저가의 RFID시스템 환경의 프라이버시 보호

이경효*, 양성훈, 명근홍, 박익수, 오병균
*목포대학교 정보공학부
e-mail: {mediakh, bbs510d, upark, obk}@mokpo.ac.kr, {gh6604}hanmail.net

Protection of privacy using Low Cost RFID Schemes

*Kyoung-Hyo Lee, Seong-Hoon Yang, Keun-Hong Myoung,Ik-Su Park,
Byeong-Kyun Oh
*Department of information Security Mokpo National University

요약

차세대 유비쿼터스 환경에서 중요한 기술적 위치를 차지할 것으로 예상되는 무선주파수 인식기술(RFID)은 다양한 분야에서 적용될 것으로 기대가된다. 하지만 핵심이 되는 태그 자체의 특성으로 인하여 사용자의 프라이버시 침해라는 역기능도 내포하고 있다. 따라서 본 논문에서는 이러한 RFID 태그 사용자의 정보 누출에 의한 프라이버시 보호를 위하여 기존의 암호학적 보호기법을 적용하기 어려운 저가의 태그를 이용한 RFID시스템 환경에서 효율적으로 태그의 정보를 보호하는 기법인 블록커 태그를 이용하였다. 블로커 태그는 보호하고자하는 태그의 정보를 알아내고자 하는 공격자의 요청에 대하여 실제 태그와 같은 정보로 응답하되 특정 태그정보가 아닌 전체 태그 정보를 전달하는 형태로 공격자가 특정 태그 정보를 찾지 못하게 하여 사용자의 프라이버시 보호가 가능함을 보였다.

1. 서 론

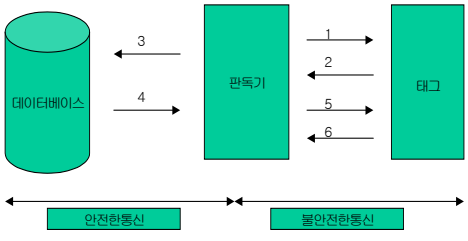
RFID (Radio Frequency Identification) 기술은 초소형 반도체에 식별정보를 넣고 무선 주파수를 이용해 사물을 판독, 추적, 관리하는 기술로 차세대 물류 유통뿐 아니라 전자 지불, 보안 등 다양한 분야에서 새로운 시장을 형성할 것으로 기대되고 있다.

RFID 보안 문제는 크게 두 가지로 구분되는데, 첫째는 태그 내 데이터의 누출이고, 두 번째는 임의의 태그 ID를 추적함으로서 일어날 수 있는 불법 추적행위이다. 이러한 보안요구 사항을 해결하기 위하여 RFID시스템에서 사용자 프라이버시의 보호를 위한 많은 연구들이 진행되고 있다. 본 논문은 RFID기술을 적용하면서 보다 현실적으로 사용자의 프라이버시를 보호할 수 있는 방안으로서 는 별도의 태그를 이용하여 공중파로 노출되는 태그 정보의 노출을 막아 보고자 하는 방안을 제안해본다.

2. 관련연구

RFID시스템은 일반적으로 무선 T(Tag), 무선리더기 R(Reader), 백-엔드 서버(back-end server)로 구성된 정보추적 시스템이다. RFID시스템에서 개인 정보 프라이버시와 위치 프라이 버시를 보장하기 위한 방법 중 하나가 RFID인증 프로토콜이다.

RFID인증 프로토콜에서 태그는 두 가지의 프라이버시를 만족시키기 위해 해쉬 함수를 가진다. RFID 태그는 그 기능에 따라 수동형 태그와 수동형 태그와 인증형 태그로 나눌 수 있는데 본 논문에서 태그는 읽기/쓰기가 가능한 태그로 능동형 태그이다.



