論 文
54P-4-9

고기능 RFID 태그를 위한 보안 프로토콜

A Secure Protocol for High-Performance RFID Tag

朴 鎭 成† · 崔 明 烈*
(Jin-Sung Park · Myung-Ryul Choi)

Abstract - In this paper, we have proposed a secure dynamic ID allocation protocol using mutual authentication on the RFID tag. Currently, there are many security protocols focused on the low-price RFID tag. The conventional low-price tags have limitation of computing power and rewritability of memory. The proposed secure dynamic ID allocation protocol targets to the high-performance RFID tags which have more powerful performance than conventional low-price tag by allocating a dynamic ID to RFID using mutual authentication based on symmetric encryption algorithm. This protocol can be used as a partial solution for ID tracing and forgery.

Key Words : RFID, Authentication protocol, Privacy

1. 서 론

근래 들어 RFID 시스템은 공급망 관리를 시작으로 생산, 재고관리 분야는 물론 다양한 산업 전반에서 관심을 받고 있다. 현재 바코드를 대체한다는 전제를 바탕으로 작고 값싼 태그에 대한 집중적인 연구가 진행되고 있으며 그에 따른 보안 문제와 프라이버시 보호 또한 해결해야할 문제이다[1]. 저가형 RFID 태그의 경우 단일의 고정된 ID를 저장하고 있기 때문에 이를 도청하면 위치 추적과 이동 경로를 파악할 수 있어 개인의 사생활 침해가 가능하며, 위조된 ID를 구별할 수 없는 등의 보안 문제가 그 대표적인 예이다[2]. 이러한 문제를 해결하기 위해 Kill 명령[3], 해쉬-락[2], 재암호화[4], 해쉬 체인[5], 블로커(Blocker) 태그[6] 등의 다양한 보안방식이 연구되고 있으나, 모두 RFID 태그 가격을 5센트 미만으로 목표하고 있어 그 구현과 보안성에 상당한 제약이 따른다. 그러나, 이러한 문제는 보다 우수한 계산 능력과 큰 저장 공간을 가지는 고가형/고기능 RFID 태그에서는 다른 접근 방식으로 해결될 수 있는 문제이다. 따라서, 본 논문에서는 저가형 태그보다는 향후에 더 사용이 활성화될 고기능(High-Performance) RFID를 대상으로 그에 적합한 동적 ID 할당 프로토콜을 제안한다. 이 프로토콜은 DES나 AES, SEED와 같은 대칭형 암호화 알고리듬에 기반한 상호 인증을 통해 보안을 유지한다. 이미 RFID에 상호인증과 대칭형 암호화 알고리듬을 적용하는 연구가 진행되고 있으나, 고기능 RFID보다는 저가형 태그를 중심으로 하고 있다[7,8]. 고기능형 RFID는 현재의 스마트카드가 채택하고 있거나 그 이상의 계산능력을 가지는 RISC CPU에 대용량의 EEPROM 혹은 FRAM과 같은 재기록 가능한(rewritable) 메모리를 가지고 있으며, 저전력 문제를 해결하기 위해 자체 전원을 내장하는 semi-active 혹은 active형 태그라고 상정한다[9]. Auto-ID 센터에 따르면, 현재의 저가형 태그는 클래스 0와 클래스 Ⅰ에 해당하며, 향후 클래스 Ⅱ에서 클래스 Ⅴ 이상으로 진화하는 경우 암호화 기능과 메모리를 내장할 것으로 전망하고 있다[9]. 2006년 초 개정 확정 예정인 국제규격 ISO 18000 Part 6 Type C가 바로 클래스 Ⅰ의 Generation 2이므로, 클래스 Ⅱ이상으로 진화하는 것도 머지않으리라 예상된다(그림 1 참조). 하지만, 고기능 RFID 태그는 저가형 RFID 태그를 교체하는 것이 아니라 저가형 RFID 보다는 좀 더 강력한 보안이 필요한 응용 분야에 사용될 것으로 전망된다. 이러한 고기능 RFID 태그에서는 단순한 수동형 동작뿐 아니라 능동적으로 외부 환경에 따라 동작하는 기능도 가능하기 때문에 이를 고려한 보안 방식이 요구되어진다. AES와 같은 대칭형 암호화 알고리듬으로 인증을 수행하는 알고리듬들이 제안되고 있지만, 아직까지는 단순한 인증에만 초점을 맞추고 있다[7,8]. 고기능형 RFID는 개방형 스마트카드가 채택하고 있는 GOP(Global Open Platform)의 상호 인증 프로토콜[10]을 수행하기에는 통신 시간의 제약[1]을 받기 때문에 그보다는 좀 더 간단한 인증 프로토콜이 필요하다. 또, 고정된 ID 때문에 발생하는 보안 문제를 해결하기 위해 수시로 새로운 ID를 암호화하여 부여하고 서버는 항상 새로운 ID를 통해 태그를 인식하게 하면 설령 공격자가 ID를 추적한다 하더라도 이전 ID와 변경된 ID간의 상관관계를 알 수 없기 때문에 위치 파악이 불가능하다. 따라서 본 논문에서는 저가형 RFID용 보안 프로토콜보다는 강력하지만 스마트카드의 보안 프로토콜보다는 간단하면서 동적인 ID 부여와 상호인증이 가능한 프로토콜을 제안한다. 이러한 고기능 RFID와 보안 프로토콜은 명품

† 교신저자, 正會員 : (주)CEN 연구소장
E-mail : pjs72@asic.hanyang.ac.kr
* 正 會 員 : 한양대학교 전자컴퓨터공학부 교수
接受日字 : 2005年 11月 10日
最終完了 : 2005年 11月 14日

브랜드 제품이나 고가 의약품의 관리, 문화재 관리 등과 같은 고가이면서 엄격한 보안과 관리가 필요한 분야에 적용할 수 있다. 또한, ID를 변경할 수 있다는 것은 RFID 태그의 재활용이 가능하다는 의미이므로 한번 사용하고 버리는 것이 아닌 고부가가치를 지니는 품목에 대한 관리에 적용하는 것이 적합할 것이다.

