고받는 모든 정보는 누구나 엿들을 수 있다는 결론에 이르게 된다.

Copyright © Korea Univ. Library All Right Reserved.

[그림 4]보다 안전하고 효율적인 RFID 인증 프로토콜



1. 프로토콜 STEP

가) 처음 RFID태그를 만들 때 DB와 태그에 동일한 정보를 쓴다.

나) 태그가 리더기의 쿼리(query)와 전원을 받아 첫 번째 메시지를 만들어 리더기에 보낸다.

다) 리더기는 태그와 리더기 사이에서 메시지를 전달해 주는 역할을 한다.

DB는 태그가 보내온 값을 자신이 가지고 있는 테이블의 리스트와 비교하여 태그의 정보를 찾아낸 후 새로운 난수 r, s를 생성하여 [그림4]의 두 번째 메시지와 같이 보내준다.

라) 태그는 DB의 메시지를 받아 i,j와 함께 새로 받은 r, s를 섞어서 DB에 보낸다.

마) DB는 태그가 보내온 값을 확인하여 자신이 보낸 r, s이면 4번째 메시지를 보내고 틀리면 임의의 수를 보내어 잘못된 값으로 태그가

Copyright © Korea Univ. Library All Right Reserved.

업데이트하지 못하게 한다.

2. 공격에 대한 안전

제안한 프로토콜은 저가형/수동형/재사용 RFID태그에서도 상호 인증이 가능하도록 설계하였다. 인증(Mutual Authentication)이란 수신자가 받은 메시지가 송신자로부터 전송된 것인지를 확인할 수 있게 하고 도한 송수신자간의 신원을 확인할 수 있는 성질이다. 불법적인 사용자가 정당한 사용자로 위장함으로써 발생할 수 있는 문제점을 막을 수 있는 기법으로 암호학적 기법을 통해 제공될 수 있다. RFID시스템에서 인증되지 않은 태그와 데이터베이스나 리더기가 상대에게 인증 받으려는 시도를 행할 수 있다. 이때 태그와 데이터베이스는 정당한 상대인지 아닌지를 인증할 수 있다.

기밀성의 제공: 저자의 프로토콜은 새로운 난수와 비밀 값이 섞인 상태로 네트워크에 전달되기 때문에 도청을 하더라도 비밀 값을 알아낼 수 없다. 또한 모든 세션을 도청할 수 있더라도 그 정보를 가지고는 어떠한 비밀 정보도 알 수 없다.

무결성의 제공: 태그와 리더기 사이에서 혹을 리더기 일지라도 임의의 메시지를 추가 하거나 변조하더라도 인증을 통해 메시지가 변조되었는가를 알 수 있다.

익명성의 제공 : 이동하는 태그의 위치 정보는 인증서버 이외에는 알 수 없고 네트워크를 통해 돌아다니는 정보는 매번 다른 값이 전달되므로 태그의 위치를 추적 할 수 없다.

여기서 기밀성, 무결성과 익명성을 침해하려는 시도들에 대해 안전함을 예로 들어 보겠다.

1)기밀성

· 메시지 추출 시도 공격에 안전하다.

수동적 공격으로 아무런 정보를 얻어낼 수 없으므로 추후 세션에서 사용할 메

Copyright ⓒ Korea Univ. Library All Right Reserved.

시지를 추측해 낼 수 없다. 모든 통신에서 난수와 섞여있는 정보들의 내용을 알아내는 것은 불가능하다.

2)무결성

· 정당하지 못한 태그의 인증 시도 공격에 안전하다.

정당하지 못한 태그는 정당한 태그가 가진 정보에 난수를 섞은 세션의 첫번째 메시지를 만들어 낼 수 없다. 수동적 공격으로 ID나 난수를 알아낼 수 없기 때문에 태그는 오라클로부터 난수를 얻어내어 리더기에 인증을 요청 하는 수밖에 없는데 첫 번째와 세 번째 메시지를 모두 알아맞혀야 한다. 인증에 성공할 확률은 거의 없다.

· 정당하지 못한 리더기의 인증시도에 안전하다.