[그림1] RFID인증 프로토콜 모델

RFID 인증 방안으로 Hash Base Access Control 기법, Hash lock 기법의 확장인 Randomized Access Control기법, Anonymous ID schme 기법, 공개키 암

호화를 사용하는 외부 재 암호화기법, XOR 기반 원타임 패드기법, 전 방향 안전성을 제공하는 Forward-secure RFID Privacy protection schme 기법, 해쉬 체인 기법에서 서버 B의 계산 로드를 줄이기 위해 제안된 확장된 Forward secure RFID Privacy protection schme, ID값을 다양함으로써 위치 프라이버시를 보장하는 해쉬 기반의 ID변형 프로토콜 등이 있다. 하지만 이러한 방법들이 현재 저가의 RFID 태그의 응용에 적용하기에는 어려움을 가지고 있다.

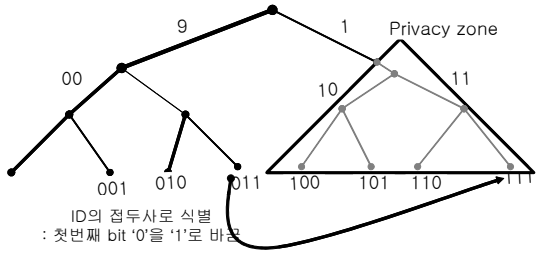
Blocker tag 방법은 기본적으로 위에서 제시된 RFID태그의 응답에 대한 충돌 회피 기법을 제안된 이진 트리를 이용한 2진 트리 프로토콜을 이용하고 있다.

2.1 Full Blocker

Blocker 태그는 기본적으로 2^k인 모든 RFID 태그의 시리얼 번호를 시뮬레이션 하한다. 어떤 노드 B에서 태그 리더에 의하여 다음 한 비트에 대한 질의가 있을 때, 태그는 '0'과 '1'를 동시에 전송함으로서, 의도적인 비트의 충돌로 인하여 리더를 모든 노드로 회귀하게 하여 트리 전체를 탐색하게 한다. 즉 blocker 태그는 모든 가능한 태그의 시리얼 번호를 simulation 함으로서 태그들의 식별을 어렵게 한다.

2.2 Seletive Blocker

Tree-walking에서 동일한 식별자의 접두사를 갖는 태그는 같은 서브 트리 영역에 존재하게 되는 특성을 blocker 태그에 적용하여, 어떤 특정 제조업자에 의해서 생산된 모든 제품을 같은 접두사를 써서 그 제품의 ID를 같은 서브 트리에 둘 수 있고, 이들 ID 역시 tree-walking 알고리즘에 의하여 탐색이 가능하게 된다. 또한 ID의 시작 비트가 '1'인 어떤 특정 영역을 프라이버시 영역으로 설정하여 정보보호를 가능하게 한다.



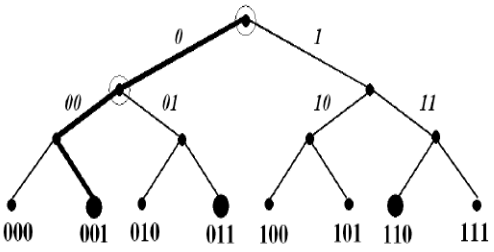
2.3 Reader-friendly Blocking

블러커 태그는 특정 영역은 blocking 하면서 다른 영역은 방해 하지 않고 그대로 놓아준다. 즉'0'으로 시작한 ID가 blocking되면 리더에게 어떤 특정한 서브트리 내에서는 판독하려고 시도 하지 말아야 한다는 사실을 알게 하기 위한 어떠한 방법이 필요하게 된다. 즉 리더는 서브 트리가 blocking 된 시기를 알 필요가 있고 그렇게 함으로써 blocking 된 트리에서 시간을 낭비하지 않고 트리의 다른 부분으로 이동 할 수 있다.