본 논문의 2장에서는 기존 RFID의 보안 방식과 그에 따른 보안 요구 사항 등에 대해 알아보고, 3장에서는 제안한 프로토콜에 대하여 설명하였다. 4장에서는 제안 프로토콜의 데이터 구조를 설명하며, 5장에서는 제안된 프로토콜에 대한 보안 특성을 분석한다. 마지막으로 결론과 향후 진행방향은 6장에서 논하였다.

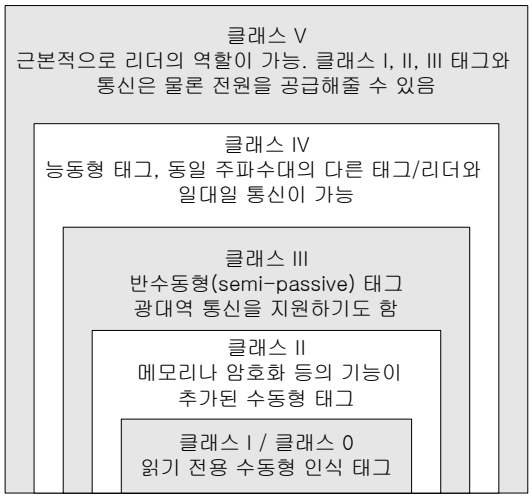

그림 1 RFID 태그의 클래스 구분
Fig. 1 Class of RFID Tag

2. RFID 보안

2.1 RFID 보안 요구 사항

RFID 시스템은 그 통신 수단이 무선이지만, 태그 자체의 계산 능력과 메모리의 재기록(rewrite)이 어려운 제약으로 인해 보안상 많은 취약점을 가진다. RFID 시스템에 가해질 수 있는 보안 공격에 대해 살펴보면 다음과 같다[11].

(1) 도청 : RFID의 통신방식은 무선이므로 공격자가 태그와 리더간의 통신을 도청하는 것은 쉬운 일이나, 도청을 통해 얻은 정보가 공격에 활용되지 않도록 통신 데이터를 선정하여야 한다.

(2) 위치추적 : 태그가 고정된 ID를 가지고 있고, 공격자가 다수의 리더기를 이용하여 그 ID의 위치 변화를 감시하는 경우 태그 소유자의 이동경로를 파악할 수 있다.

(3) 스푸핑(Spoofing) : 공격자가 정당한 리더로 위장하여 태그의 정보를 수집하거나 그 반대로 정당한 태그로 위장하여 리더기를 속이는 경우인데, 상호 인증을 통해 방지할 수 있다.

(4) 서비스 거부 : RFID 시스템이 사용하는 주파수 영역을 교란하는 방해전파를 발산하여 통신이 불가능하게 하거나, 다수의 태그가 존재하는 것처럼 대량의 태그 정보를 일시에 리더로 전송하여 리더의 정상적인 동작을 방해하는 방법이다.

이러한 공격으로부터 안전한 인증 방식을 설계하는 경우, 고려해야할 사항은 다음과 같다.

(1) 도청에 대한 안전성 : 공격자가 태그와 리더기간의 통신을 도청하여도 공격에 유용한 정보를 얻지 못하여야 한다.

(2) 위치 추적 방지 : 정당한 시스템 이외에는 시스템이나 리더에서 태그의 이동 경로 파악이 불가능하여야 한다.

(3) 스푸핑 방지 : 통신 상대방이 정당한지를 상호 인증으로 확인하고 중요 데이터를 교환하며, 확인할 방법이 없다면 중요 정보를 전송하지 않아야 한다.

(4) 재생 공격(replay attack) 방지 : 공격자가 정당한 태그와 리더간의 통신을 도청하고 이를 그대로 다시 사용하여 어느 한쪽을 가장하는 것이 불가능하여야 한다.

2.2 기존 RFID 보안 방식

2.2.1 Kill 명령어[3]

MIT의 Auto-ID 센터(현재 EPCglobal)에서 제안한 방식으로 태그에 8비트의 패스워드를 내장하고 있다가 동일한 패스워드와 Kill 명령이 전달되면 자신의 모든 기능을 중지시켜 다시는 사용할 수 없도록 하는 것이다. 이 명령을 실행하면 태그 내부의 회로들이 완전히 단락되며, 한 번 죽은 태그는 되살릴 수 없게 되어 태그를 재사용할 필요가 있는 분야에는 적용이 불가능하다. 이 방식은 현재 EPC 클래스 1 태그와 ISO 18000 Part 6 Type C 태그에 기본 기능으로 내장되고 있다.

2.2.2 해쉬-락 방식[2]

이 방식에서 리더는 각 태그에 대한 키를 가지고 있으며, 태그는 기본적으로 잠김 상태에 있어서 그 키에 대한 해쉬 값 metaID를 저장하고 있다가 리더에게 접근하면 이 metaID를 전송한다. 리더는 이 metaID로부터 키를 유추하여 키 값을 태그로 보내고, 태그는 키에 대한 해쉬 값을 계산하여 자신의 metaID와 일치하는 경우에만 잠김 상태에서 빠져나와 자신의 ID를 리더에게 전송한다. 이 방식은 태그가 가지는 metaID가 항상 일정하기 때문에 추적이 가능한 단점이 있으며, 공격자가 태그의 metaID를 입수하여 정당한 리더에게 재생하여 보내는 경우 리더는 올바른 키를 공격자에게 보내게 되는 위험이 있다.