정당하지 못한 리더기가 인증에 성공한다면 태그에는 리더기가 임의로 만든 난수가 업데이트되기 때문에 태그가 나중에 정당한 리더기에게 인증을 받을 때 인증을 받을 수 없게 된다. 태그가 망가지게 되는 것이다. 정당한 리더기는 수동적 공격으로 아무런 정보도 얻지 못하기 때문에 태그에게 세션의 두 번째 메시지는 만들어 보낼 수 있어도, 4번째 메시지는 제대로만들 수 없기 때문에 공격이 불가능하다. 리더기의 공격에도 안전하므로 무선구간에서 리더기보다 강한 능력을 가진 공격자가 등장하지 않는 한 안전하다. 그런데 리더기보다 강력한 공격자는 실제로 존재하기 힘들다.

· 재사용 시도 공격에 안전하다.

메시지를 도청한 공격자는 자신이 모은 메시지의 내용은 모르더라도 이를 재사용함으로써 태그나 리더기에게 인증 받으려 할 수 있다. 그러나 항상 새로운 난수와 섞여서 전송되기 때문에 같은 값이 사용되는 경우는 없다. 그러므로 재사용 공격은 불가능하다.

· 메시지 추가시도 공격에 안전하다.

두 연산간의 결합법칙이 성립하지 않기 때문에 공격자가 메시지에 임의의 수

Copyright © Korea Univ. Library All Right Reserved.

를 집어넣는다 해도 인증하는 과정에서 정당한 값이 들어가지 않게 되어 인증에 실패하게 된다.

3)익명성

· 태그의 위치정보를 추적 할 수 없다.

매번 새로운 난수와 섞인 값이 네트워크를 떠다니게 되기 때문에 동일한 태그의 통신정보를 찾아 추적할 수 없다. 유비쿼터스의 세상에서 중요하게 요구 되는 성질이다.

4)메시지 차단 시도 공격에 안전하다.

RFID시스템에서 악의적인 공격자에 의해 메시지 차단 공격이 일어날 수 있다. 이는 태그에는 새로운 값으로 업데이트되지 않고 DB쪽에는 업데이트되 일이 생길 수 있기 때문이다. 그러나 DB쪽에서 로그데이터를 보관하고 있으므로 이를 이용하면 태그와 DB사이에 메시지 차단 공격이 일어났는지 알아낼 수 있고 태그가 정당하지 못한 값으로 업데이트된게 아니기 때문에 태그와 DB사이에 새로운 값으로의 업데이트가 가능하다.

저자의 프로토콜은 상호 인증을 해야만 하는 프로토콜이다. 인증이 끝나면 새로운 난수들을 업데이트한다. 혹시 태그는 업데이트를 행하지 않고 DB만 업데이트를 행하여 서로 다른 값을 가질 수 있는데 DB에서 로그 데이터에서 이전 값을 찾아 태그와 통신 할 수 있다. 또한 난수와 두 연산간의 결합법칙이 성립하지 않는 성질에 안전성이 달려있다.

3.프로토콜의 비교

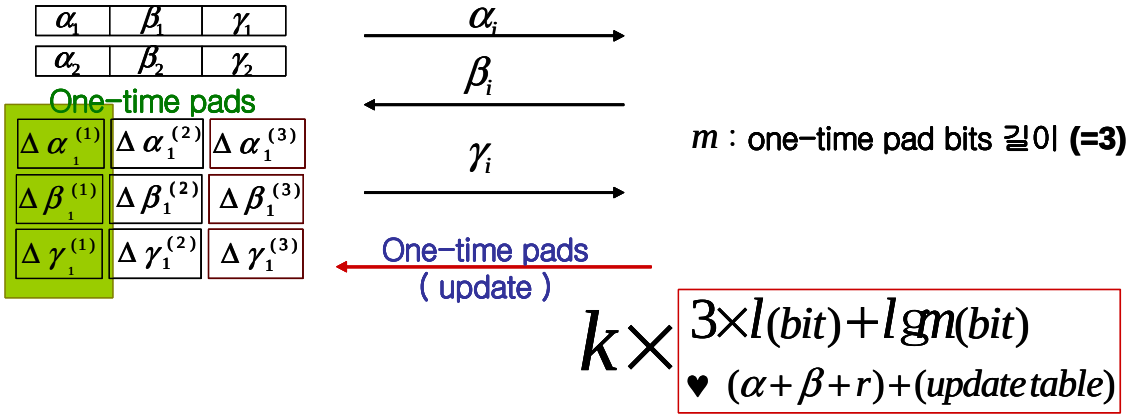
RFID 시스템에서 AES알고리즘을 사용한 암호화를 이용하는 것은 거의 불가능하다. 가능하다 하더라도 상업적으로 이용불가능하다. 왜냐하면 대칭키 암호를 사용하는 것보다 PRF(Pseudo Random Function)를 사용하는 것이 하드웨어로 구현하는 비용이 덜 드는데 아직까지 해쉬를 사용한 RFID조차도 만들기 힘들기

Copyright ⓒ Korea Univ. Library All Right Reserved.

