저가 RFID 태그를 위한 Selective Blocking 기반 프라이버시 향상 기법*

김수철° 여상수 김성권
중앙대학교 컴퓨터공학부
{sckim°, ssyeo}@alg.cse.cau.ac.kr , skkim@cau.ac.kr

Selective Blocking-Based Privacy Enhancing Scheme for Low-cost RFID Tags

Soo-Cheol Kim° Sang-Soo Yeo Sung Kwon Kim
School of Computer Science and Engineering, Chung-Ang University

요 약

최근 RFID에 대한 관심이 높아지고 있다. RFID 사용량도 증가하는 추세에 있으며, 앞으로는 생활 전반에서 RFID를 이용하게 될 것으로 전망한다. 그러나 사용자 프라이버시 보호 기법의 개발은 아직 해결해야 할 문제이다. 저가형 태그에는 기존 다른 시스템에서 사용되던 여러 가지 암호시스템의 적용이 어렵다. 그래서 많은 사람들이 RFID 태그에 적용 가능한 여러 가지 기법을 제시하였다. 그 중 Blocker 태그를 사용해서 프라이버시 보호와 범죄방지를 하는 기법이 있다. 그러나 Blocker 태그 기법에서는 쓰기 능력을 가지고 있는 태그에 적용 가능하다는 단점이 있다. 본 논문에서는 읽기만 가능한 저가형 태그에서도 Blocker 기능을 수행할 수 있는 새로운 기법을 제안하였다. 제안하는 기법은 현재 태그에서 최소한의 변경으로 프라이버시 보호와 범죄방지를 위한 실질적인 해결책으로 사용이 가능하다.

1. 서 론

근래에 RFID 시스템을 사용하는 회사나 곧 사용하고자 하는 곳이 많이 늘어나고 있다. 그 이유로는 RFID 시스템을 사용하는데 가장 문제점이 되었던 태그 가격이 적정수준에 근접해가고 있기 때문이다.

태그에도 여러 가지 종류가 있는데 태그의 전원 공급 방식에 따라 능동형, 수동형 태그로 나눌 수 있다. 능동형 태그는 태그가 자체적으로 전원을 가지고 있어 통신 거리는 강력하지만 그에 따라 크기와 가격도 올라간다. 그에 반해 수동형 태그는 전원이 없는 태그로서 통신 거리가 짧지만 크기와 가격이 저렴해 질 수 있다. 현재 수동형 태그를 가장 중점적으로 개발하는 중이고 본 논문에서도 수동형 태그를 고려대상으로 한다.

RFID에 가장 영향력 있는 EPC Global의 기본 태그인 EPC(Electronic Product Code) 태그를 예를 들겠다. 현재 진행되고 있는 UHF 대역의 EPC 표준은 수동형 태그를 위한 class 1의 generation 2 표준으로써 2005년 초에 표준화가 완료될 것으로 보인다. class 1 태그는 identify 태그로서 바코드를 대체하는 물류와 유통을 위한 SCM(Supply Chain Management)을 목표로 하고 있다[1].

그러나 RFID 시스템은 안정성과 프라이버시 측면에서 여러 가지 문제점이 발생하고 있다. 그 중에서도 쉽게 도청이 가능한 점과 위치추적이 용이하다는 점은 사용자 프라이버시에 심각한 문제이다. 그러므로 RFID 시스템을 사용하고자 할 때 보안 및 프라이버시 문제 해결이 우선되어야 한다.

프라이버시 보호를 위해 여러 가지 방법이 제시되었는데 가장 단순하면서도 확실한 방법은 kill 태그[1]를 사용하는 것이다. 그 외에도 hash를 사용해서 사용자 인증을 하는 방법[2]과 Blocker 태그[4,5]를 사용하여 사용자 프라이버시를 보호하는 방법들이 있다.

본 논문에서는 기존에 제안된 여러 가지 프라이버시 보호 방법들을 간략히 설명하고 그 기법들의 문제점에 대해 이야기한다. 그리고 저가형 태그에 적용될 수 있는 효율적이고 실용적인 프라이버시 보호 기법을 제안한다.