2.2.3 랜덤화된 해쉬-락 방식[2]

위의 해쉬-락 방식에 가지는 문제를 해결하기 위해 태그는 의사난수생성기를 이용한다. 태그는 자신의 ID와 자신이 생성한 난수로 해쉬를 계산하여 리더로 전송하기 때문에 항상 해쉬 값이 변하게 된다. 리더는 태그로부터 전달된 해쉬 값과 난수를 가지고, 서버로부터도 모든 태그의 ID를 받아 수신한 난수로부터 해쉬값을 계산하여 일치되는 태그 ID를 찾은 후 태그로 전송한다. 따라서, 추적을 피할 수는 있으나 태그에 의사난수 생성기를 내장하여야 하며 서버/리더기의 계산량이 많아진다는 부담이 있다.

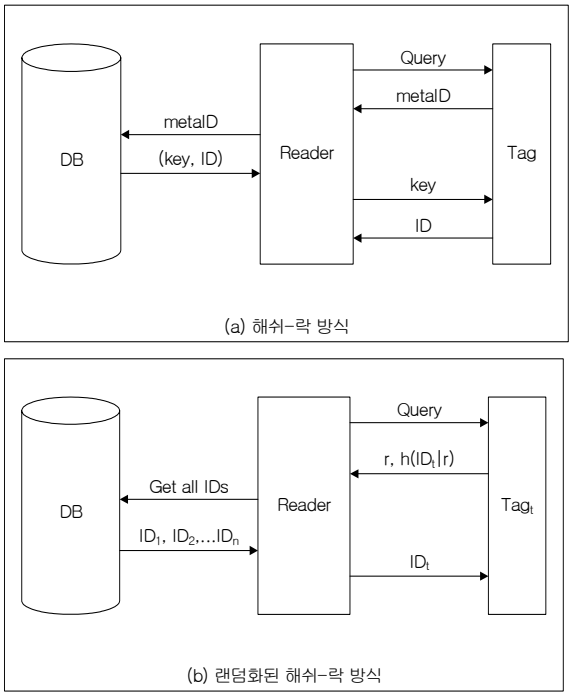

그림 2 해쉬-락 방식과 랜덤화된 해쉬-락 방식
Fig. 2 Hash Lock and Randomized Hash Lock

2.2.4 해쉬 체인 방식[5]

두 개의 해쉬 함수 H와 G를 사용하여 해쉬 체인을 구성한 것으로 태그가 초기에 정보 si를 가지고 있으면, 리더와의 i 번째 통신에서 ai = G(si)를 보내고 자신의 정보는 si+1 = H(si)로 갱신하여 보안을 유지한다. 리더에게 응답할 때는 H 함수를 사용하고, 자기 자신의 비밀 값을 갱신하기 위해서는 G 함수를 사용하기 때문에 이동경로 파악을 방지할 수 있으나, 백엔드 시스템에서의 계산량이 많고 2개의 해쉬 함수를 사용한다는 점이 해쉬락 방식에 비해 부담이 된다.

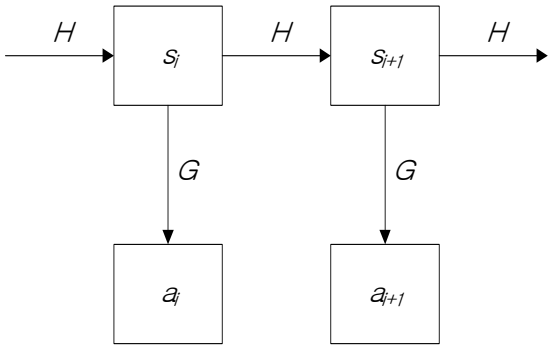

그림 3 해쉬 체인 방식
Fig. 3 Hash-Chain

2.2.5 블로커 태그 방식[6]

이 방식은 하나의 품목에 일반적인 태그와 함께 블로커 태그를 하나 더 부착하는 것이 특징이다. 이 블로커 태그는 모든 질의에 대해 "그렇다"라고 응답하기 때문에 리더기가 혼란을 일으켜 올바른 태그 데이터를 읽지 못하게 되며, 공격자가 있을 경우 블로커 태그의 무조건적인 응답으로 인해 실제 필요한 태그의 정보를 읽을 수 없도록 하는 것이다. 태그를 탐색하는 방식이 이진 탐색 트리 기법이라면, 모든 질의에 대해 블로커 태그가 응답하므로 리더는 모든 태그를 검색하는 결과가 되고 이것은 리더가 원하는 태그를 찾을 수 없는 것과 마찬가지이다. 이러한 블로커 태그는 일반 태그와 함께 있을 때 태그가 보호되는 것이고, 다시 정상적으로 4사용하기 위해서는 블로커 태그를 제거하면 일반 태그를 판독할 수 있게 된다.

2.2.6 재암호화 방식[4]

재암호화(Re-encryption) 방식은 ElGamel 공개키 암호화 알고리듬을 기반으로 하고 있으며, 유로화 지폐에 RFID 태그를 내장하기 위해 사용된다. 이 방식은 태그가 전송하는 ID의 암호문 c를 임의의 난수 r과 공개키를 이용하여 새로운 암호문(c′)으로 변형하는 것이다. 즉, r에 의해 ID에 대한 여러 개의 암호문이 생성가능하기 때문에 사용자의 추적이 불가능하다. 이 방식은 외부(즉, 리더나 백엔드 시스템)에서 고유 ID를 암호화하여 태그에 저장하기 때문에 공개키를 알고 있는 믿을만한 외부 시스템이 필요한 부담이 있다.