때문이다[20]. 그래서 해쉬 함수를 이용해 PRF로 사용하려는 연구가 진행 중이다. 현재 RFID에 하드웨어로 구현할 때 20,000~30,000개의 게이트가 필요한 것으로 연구되어 있다[21,22]. 현재는 불가능 하지만 앞으로는 가능 할 수도 있다는 연구도 어느 정도 진행되어 있다[23,24]. 현재 200~ 2000개의 게이트정도는 RFID에서 구현가능하며 10,000클럭 사이클도 가능하다. Xor 연산은 현재 하드웨어로 만든 수 있는 정도의 능력이면 충분히 구현가능하다. 이렇게 RFID를 이용한 인증에서 Xor를 이용한 인증이 해쉬나 대칭키 연산을 이용하는 인증에 비해서 구조적으로 훨씬 실현 가능하다.

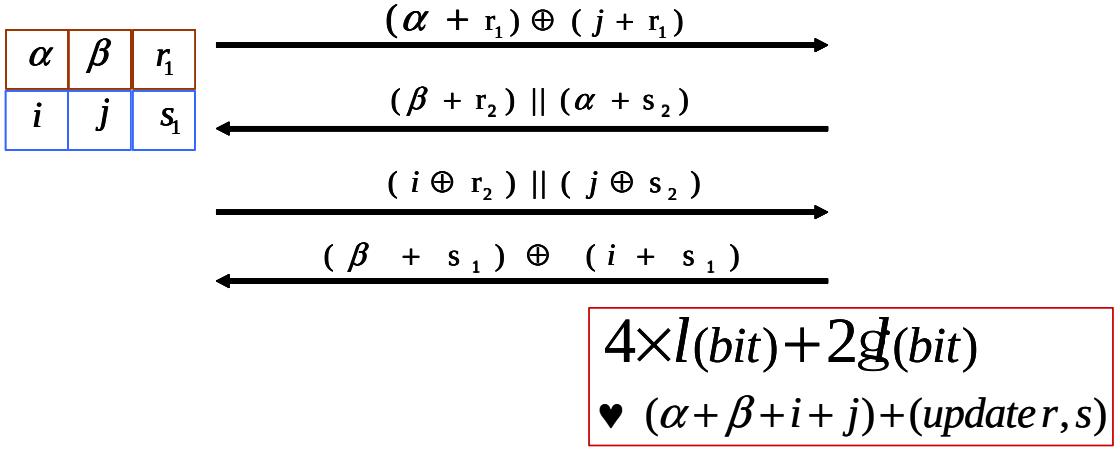
[그림 5]와 [그림 6] Xor 연산을 사용한 Ari Juels[18]의 방법은 저자가 제안한 방법에 비해 메시지의 수는 같으나 메모리나 전송양이 큰 차이를 보인다. RFID에서 하드웨어로 구현하기위해 필요한 게이트의 수만큼 중요한 것이 메모리의 양이다. 그러므로 저자가 제안한 프로토콜이 훨씬 효율적이라는 것을 알 수 있으며 상업적으로도 보다 유용하다.

[그림 5] Ari Juels의 프로토콜에서 필요한 메모리



Copyright © Korea Univ. Library All Right Reserved.

[그림 6] 제안한 프로토콜이 가지는 메모리



VI. 결론

RFID 시스템에 프라이버시를 제공하기위해 인증이 필요로 되는 때에 기존에 연구되던 대칭키 암호화 방식이라든가 해쉬를 이용한 인증방법이 아직은 현실적으로 구현하기 어렵다. RSA security에서 Xor를 이용한 새로운 방법의 인증 방법을 제안하였다. 저자는 같은 Xor를 이용하면서도 검증자(verifier)를 리더기와 DB로 분리하였으며 인증을 방해하려는 몇 가지 능동적 공격에 대해 안전하게 만들었으며 모든 세션을 볼 수 있어도 안전하도록 프로토콜을 제안 하였다.