2. 관련 연구

RFID 프라이버시 보호를 위한 가장 극단적인 방법은 사용자가 가게에서 물건을 사고 나면 출구에서 RFID 태그를 파괴하거나 kill 명령어를 사용해 사용 중지해 버리는 것이다[1]. 태그는 내부에 단락회로가 있기 때문에 이를 끊음으로서 'kill 명령'을 실행하게 되는데 한 번 죽은 태그는 다시 살릴 수 있는 방법이 없게 된다. 그러면 위치트래킹 같은 공격을 원천적으로 막을 수 있지만 RFID의 다양한 서비스를 포기하게 된다. 그래서 단순히 태그를 무력화 시키는 방법은 너무 극단적인 방법이다.

kill 태그의 극단적인 방법을 피하고 인증된 리더만 정보를 읽을 수 있게 하는 방법으로 hash-lock 기법이 제안되었다[2]. hash-lock 접근 제어 태그를 잠그기 위하여 리더는 난수 형태의 키를 hash 하여 DB에 저장하고 이

* 본 연구는 한국과학재단 특정기초연구 (R01-2005-000-10568-0) 지원으로 수행되었음.

를 태그의 metaID로 사용한다. 그리고 리더는 태그에서 metaID를 보내고 태그는 이를 저장하고 잠김 상태가 된다. 태그를 풀기 위해서는 리더가 질의를 하면 태그는 자신이 저장한 metaID를 전송하게 된다. 리더는 그 metaID로 DB에서 정확한 key값을 찾아 자신이 정당한 리더임을 증명한다. 리더가 보낸 key값을 hash 하여 나온 값이 자신의 metaID와 동일하다면 그 후 정상적인 통신이 이루어지는 방식이다. 평상시에는 lock 상태이지만 정당한 리더만 태그를 unlock 할 수 있다는 것이다. 하지만 이 기법은 metaID가 고정되어 있기 때문에 위치 트래킹 공격을 막을 수 없다. 또한 태그는 반드시 hash 값을 계산할 수 있어야 한다(그림 1).

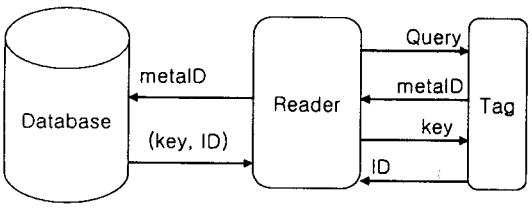

그림 1. hash-lock 기법[2]

Ohkubo는 태그가 hash 함수를 가지고 내부 비밀 값을 변경해가면서, 출력도 hash 함수를 해서 얻은 값을 전송하게 하는 기법을 제안하였다[3]. 리더는 태그의 출력값을 후방 서버에 전송하고, 후방 서버는 brute-force 방법으로 모든 태그의 hash seed에 대해서 hash chain 길이만큼의 연산을 수행해야 태그의 ID를 판별 할 수 있다. 2개의 hash 함수로 이루어진 hash chain 기법은 지금까지의 기법 중 가장 안전하다고 알려졌다. 그러나 태그 판별을 위한 후방 서버의 계산양이 매우 많아서 태그의 수가 증가할수록 태그 인식에 걸리는 시간이 급격히 늘어나게 된다.

다음으로 Juels가 제안한 Blocker 태그 기법이다[4,5]. 이 기법의 요점은 상품 태그 이외에 사용자가 "Blocker 태그"를 가지고 있는 방식이다. Blocker 태그는 리더가 여러 개의 태그를 읽기 위해서 사용하는 anti-collision 프로토콜(그림 2)을 역이용하여 질의응답 할 때 항상 0과 1을 모두 대답함으로써, 특정 태그의 존재 여부를 숨기고, 리더가 중도에 포기하게 만든다. 일종의 전파방해로서 리더가 태그들의 ID를 알아내는 것을 방해한다. 모든 태그를 blocking 하는 방식을 universal Blocker 라고 하는데 이 방식은 Blocker 태그를 이용한 범죄행위에 악용될 가능성이 있다. 상점에 Blocker 태그를 들고 가서 특정 물품의 태그를 blocking 하게 되면 쉽게 절도를 할 수 있다. 그와 반대 개념으로 일부만 blocking 하는 방식을 selective Blocker 라 한다. 예를 들어, 최상위 비트(most significant bit)가 0이면 blocking 하지 말고, MSB가 1로 시작하는 태그들만 blocking 하는 방식이다. Juels는 이를 이용해 상점에서의 범죄 행위를 막을 기법을 제시하였다. 각 태그들은 쓰기가 가능한 태그라는 전제조건으로 물건들이 상점 안에 있을 때는 각 물품 태그들의 MSB를 0으로 해둔다. 이 상황에서는 Blocker 태그가 아무런 방해를 할 수 없다. 물건을 구입하여 계산대를 통과하면 태그의 MSB를 1로 바꿔준다. 즉, 태그들은 privacy zone에 들어가게 되는 것이다[5].