2.2.7 대칭형 암호화 기반 인증 방식[7]

M.Feldhofer 등은 그림 4(a)에 나와있는 것과 같이 대칭형 암호화 알고리듬인 AES를 RFID에 내장하여 리더가 보낸 난수를 태그가 AES로 암호화하여 인증하는 방식을 구현하였다. 또, 이보다 진보된 상호인증 방식도 제안하고 있으나 저가의 수동형 태그에 기반하고 있으며, 13.56MHz 대역에 초점을 맞추고 있어 비접촉식 스마트카드와 유사한 통신환경을 배경으로 하고 있다.

2.2.8 개방형 스마트카드 인증 방식[10]

개방형 스마트카드는 카드 메모리에 저장되는 내용물(프로그램과 데이터)의 추가/삭제가 가능한 스마트카드로, 카드와 리더 사이에 3-DES 암호화 알고리듬에 기반한 보안채널 프로토콜을 통해 상호인증을 수행하여 불특정 다수가 카드 내용물을 함부로 변경하는 것을 방지하고 있다. 이 인증방식은 GOP(Global Open Platform)에 의해 규정되었으며 현재 국제적인 산업규격으로 대부분의 개방형 스마트카드에 채택되고 있다. 그림 4(b)에 나타나있듯이, 먼저 리더가 카드로 사용할 키 인덱스 IK와 자신이 생성한 난수 rR을 보내면, 카드는 난수 rC를 생성하고 리더의 난수와 조합하여 세션키를 생성한다. 생성된 세션키로 rR과 rC에 대한 암호화를 수행하여 그 최상위 일부만을 인증값 c1으로 리더기에 응답하면, 리더는 카드의 난수와 ID를 이용해 동일한 세션키를 생성하고 c1을 검증한 다음, 카드에 제시할 c2와 MAC(Massage Authentication code)을 생성하여 카드로 전달한다. 카드는 c2와 MAC을 세션키로 검증하고, 올바르면 성공코드를 응답하는 것으로 상호인증을 완료하게 된다.

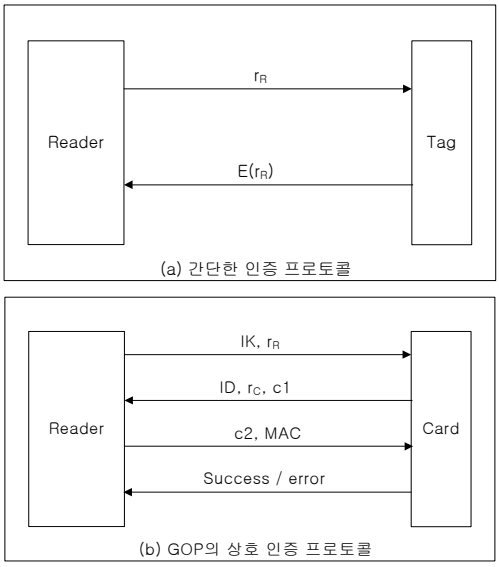

그림 4 암호화 알고리듬을 이용한 인증방식
Fig. 4 Authentication methods

3. 제안 프로토콜

위 2장에서 살펴본 다양한 보안 방식은 저가형 태그에 구현하기 위해 계산량과 간단한 구조를 우선적으로 고려하고 있다. GOP 인증 방식의 경우에는 스마트카드에 3-DES 암호화 처리 프로세서가 내장되기 때문에 보다 강력하고 빠르게 처리할 수 있지만, 상호 인증을 위한 세션키를 생성해야하는 등의 절차로 인해 RFID에 적용하기에는 처리 시간이 너무 많이 소요되는 단점이 있다. 본 장에서 제안하는 보안 프로토콜은 고기능 태그를 위한 것으로 스마트카드보다는 간단하지만 저가형 태그에 비해서는 강력한 보안 성능을 제공하면서 ID를 부여하는 것을 목표로 한다. 이 방식은 리더 측에서 태그에게 ID를 부여할 때 암호화된 ID를 전송하기 때문에 공격자는 태그의 이전 ID와 부여되는 ID 간의 상관 관계를 파악할 수 없어 ID를 이용한 위치 추적이 불가능하다. 백엔드 서버는 발급할 ID들을 미리 생성하여 두었다가 새로운 ID를 할당할 필요가 있을 때마다 이를 부여하게 된다. 하나의 태그에 대한 원래의 ID와 새로 부여된 ID의 상관관계와 변경 이력은 모두 백엔드 서버가 관리하므로 오로지 백엔드 서버만이 위치추적에 필요한 정보를 가지게 된다. 부여된 ID는 일반적인 질의(query)의 응답으로 사용되며, 더 이상 필요가 없거나 일정 질의 횟수가 넘어가면 파기되고 새로운 ID를 부여받도록 할 수도 있다. 따라서, 공격자가 동일한 ID를 추적하고 있다 하더라도 얼마안가 새로운 ID로 변경되기 때문에 위치 추적이 불가능해진다.