저자가 제안한 프로토콜은 기존의 방식에 비해 안전하면서도 현실적인 모델에서 적은 메모리를 사용하는 프로토콜을 제안하였다. 이는 곧 다가올 유비쿼터스 시대에 대비할 수 있는 최소한의 암호학적 연산만을 사용한 인증이 될 것이다.

그러나, 아직은 취약한 형태의 능동적 공격이 존재하며 완벽한 forward security와 backward security를 제공하지 못한다. 그러나, 현대암호에서 말하는 완벽한 암호학적 안전성을 RFID에 요구한다는 것 자체가 문제가 있을 수 있기 때문에 어느 정도의 안전성을 제공해야 되는지에 대한 연구가 필요하다. RFID는 구조적으로 제공할 수 있는 보안적 요소가 지극히 제한적이기 때문이다. 그러나 저자가 제안한 프로토콜은 RFID분야뿐만이 아니라 제한된 연산능력을 가지면서도 인증을 제공해야 하는 다양한 환경의 네트워크에서 응용이 가능하다.

Copyright © Korea Univ. Library All Right Reserved.

참고 문헌

[1] 정보통신부,“U-센서 네트워크 구축" 기본계획(안)”, 2004.2

[2] 삼성경제연구소,“유비쿼터스 컴퓨팅: 비즈니스 모델과 전망”, 2003.12

[3] Benetton undecided on use of 'smart tags'. Associated Press , 2003.8

[4] http://www.ubicomp.com/weiser/

[5] 김완석,“마크웨이저가 말하는 ‘유비쿼터스 컴퓨팅’. ”,전자신문,2002.10.4

[6] 노무라종합연구소,,“유비쿼터스 네트워크와 시장 창조”,전자신문사,2003.3

[7] Klaus Finkenzeller, "RFID-Handbook“, 2nd edition, 영진닷컴, 2004.3

[8] 장재득,장문수,최송인, “무선 주파수 인식[RFID] 시스템 기술 분석”, 전자통신동향분석 제19권 제2호, 2004.4.

[9] "RFID(Radio Frequency Identification)동향”,전자부품연구원 동향분석,2004.2.

[10] Weis, S. et al,: Security and Privacy in Radio-Frequency Identification Devices, Massachusetts Institute of Technology, 2003.

[11] Auto-ID Center. http://www.autoidlabs.org.

[12] Auto-ID Center. Draft Protocol Specification for a Class 0 Radio Frequency Identification Tag, February 2003.

[13] Declan McCullagh,“ RFID tags: Big Brother in small packages”, www.news.com, 2003.1.

[14] http://www.nocards.org

[15] IEEE Standard 802.11, 1997.

[16] Arunesh. Mishra. "An Initial Security of the IEEE 802.1x Standard",University of Maryland, 2002.2

[17] S. E. Sarma, S. A. Weis, and D.W. Engels. Radio-frequency identification systems. In Burton S. Kaliski Jr., C¸ etin Kaya Ko¸c, and Christof Paar, editors, CHES '02, pages 454 - 469. Springer-Verlag, 2002. LNCS no. 2523

[18] Ari Juels,“Minimalist Cryptography for Low-Cost RFID Tags”, RSA Laboratories. 2003.

[19] J. M. Kahn, R. H. Katz, and K. S. J. Pister. Next Century Challenges: Mobile Networking for "Smart Dust". In MOBICOM, pages 271-278, 1999.