3. Tree Walking Singulation 프로토콜

3.1 Tree-walking Singulation 알고리즘

Tree-walking 알고리즘은 RFID 태그 리더가 가까이에 있는 개별적인 태그의 시리얼 번호를 2진 트리 구조의 탐색 기법을 근거로 2진 비트 단위로 질의에 응답하게 함으로서 태그의 식별 정보를 인식하는 반복적인 depth-first 탐색 기법이라 할 수 있다. [그림 3]는 Tree-walking 알고리즘의 동작을 설명하기 위한 그림이다. 이 트리의 깊이는 3이고, 태그의 개수는 8이며 나무의 잎의 노드의 수와 일치하며, 서브트리는 각각 이태릭체로 표현하였고, 001, 011, 110과 같은 3 개의 태그가 존재 한다고 가정할 때, Tree-walking 알고리즘은 먼저, 진한 선으로 표시된 경로를 따라서 011 태그를 singulation한다.



[그림 3] Tree- walking example

3.2 Blinded Tree Walking

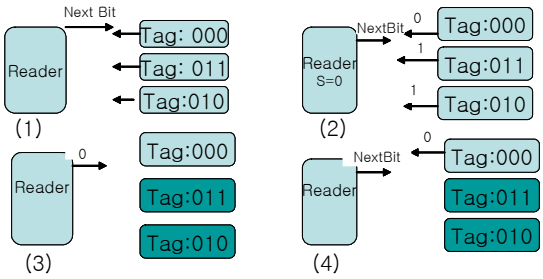
[그림4]는 Blinded Tree walking 알고리즘으로 태그 ID를 통해 변형된 이진 트리 워킹을 보인다.

1.Reader queries the first bit. No collision occurs

2.Reader stores first secret bit ardects and collosion on second bit.

3.Reader chooses tags with 0 in second bit tags by sending (0XOR s) Other tag deactivate

4. Reader singulates remaining tags



[그림4] Blinded Tree walking 알고리즘

이 기법에서는 태그가 공통의 ID접두사를 공유하고 있다고 가정했기 때문에 리더는 판독하는 과정에서 그것을 후 방향 채널을 통해서 공유된 비밀로써 가질 수 있다. 공유 된 비밀 접두사는 ID의 특정한 부분의 값을 숨기는데 사용될 수 있다.

3.3 Randomized Tree Walking

위에서 무작위화를 통해 Blinded Tree Walking 알고리즘은 간략화 될 수 있다. 각 태그는 각 트리에 무작위 pseudo-ID를 생성하고 리더는 pseudo-ID를 후방위부 채널로 전달하면서 각 트리 전달 세션에 새 pseudo-ID를 갖는다. 파워 공급이 중단되면 pseudo-ID는 삭제된다.

이 기법 안에서 주로 pseudo-ID비트가 전 방향 채널로 브로드 캐스트 될 것이다. 리더 쪽에서의 태그 접두사 또는 비밀키 관리에 관한 어떠한 가정도 필요하지 않는다.

Pseudo-ID비트는 실제적으로 몰래 생성 되어진다. 리더는 무작위 비트에 대해서 모든 태그에게 질문한다. 태그는 그들이 활동 중단 시킨 비트를 유지하고 있어야 한다. 충돌이 없는 몇몇 비트 이후, 리더는 태그가 구분 되어졌다고 확신할 것이다. 두 태그가 같은 무작위 비트를 생성한 상황에서도 리더는 보통 ID를 통해서 충돌을 감지 할 수 있을 것이다. 이 방법에 대한 리더의 두개의 인자를 받는 탐색 알고리즘은 [그림5]에 나타나 있다

i는 현재의 비트위치이고 num은 충돌 없는 연속적인 비트의 수이다. 만약 num이 미리 정해진 인계치를 넘으면 리더는 태그가 구분되어 졌다고 여기고 그 태그의 ID를 읽으려고 할 것이다.