3.1 준비 단계

그림 5와 같이 태그는 사용되기 전에 발급자가 미리 보안에 사용할 키(Key1, Key2, ... Keyn)들과 그 키를 나타내는 키 인덱스(IK1, IK2, ... IKm)를 태그에 저장하며, 백엔드 서버의 데이터베이스에도 동일한 키들과 그 인덱스를 저장하여 둔다. 이 때 키의 개수는 n < m으로 DB는 많은 수의 키들을 준비하고, 개별 태그에는 3~5개 정도의 키를 부여한다. 또한 서버는 태그에 별 태 할당할 ID들(Dynamic ID1, ... Dynamic IDx)을 미리 준비하여 둔다. 태그의 Fail counter는 외부로부터의 명령이 완성되지 않거나 암호화 데이터 검증에 실패한 경우 증가하는 카운터로 외부 공격을 방지하는데 사용된다. 태그는 자신의 고유 ID(fixed ID)와 동적 ID를 따로 저장하고 있으며, 모드에 따라 고정 ID를 사용하거나 동적 ID를 사용하게 된다. 본 단계에서 리더는 충돌방지 알고리듬을 이용하여 태그를 인식한다. ISO 18000-6[12]에서는 Type A, B, C 태그에 각각 슬롯 ALOHA 프로토콜과 이진 트리 프로토콜, 슬롯 랜덤(Slotted random) 프로토콜 등을 사용하도록 규정하고 있는데, 어떤 프로토콜을 사용하건 간에 리더는 자신의 통신 영역 내에 있는 태그들을 모두 파악하게 되며, 그 결과로 선택된 태그는 자신의 ID를 리더로 응답하게 된다. 이 과정에서 태그는 자신이 가진 동적 ID를 계속 사용할지, 아니면 새로운 ID를 부여 받을지에 대해 결정하고 새로운 ID를 부여받기로 결정하였다면, 다음 절의 프로토콜을 통해 ID를 부여받는다고 가정한다. 따라서, 리더가 태그를 인식하는 과정에서 태그가 자신의 ID를 변경하기를 리더에 요청하게 되면 리더가 새로운 ID를 부여하게 된다. 현재의 ID와 새로 부여되는 ID 간에는 코드 체계만 동일하며, 일련 번호 등은 랜덤하게 생성하여 사용하게 되면 그것을 생성하고 관리하는 백엔드 서버 이외에는 상관 관계를 알 수 없게 된다. 예를 들어 ID가 EPC(Electrical Product Code) 체계라면, 64비트의 ID 중 마지막 24 비트가 일련 번호로 사용된다[13]. 이 일련 번호를 백엔드 서버가 체계적으로 고정 ID와 동적 ID에 할당하여 관리한다면 여기서 제안하는 프로토콜을 통한 ID 부여가 가능할 것이다. 태그가 고정 ID와 동적 ID중 어떤 ID를 사용할지 결정하는 방법과 동적 ID의 갱신이 어떤 주기나 계기에 의해서 이루어질 것인지는 본 제안에서 다루지 않기로 한다. 본 제안은 단지 동적 ID를 갱신하게 되었을 때, 어떤 방법으로 할당하게 되는지에 초점을 맞추고 있다.

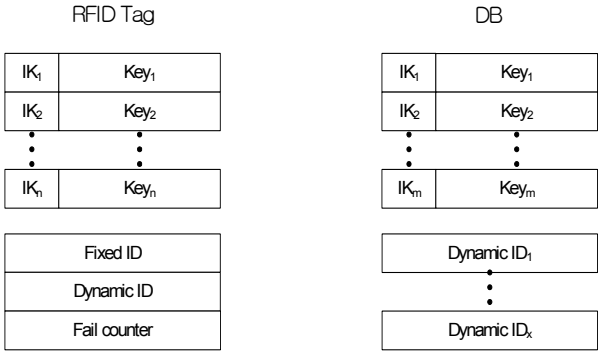

그림 5 태그와 데이터베이스 저장 정보
Fig. 5 Data stored in Tag and DB

3.2 ID 할당 단계

그림 6에 할당 프로토콜에 대한 흐름도가 나타나 있다. ①과 ③에 대해 GenerateRandom과 ChnageID 명령이라 이름 붙였으며, 이에 대한 자세한 데이터 구조는 Ⅳ장에서 설명한다.

① 리더는 태그 인식 과정에서 ID 변경 요청을 받으면 새로 부여할 ID를 준비하고, ID를 변경하고자 하는 태그에게 GenerateRandom 명령을 보낸다. 여기에는 태그의 ID를 함께 전송하여 이 명령을 받은 태그 중에 자신의 현재 ID와 일치하는 태그만 이 명령에 응답하게 된다.

② 태그는 난수 R을 생성하여 이를 응답한다.

③ 리더 혹은 백엔드 시스템은 태그의 현재 ID로부터 그 태그에 저장된 키 셋(IK1....IKn)을 알 수 있으며, 그 키 중에서 하나를 임의로 선택하여 암호화하여 EID를 생성하고, 그에 따른 인증값 M1을 생성한다. EID를 생성함에 있어 단순히 ID만을 암호화하지 않고, ID와 R의 XOR 연산 결과를 암호화한 이유는, 스푸핑 공격과 재생공격을 막기 위해서이다. 계산이 끝나면, ChangeID라는 명령을 통해 태그로 암호화에 사용된 키의 인덱스 IK, EID와 M1을 전송한다. 여기서 E() 함수는 T-DES나 SEED와 같은 대칭형 암호화 연산이며, MAC() 함수는 E() 함수를 CBC(Cipher Block Chaining) 모드로 연산하여 그 최종 결과의 최상위 일부분만을 취하는 함수이다.