[20] Matthias Krause and Stefan Lucks. On the Minimal Hardware Complexity

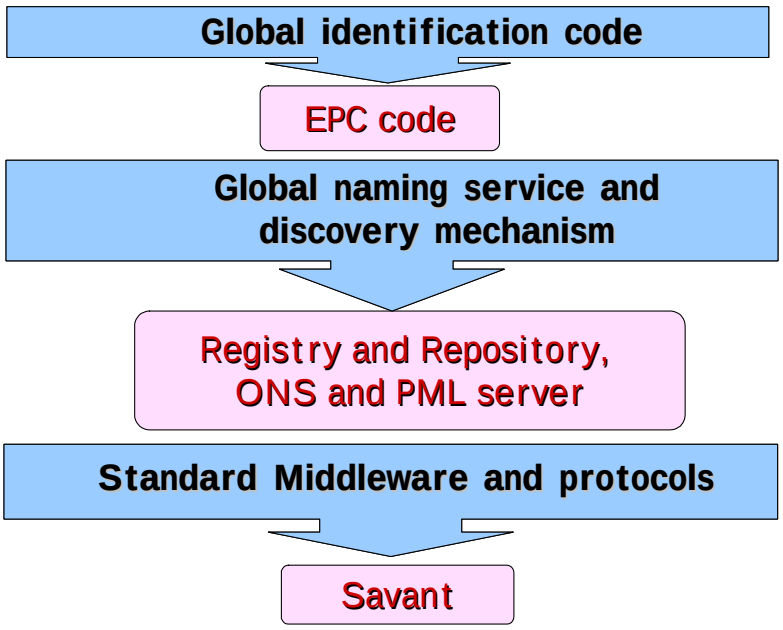
Copyright © Korea Univ. Library All Right Reserved.

of Pseudorandom Function Generators. In Theoretical Aspects of Computer Science, volume 2010,page 419-435.Lecture Notes in Computer Science,2001.
[21] Alma Technologies. SHA-1 Core. http://www.alma-tech.com.
[22] Bart Preneel. Analysis and Design of Cryptographic Hash Functions Based on Block Ciphers: A Synthetic Approch. in Advances in Crypotology-CRYPTO,LNCS, pages 368-378. Springer-Verlag,1994.
[23] Birgit Pfitzmann, Michael Waidner: Fail-stop Signatures and their Application to Byzantine Agreement; submitted for publication, Universität Karlsruhe 1990.
[24] Ari Juels "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy " CCS03 , ACM 2003
[25] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets, 2002. In submission.
[26] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In R. Wright, editor, Financial Cryptography '03. Springer-Verlag, 2003. To appear.
[28] 일본 총무성, 전자태그 고도활용을 향한 조사 -최종보고(안). 2004.3
[29] http://www.epcglobalinc.org/
[30] Birgit Pfitzmann and Andreas Pfitzmann, "How to Break the Direct RSA-Implementation of MIXes" EUROCRYPT 1989, 1990.
[31] 박창섭,"암호이론과 보안",大英社,1999.11.

Copyright © Korea Univ. Library All Right Reserved.

APPENDIX Auto-ID

다음의 그림과 같은 이유로 Auto-ID가 필요하게 되었다.



A. EPC 코드

・Electronic Product Code (EPC)라 불리며 Global Identification Code의 필요에 의해 생겨났다. 64비트와 96비트 방식이 있으며 각각의 태그마다 유일한 Identity가 주어진다. 이는 상품, 상자, 운반함, 위치, 화물 등에 적용될 수 있으며 활용 예는 수없이 많다. 수많은 활용범위에 맞게 다양한 방법의 Identity표현방식과 인코딩 방식이 제안되었다.

현재 EPCglobal에서는 V1.1 R1.23이 표준안으로 나와 있고 , EAN.UCC에 의해 제안되고 있다. 세 개의 계층으로 구성 되어있으며 EPC코드를 저장하는 Pure Identity 계층과 인코딩 계층이 있고 Physical 계층이 있다.

Pure Identity 계층은 다음의 세가지 요소로 구성된다.

가) Genaral Manager Number : Product의 이름이 들어가며 unique하다.

나) Object Class : 제품의 이름이나 타입에 관한 정보가 들어간다. Product가 결정하고 책임진다.

다) Serial Number : 동일 제품마다의 유일한 값을 구분하기 위해 사용된다.

다음의 표에 EPC코드를 표기하는 방식이 나와 있다.

Copyright © Korea Univ. Library All Right Reserved.