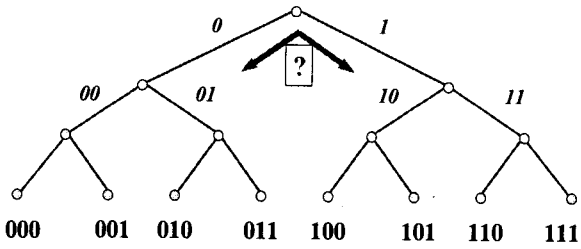

그림 2. tree walking protocol

3. 제안하는 기법

지금부터는 selective Blocker 기반에서 저가형 RFID 태그를 이용한 프라이버시 향상 기법을 제시한다. 앞서 나왔던 Blocker 태그 기법은 쓰기가 가능한 태그만 사용할 수 있는 단점이 있지만 제안 기법은 훨씬 싼 읽기 전용 태그도 가능하다. 읽기 전용 태그를 사용해도 프라이버시 보호와 범죄 방지 효과는 동일하다. 그림 3과 같이 첫 번째 태그는 기본적인 ID 태그로서 각 물품마다 가지고 있다. 상점에서 물품 진열시 MSB를 0으로 가지는 두 번째 태그(임시 태그)를 사용하는 것이다. 임시 태그에서 사용하는 임시 ID는 간단하게 물품 태그 ID의 MSB만 1로 바꿔서 쓰는 것이 임시 ID와 물품 ID를 연동하는데 편할 것이다. Blocker 태그를 이용한 범죄를 시도할 시 물품 자체의 태그는 리더를 피할 수 있지만 두 번째 태그인 임시 태그가 존재하므로 범죄는 불가능 하게 된다. 물품을 사고 나간 후 출구에서는 임시 태그만 kill 해주면 된다. 그러면 바깥에서는 상품이 물품 태그만 가지고 있으므로 Blocker 태그가 정상적으로 동작하여 사용자의 프라이버시 보호가 된다.

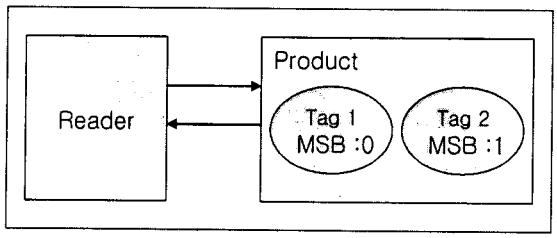

그림 3. 제안한 Blocker 태그 방지 기법

제안하는 기법에서 프라이버시의 보호는 Blocker 태그 기본 기법의 원리를 그대로 이용하게 된다. Blocker 태그를 사용하면 기본적으로 모든 리더의 스캔을 방해하게

되므로 위치트래킹 공격이나 스푸핑 공격은 시도 할 수 없다. 프라이버시 보호를 위해 정상적인 리더와 공격자 리더의 구분 없이 방해해 버리는 것이다. 정상적인 RFID 태그를 사용하고자 할 때는 Blocker 태그를 없애면 되므로 전적으로 사용자의 선택에 의하여 프라이버시 보호 수준과 RFID 태그의 사용 여부를 결정하게 되는 장점이 있다. 또한 Blocker 태그의 문제점이었던 범죄악용 가능성도 막을 수 있다.