$$EID = E(ID \text{ xor } R) \quad (1)$$

$$M1 = MAC(ID) \quad (2)$$

④ 태그는 IK가 가리키고 있는 키를 사용하여 전달된 EID를 복호화하고 자신이 생성한 R로 XOR 연산을 수행하여 ID를 추출한 후 인증값을 계산하고 전송되어온 M1과 비교한다. 동일한 인증값을 가지면 자신의 메모리 영역에 이 ID를 저장한다. 성공적으로 저장이 완료되면 M2를 생성하여 리더기에 응답으로 보낸다. 여기서 | 기호는 데이터 연접 연산을 나타낸다.

$$M2 = MAC(R \mid ID) \quad (3)$$

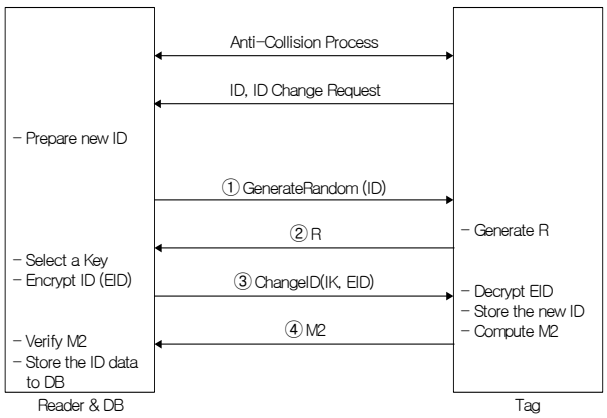

그림 6 제안한 동적 ID 할당 프로토콜의 흐름도
Fig. 6 Dynamic ID allocation Protocol

공격자가 위 과정을 반복하여 키 값을 알아내려는 시도를 하는 경우를 방지하기 위해, 암호화된 ID를 받지 못하거나 인증값 M2의 검증이 연속으로 실패하는 경우에는 카운터(Fail counter)가 증가하며, 이 카운터가 일정 한도를 넘어서면 태그는 스스로 잠김 모드로 들어가 특별한 인증 절차를 거치지 않는 한 외부에 응답을 하지 않게 된다. 리더는 전달된 M2를 검증하고 ID 부여가 완료되었다는 정보를 DB에 저장한다. 따라서, 리더와 DB를 가지는 벡엔드 서버는 하나의 태그에 대해 그 태그의 ID가 언제 어떻게 부여되어 변경되었는지에 대한 이력을 모두 저장하기 때문에 특정 태그를 추적할 수 있는 유일한 주체이다.

4. 제안 프로토콜의 데이터 구조

여기서는 3장의 프로토콜을 실제 RFID 통신 프로토콜(ISO 18000-6의 Type C)에 적용할 경우에 어떠한 데이터 구조를 이루고 있어야 하는지를 설명한다. 서론에서 설명하였듯이 ISO 18000-6 Type C는 860MHz - 960MHz의 통신 대역을 가지는 태그 규격으로 클래스 I의 Generation 2에 해당하여 현재 시점에서 참조할 수 있는 가장 최신의 국제 규격이다. 제안 프로토콜은 고기능 RFID 시스템을 위한 것이지만 현재 시점에서 참조할 수 있는 국제 규격은 ISO 18000 시리즈 밖에 없으므로 그 규격 중 가장 진보된 Part 6의 Type C 규격을 참조하여 제안 프로토콜의 명령어를 구성하였다. 리더와 태그 간 명령-응답의 일반적인 형식은 먼저 명령의 경우 Frame-Sync로 시작하여 명령 코드와 명령을 수행하기 위한 데이터, 그리고 앞의 데이터에 대한 CRC(Cyclic-Redundancy Check)로 구성된다. 응답의 경우에는 Preamble로 시작하여 응답 데이터와 그에 대한 CRC로 구성된다. Frame-Sync와 Preamble, 그리고 CRC의 형식은 모두 규격에 명시되어 있는 그대로 사용한다.

4.1 GenerateRandom 명령의 데이터 구조

그림 7의 (a), (b)와 같이 GenerateRandom 명령어와 그에 대한 응답을 구성하였다. Frame-Sync는 리더에서 태그로 명령을 전송하기 시작한다는 것을 알리는 일종의 헤더이다. 16비트의 명령 코드는 규격에 명시된 코드 중에서 맞춤형 명령(custom command)으로 사용할 수 있는 부분에 할당하였다. 명령 코드 다음에는 64 비트 길이의 태그 ID가 뒤따르며, 마지막으로 FS와 CRC 사이에 있는 Command, ID에 대한 16 비트 길이의 CRC를 추가함으로써 통신 오류에 대비한다. 이 명령을 받은 태그의 응답은 Preamble을 시작으로 64 비트 길이의 난수 R과 R에 대한 16 비트 CRC로 구성된다.

4.2 ChnageID 명령의 데이터 구조

ChangeID 명령은 그림 7의 (c), (d)에 나타나 있듯이 Frame-Sync로 시작하여 16 비트의 명령 코드, 8 비트로 이루어진 키 인덱스(IK), 64 비트 길이의 암호화된 ID(EID), 32 비트의 인증값(M1)으로 이루어지며, 마지막으로 FS 이후의 모든 데이터에 대한 CRC 값이 추가된다. 이에 대한 응답은 32 비트 길이의 인증값(M2)과 CRC이다. 명령 코드는 위 4.1 절에서 부여한 코드와 인접하도록 부여하였으며, M1과 M2가 32 비트인 것은 암호화 결과가 64 비트 길이이고 그 중에서 상위 32 비트를 인증값으로 사용한다고 가정하여 할당한 것이다.