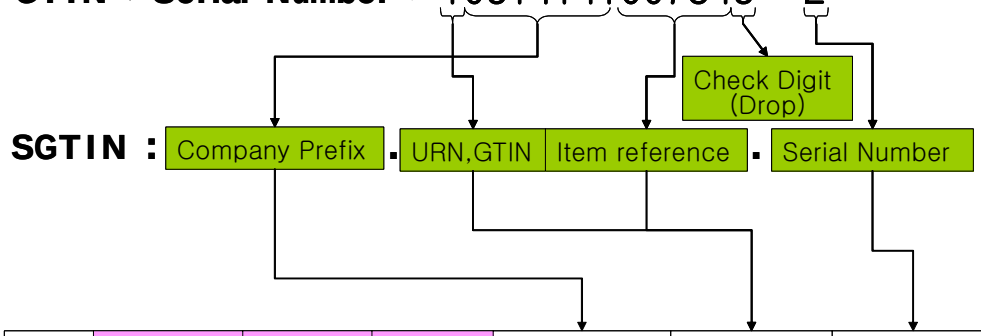
Identity 타입	태그 Encodings	EAN.UCC Code 표기
GID	GID-96	
SGTIN (Serialized Global Trade Identification Number)	SGTIN-64 SGTIN-96	GTIN (with added serial #)
SSCC (Serial Shipping container Code)	SSCC-64 SSCC-96	SSCC
SGLN (Global Location Number)	SGLN-64 SGLN-96	GLN (with additional serial #)
GRAI (Global Returnable Asset Identifier)	GRAI-64 GRAI-96	GRAI
GIAI (Global Individual Asset Identifier)	GIAI-64 GIAI-96	GIAI

위의 방식 중 SGTIN방식을 사용한 예들 들어 다음에 표기되어 있다.

Copyright ⓒ Korea Univ. Library All Right Reserved.

SGTIN (Serialized GTIN)방식을 사용한 예제.

GTIN + Serial Number : 10614141007346 + 2



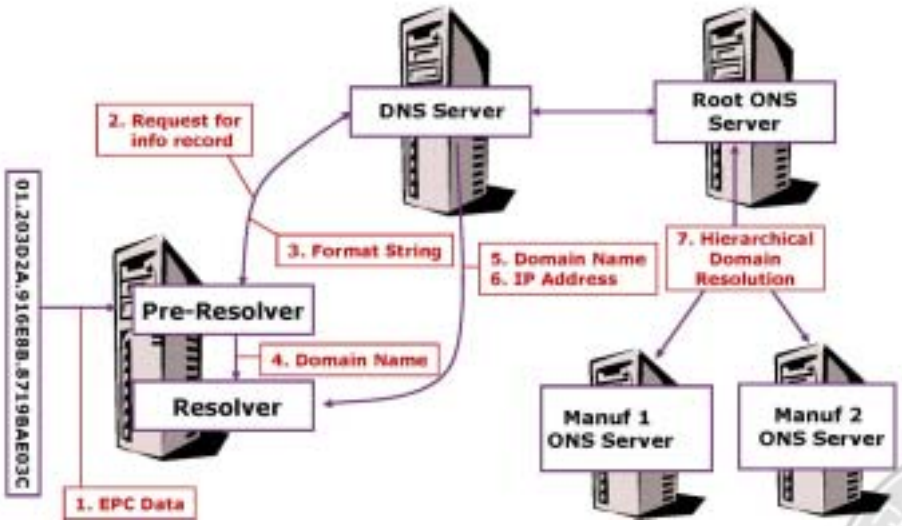
	Header	Filter Value	Partition	Company Prefix	Item Reference	Serial Number
SGTIN -96	8 bits	3 bits	3 bits	24 bits	20 bits	38 bits
	0011 0000 (2진수)	7 (10진수)	5 (10진수)	0614141 (10진수)	100734 (10진수)	2 (10진수)

B. ONS와 PML

1. ONS(Object Name Service)는 EPC 정보를 이용하여 객체의 더 많은 정보를 가지는 서버(PML 서버) URL 를 제공하는 'a global lookup service'이다. 인터넷에서의 DNS(the Domain name Service)와 같은 기술로 ONS는 Framework 기반 위에서 동작한다.

- static ONS : product 생산자의 URL 을 제공
- dynamic ONS : product의 이동에 따른 보관인들의 경로 제공

·local ONS cache는 자주 요청되거나 최근에 요청된 값들이 저장되어 있어 global ONS에 가중되는 통신량의 부담을 덜어준다.