다음으로 위에서 제안했던 태그 2개를 사용하는 방법을 발전시켜 좀 더 가격을 줄일 수 있는 향상된 기법을 소개한다. 각각의 태그에는 통신을 위한 안테나가 필요한데 그것이 태그 가격의 큰 부분을 차지한다. 따라서 2개의 태그에 2개의 안테나를 사용하지 말고 태그 내에 하나의 안테나와 두 가지의 모듈을 가지는 새로운 형식의 태그를 만드는 것이다. 그림 4에 표현되어 있듯이 한 태그에 MSB가 0인 모듈과 1인 모듈로 나눠져 있다. 태그를 만들 때 이런 형식으로 만들어서 물품 생산 공장에서는 MSB가 1인 모듈에 물품의 ID를 넣고, 물품을 판매하는 상점에서는 MSB가 0인 모듈에 임시 ID를 등록하는 것이다. MSB가 1인 모듈만 있을시 정상적인 태그로 작동하는 것이고 MSB가 0인 모듈도 같이 있을 때는 앞쪽에 있는 MSB가 0인 모듈이 우선순위를 가지게 되는 것이다. 물품이 판매되었을 경우 태그에서는 앞쪽 모듈만 막아주면 자연적으로 Blocker 태그 사용가능한 일반 태그가 된다.

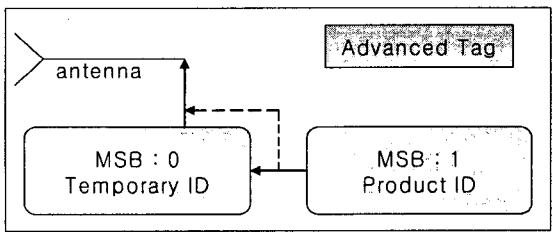

그림 4. 향상된 제안 기법

4. 비교 분석

지금까지 사용자의 프라이버시를 보호하기 위한 기존 RFID 인증 기법에 대해 알아보았으며, 그들의 단점을 보안하기 위해 제안한 기법을 설명하였다. 아래의 표1은 위에서 설명한 각 기법과 논문에서 제안한 기법에 대한 안정성과 효율성, 계산량, 비용 측면에서 서로 비교분석한 것이다. 표1에 따르면 우리가 제안한 기법은 여러 가지 측면에서 강점을 보이고, 특히 비용 면에서 가장 경쟁력이 있음을 보여준다.

표 1. 각 기법과 제안기법 비교분석

	Kill 명령어	hash -lock	Ohkubo 기법	Blocker Tag	제안하는 기법
안전성	우수	보통	매우우수	우수	우수
범용성	나쁨	우수	우수	우수	우수
계산량	우수	보통	나쁨	우수	우수
비용	우수	보통	보통	보통	매우우수

5. 결 론

본 논문은 현재 사용되고 있는 저가형 태그에 적용될 수 있는 프라이버시 보호와 범죄이용 방지를 위한 기법을 제안하였다. 제안하는 기법은 현재 사용되고 있는 태그에서 특별한 모듈을 첨가 하지 않고서도 쉽게 적용 할 수 있는 장점이 있다. 최소한의 변경으로 RFID 시스템 구축에 가장 문제가 되는 비용 측면에서 많은 장점을 보인다.

향후에는 논문에서 제시된 기법에서 중점적으로 다루지 않았던 물품이 반품되었을 경우에 쉽게 처리할 수 있는 개선 기법에 대하여 연구할 필요가 있다.

6. 참고문헌

[1] S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications", In CHES 2002, vol. 2523 of LNCS, pp. 454-469, August 2002.

[2] S. Weis, S Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", In Proceedings of the 1st International Conference on Security in Pervasive Computing, 2003

[3] M. Ohkubo , K. Suzuki, and S. Kinoshita, "Cryptographic approach to `Privacy-Friendly` tags", In RFID Privacy Workshop, MIT, November 2003.

[4] A. Juels, R. Rivest, and M Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy" , In Proceedings of 10th ACM Conference on Computer and Communications Security(CCS 2003), pp. 27-30, October 2003.

[5] A. Juels and J. Brainard , "Soft Blocking : Flexible Blocker Tags on the Cheap" , WPES '04 (one of worksEhop of ACM CCS 2004), October 2004.