FS	Command (16 bit)	ID (64 bit)	CRC (16 bit)
Frame-Sync	11100000 00000001	ID Value	CRC Value

(a) GenerateRandom 명령

P	R (64 bit)	CRC (16 bit)
Preamble	Random Number	CRC Value

(b) GenerateRandom 명령에 대한 응답

FS	Command (16 bit)	IK (8 bit)	EID (64 bit)	M1 (32 bit)	CRC (16 bit)
Frame-Sync	11100000 00000010	Key Index	Encrypted ID	MAC 1	CRC Value

(c) ChangeID 명령

P	M2 (32 bit)	CRC (16 bit)
Preamble	MAC 2	CRC Value

(d) ChangeID 명령에 대한 응답

그림 7 제안 프로토콜의 명령어 데이터 구조
Fig. 7 Command data structure of protocol

5. 제안 프로토콜의 안전성

여기서는 2.2절에서 살펴본 위협에 대해 제안한 프로토콜이 안전함을 설명한다.

(1) 도청에 대한 안전성 : 공격자가 태그의 응답 ②를 도청하여 얻을 수 있는 것은 난수 R 뿐이다. 리더의 전송 명령 ③은 키 인덱스(IK)와 암호화된 ID(EID), 그리고 인증값(M1)이 전달되므로 도청자는 새로 부여되는 ID를 전혀 알 수 없다. 암호화되지 않은 키 인덱스만을 이용하여 해독할 수 있는 정보는 거의 없으며, 암호화 키가 여러 개의 키 셋 중에서 임의로 선택되어 사용되기 때문에 장시간에 걸친 도청을 하여도 암호화된 ID를 해독하기에 충분한 데이터를 수집할 수 없다.

(2) 위치 추적 방지 : 본 프로토콜의 수행 중에 태그의 ID는 전혀 전송되지 않으며. 그 용도가 동적으로 새로운 ID를 부여하는 것이다. 따라서, 백엔드 서버 이외에는 이전 ID와 새로운 ID와의 상관관계는 물론 ID 부여 이력도 알 수 없으므로 위치 추적은 불가능하다. 하지만, 최초에 태그를 인식하기 위해 리더와 태그 간의 충돌방지 알고리듬을 통하여 태그를 인식하는 단계에서 현재의 ID가 노출되게 되는데, 태그가 현재의 ID를 일정 기간동안 변경하지 않고 유지하는 경우, 그 기간동안에는 ID를 통한 위치 추적이 가능할 수도 있다. 그러나, 일단 ID가 변경되면 추적하던 ID와 변경된 ID 사이의 관계를 알 수 없기 때문에 위치 추적의 의미가 없어지게 된다.

(3) 스푸핑 방지 : 본 프로토콜은 상호 인증을 기반으로 하고 있기 때문에 상대방과 동일한 키를 가지고 있지 않고서는 상대방을 속일 수 없다. 공격자가 태그인척 행동을 한다면 ③을 받고 EID를 복호화하여 ID를 복구하여야 하는데, 키를 모르고 있어 불가능하다. 또, 공격자가 리더인척 행동을 한다면, ②를 수신한 후 ID를 암호화하고 인증값을 생성하여 전송해야 하는데, 이 또한 키를 모르고 있으면 불가능하다. 공격자가 리더인척 ①을 발신하고 태그의 ② 응답을 받아도 얻을 수 있는 것은 태그의 난수 밖에 없다. 태그는 내부에 카운터(Fail counter)를 가지고 있어서 ②를 전송하였음에도 불구하고 ③ 응답이 없는 경우와 ③을 받았지만 인증값이 틀리면 카운터가 증가하고, 이 카운터가 누적되어 일정 한도를 넘어서는 경우 잠김 모드로 전환되어 외부에 응답하지 않게 된다. 이 카운터는 연속적인 경우에만 증가하며 성공적으로 이루어지는 경우에는 다시 0 값으로 되돌려진다. 따라서 공격자가 연속적인 공격을 시도하는 경우 태그는 잠김 모드로 전환되어 더 이상 응답하지 않게 된다. 잠겨진 태그에 대한 잠김 해제는 추가적인 보안 명령을 통해 이루어져야 할 것이다.

(4) 재생 공격 방지 : 공격자가 ②를 도청하였다가 정당한 태그인 척 리더에 전송하는 경우에도 ③을 받은 후 암호화 키를 알지는 못하기 때문에 ID를 추출해 낼 수 없으며, ④를 생성할 수 없거나 틀린 정보를 전송하게 되어 백엔드 측에서 감지할 수 있다. 공격자가 ③을 도청하였다가 정당한 리더인척 다시 태그에 전송하여도 ③의 EID를 연산하는데 태그의 난수 R이 포함되어 있기 때문에 ② 단계에서 태그가 전송한 R과 도청한 ③에 포함된 R은 다르므로 태그의 인증 과정에서 드러나게 된다.

표 1은 기존 보안 방식과 제안된 프로토콜의 비교를 나타내고 있다[14,15]. 저가형 태그를 위한 해쉬 기반 프로토콜들과 개방형 스마트카드를 위한 GOP 프로토콜과 비교해볼 때, 본 프로토콜은 상호인증이 가능하면서 ID를 동적으로 부여할 수 있는 것이 큰 차이점이며, 대칭형 암호화 알고리듬을 기반으로 하면서도 스마트카드보다는 가벼운 프로토콜을 제안하고 있다.