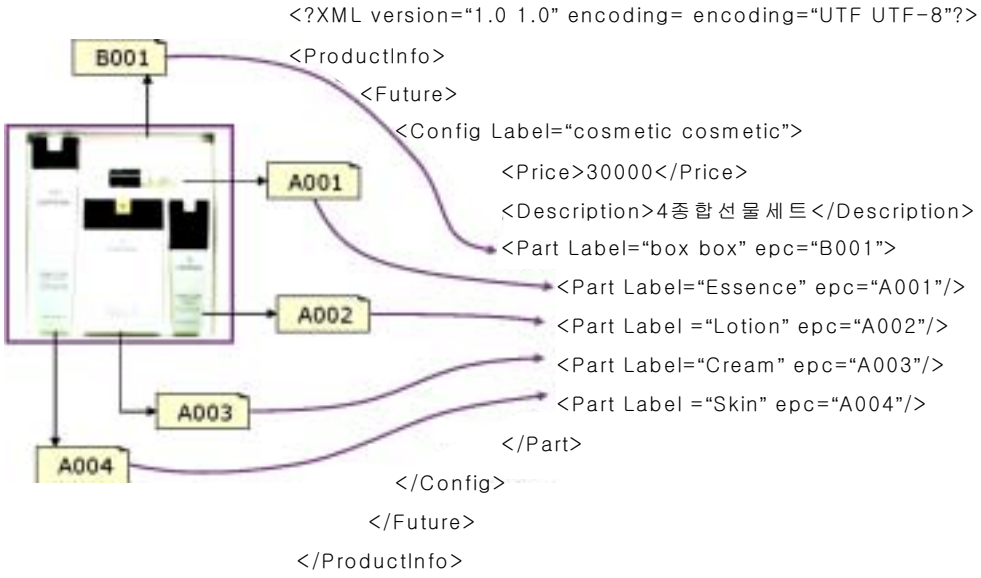


Copyright © Korea Univ. Library All Right Reserved.

2. PML(Physical Markup Language)은 Product에 대한 정보와 그에 대한 관련 정보들은 하나의 데이터 파일 포맷으로 표준화되어 전송되는데, PML은 이러한 파일 정보를 규정하는 언어이다. XML(extensible Markup Language)을 기반으로 하여 Open Format 으로 다른 Information System 과의 상호 연동을 지원한다.

· PML Server는 생산된 모든 product에 대한 정보를 제공하는 Simple Web Server이다. 생산자에 의해 유지되며, PML 형태로 데이터를 주고받는다.

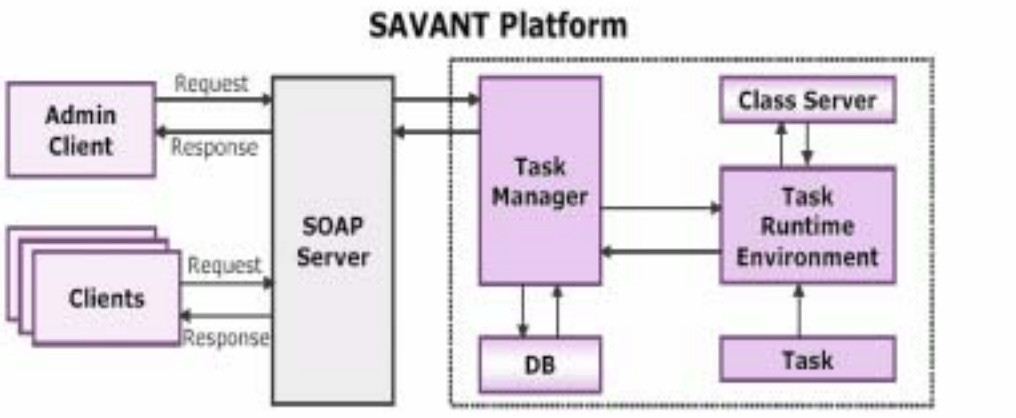
다음의 그림에 PML로 표현된 예가 나와 있다.



C. SAVANT

Savant는 데이터를 라우팅한다. 하나 혹은 더 많은 리더기로부터 모인 태그의 정보들을 가공 처리하는 "middleware"역할을 한다. Data capturing, data monitoring, filtering, aggregation, counting of tag data 등을 수행한다.

Copyright © Korea Univ. Library All Right Reserved.



Savant는 다음의 세가지 요소로 구성되어 있다.

· EMS (Event Management System) :

수집된 데이터를 용도에 맞게 분류하고 해당된 일을 처리하는 곳에 배치하는 역할을 한다.

· RIED (Real-Time in-memory Event Database) : 고성능 메모리 DB역할을 한다.

· TMS (Task Management System) : 실제 일을 처리하는 곳으로 기존의 시스템과 연동한다. Platform에 독립적이고 작은 메모리로 처리가능 하다.

Copyright © Korea Univ. Library All Right Reserved.