Traverse(i,count)
b_i:=Read random bit I from all active tags
If collsion on b_i is detected
Suspend alltags with b_i==1.
Eash suspended tags stores i.
Travers($_i$+1,0).
Wake up all tags suspended on bit$_i$.
Travers($_i$+1,0).
else if no collosion on b_i is dected:
If (count > threshold) Tree- Walk remaining tags.
else Traverse ($_i$+1, count+1)

[그림5]Randomized Treewalking알고리즘

pseudo-ID의 길이의 선택은 근처의 태그 집단의 수에 의존한다. n개의 태그 집단에 대해서 m 개의 PSEUDO-id비트가 사용된다고 가정하자. 무작위로 특정 pseudo-ID에 대한 선택할 태그의 수는 포아송 분포를따른다 . 만약 m = $\frac{n}{2^m}$이면 k 개의 태그 pseudo-ID의 기댓값은 $2^m e^{-\lambda} \frac{k}{k!}$ 이다. n =2000이고 m=16, λ=.03이라고 가정하면 k 개의 태그의 pseudo-ID의 기댓값은 [표1]에 나타나 있다.

만약 96비트 ID를 사용한다면 16비트의 pseudo-ID 는 17%의 추가 부하를 의미한다. 만약 PSEUDO-id값을 가진 K 태그의 각각의 충돌이 필수적으로 ID데이터의 k 비트를 유출한다. 대안적으로 적응될 수 있는 기법은 실제 ID가 충돌이 일어났을 때에만 pseudo-ID를 묻게 하는 것이다. [표1]에서 주어진 예에서 96비트의 ID를 가진 2000개의 태그는 약 192,000비트의 데이터를 가진다. 충돌은 각각의 트리 탐색에 있어서 이 데이터의 약 30비트를 노출 시킬 것이다. Pseudo-ID의 길이와 가짜 ID충돌을 어떻게 다룰 것인가의 선택은 태그의 사용자의 특정한 프라이버시와 수행 능력의 요구에 달려있다.

[표1]무작위 16비트의pseudo-ID에서의 2000개의 태그의 기대되는 분포

k	k개의 태그의 가짜 ID	비고
0	63599	대부분의 가짜ID는 선택되지 않았을 것이다.
1	1907	대부분의 태그는 유일한 가짜 ID를 선택할 것이다.
2	28	약간의 태그쌍이 같은 가짜 ID로 충돌할 것이다.
3	0.29	두개이상의 태그는 드물게 충돌할 것이다.

4. 결론

본 논문에서는 이러한 RFID 태그 사용자의 정보 누출에 의한 프라이버시 보호를 위하여 사용 하여진 블록커 태그에 대하여 연구하였다. 블록커 태그는 Tree-walking 알고리즘을 기반으로 모든 태그 시리

얼 번호를 시뮬레이션 할 수 있을 뿐만 아니라, 선택적으로 ID 태그의 특정 영역만 시뮬레이션을 함으로서 특정 제조업자의 제품 관리나 사용자의 프라이버시 보호가 가능하다. 블러커 태그 방법은 현재 RFID 태그에 바로 적용할 수 있다는 실용적인 측면과 향후 유비쿼터스 환경에서 RFID태그로부터의 정보를 재활용할 수 있다는 측면에서 의미를 부여할 수 있다. 향후 RFID는 유비쿼터스 환경의 기본 인프라로 그 역할이 증대될 것으로 예상되는바 전체적인 연관으로 인해 USN환경에서의 보안과 밀접하게 관련되어야 할 것으로 전망된다.

5. 참고문헌

[1] S. A. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *First International Conference on Security in Pervasive Computing* ,2003. To appear.

[2]S.A.Weis,Radio-frequency identification systems and privacy. Master's thesis, M.I.T June 2003(expected).

[3]R.Pappu,2003,Personal communication.

[4] S. E. Sarma, S. A. Weis, and D. W. Engels RFID systems, security and privacy implications. Technical Report MIT-AUT ID-WH-014, AutoID Center, MIT,2002.

[5] Benetton undecided on use of' smart tags'. *Associated Press*, 8April 2003.

[6] D. L. Brock. The electronic product code (EPC): A naming scheme for objects. Technical Report.