표 1 기존 방식과 제안 프로토콜의 비교
Table 1 Comparison of protocols

	확장된 해쉬-락	해쉬 체인	재암호화	GOP 프로토콜	제안 프로토콜
도청	안전	안전	안전	안전	안전
위치트래킹	안전	안전	안전	-	안전
스푸핑	취약	안전	안전	안전	안전
재생공격	안전	안전	안전	안전	안전
사용 ID	고정	고정	고정	고정	가변
적용 알고리듬	해쉬	해쉬	RSA	3-DES	대칭형 암호화 알고리듬
상호인증	X	X	X	O	O

6. 결 론

RFID의 보안 문제를 해결하기 위해 다양한 프로토콜이 제안되고 있으나, 대부분 저가형 RFID 태그를 대상으로 하고 있다. 본 논문에서는 고기능 RFID를 대상으로 상호인증을 통하여 안전하게 동적인 ID를 부여하는 프로토콜을 제안하였다. 이 프로토콜은 저가형 태그보다는 강력한 보안을 제공하면서, 스마트카드의 상호 인증 방식보다는 간단하고 동시에 ID 부여가 가능한 기능을 목표로 하였다. 또한, 제안 프로토콜이 현재의 국제 규격에 어떻게 활용될 수 있는지 보여주기 위해 ISO 18000 Part 6 Type C 규격에 맞추어 데이터 구조를 구성하였다. 이러한 상호인증 기능을 가지는 고기능 RFID는 향후 고가의 물품을 안전하게 관리하는데 이용될 수 있으며, 센서를 내장하여 유비쿼터스 환경의 센서 네트웍을 구축

하는 근간으로 활용될 수 있다[16]. 향후에는 동적 ID의 갱신이 어떤 주기나 계기에 의해서 이루어질 것인지를 결정하는 방식과 백엔드 서버에서의 키와 ID 관리 방법, 그리고 보다 향상된 보안성을 가지는 프로토콜에 대한 연구가 진행될 예정이다.

참 고 문 헌

[1] S.E.Sarma, S.A.Weis, and D.W.Engels, “RFID ystems, Security & Privacy Implications", White Paper, uto-ID Center, MIT, 2002.

[2] S.A.Weis, S.Sarma, R.Rivest, and D.Engels, "Security nd Privacy Aspect of Low-Cost Radio Frequency dentification Systems", Springer-Verlag, First nternational Conference on Security in Pervasive omputing, LNCS 2802, pp.201-212, 2004.

[3] Auto-ID Center, "860-930MHz Class I Radio requency Identification Tag Radio Frequency & Logical ommunication Interface Specification Candidate ecommendation Version 1.0.1", Technical Report, uto-ID Center, MIT, 2002.

[4] A.Juels, .R.Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes", Financial Cryptography '03, LNCS 2742, pp.103-121, 2003.

[5] M.Ohkubo, K.Suzuki, and S.Kinoshita, "A Cryptographic Approach to "Privacy-Frendly" Tag", RFID Privacy Workshop, 2003.

[6] A.Juels, R.L.Rivest, and M.Szydlo, "The Blocker Tag : Selective Blocking of RFID tags for Consumer Privacy", 10th ACM Conference on Computer and Communications Security, CCS 2003, pp.103-111, 2003.

[7] M.Feldhofer, "A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags", MELECON 2004 IEEE Proceedings, pp.759-762, 2004.

[8]M.Feldhofer, S.Dominikus, J.Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm", Springer, In Conference of Cryptographic Hardware and Embeded Systems 2004 Proceedings, pp.357-370, 2004.

[9] S.Sarma, D.W.Engels, “On the Future of RFID Tags and Protocols", Technical Report, Auto-ID Center, MIT, 2003.

[10] GlobalPlatform, "Card Specification Version 2.1.1", GlobalPlatform, 2003.

[11] S.A.Weis, "Security and Privacy in Radio-Frequency Identification Devices", MIT, Masters thesis, 2003.,

[12] ISO/IEC, "Information technology - Radio-frequency identification for item management - Part 6 : Parameters for air interface communications at 860 MHz to 960 MHz", International Standard, ISO, 2005.

[13] D.Engels, “The Use of the Electronic Product Code", Technical Report, Auto-ID Center, MIT, 2003.

[14] 강전일, 박주성, 양대헌, “RFID 시스템에서의 프라이버시 보호기술”, 정보보호학회지 제14권 제6호, pp. 28-36, 2004.

[15] 유성호, 김기현, 황용호, 이필중, “상태기반 RFID 인증 프로토콜”, 정보보호학회논문지 제14권 제5호, pp. 57-68, 2004.

[16] S.Haller, S.Hodges,, “The Need for a Universal Smart Sensor Network", Auto-ID Center, White Paper, MIT, 2002.

저 자 소 개

박 진 성 (朴 鎭 成)

1972년 5월 22일생. 1995년 한양대 제어계측공학과 졸업. 1997년 한양대 제어계측공학과 졸업(석사). 2000년 한양대 제어계측공학 박사과정 수료. 2000년～2002년 (주)마니네트웍 개발2팀 팀장. 2003년～2004년 노틸러스효성(주) 개발팀 과장. 2005년～현재 (주)CEN 연구소장

Tel : 017-228-8320
Fax : 031-400-3889
E-mail : pjs72@asic.hanyang.ac.kr

최 명 렬 (崔 明 烈)

1960년 9월 26일생. 1983년 한양대 전자공학과 졸업. 1991년 미시간 주립대학교 컴퓨터공학 졸업(박사). 1991년 3월～10월 생산기술연구원 전자정보실용화센터 조교수. 1991년 11월～1992년 8월 생산기술연구원 산하 전자부품종합기술연구소 선임연구원. 1992년～현재 한양대학교 전자컴퓨터공학부 교수

Tel : 031-400-5214
Fax : 031-400-3889
E-mail : choimy@asic.hanyang.ac.kr