韓國컴퓨터情報學會 論文誌
第15卷 第8號, 2010. 8.

2010-15-8-3-6

RFID 시스템에서 프라이버시 보호를 위한 보안기법 설계

오 기 욱*, 박 미 옥**

A Secure Technique Design for Privacy Protection in RFID System

Gi Oug Oh*, Mi-Og Park**

요 약

RFID 기술은 자동인식 및 데이터획득 기술로서 유비쿼터스 컴퓨팅에 필요한 기술이다. RFID는 저비용 무선인식 메모리 태그를 사용하며, 물리적 비접촉 특성에 의한 사용의 편리성과 유지 우수성으로 사용이 확대되어가고 있다. 그러나 RFID는 RF 신호를 이용하기 때문에 태그와 리더간의 불법적인 정보획득이 가능하며, 획득한 정보를 위치추적과 프라이버시의 침해를 목적으로 사용할 수 있다. 본 논문에서는 불법적인 정보획득으로 인한 사용자의 위치추적과 프라이버시의 침해를 보호할 수 있는 보안기법을 제안한다. 본고에서 제안하는 보안기법은, Gray Code를 이용하여 실제 태그의 계산용량을 줄였을 뿐만 아니라, 태그에서 리더로 전송되는 정보가 고정되어 있지 않으므로 악의적인 공격자의 트래킹이 불가능하며, 악의적인 방법을 통해 태그의 실제정보를 획득하더라도 실제 정보가 아닌 암호화된 정보가 노출되기에 다른 보호기법보다 간단하고 안전하게 사용자 프라이버시를 보호할 수 있다.

Abstract

RFID (Radio Frequency IDentification) technology, automatic identification and data capture technologies in ubiquitous computing is an essential skill. Low-cost Radio Frequency Identification tags using memory and no physical contact due to the ease of use and maintenance of excellence are going to use expanded. However, it is possible to the illegal acquisition of the information between RFID tags and readers because RFID uses the RF signal, and the obtained information can be used for the purpose of location tracking and invasion of privacy. In this paper, we proposed the security scheme to protect against the illegal user location tracking and invasion of privacy. The security scheme proposed in this paper, using Gray Code and reduced the capacity of the calculation of the actual tags, However, it is impossible for the malicious attacker to track information because tag information transmitted from the reader is not fixed. Therefore, even if the tags information is obtained by a malicious way, our scheme provides more simple and safe user privacy than any other protection methods to protect user privacy, because not actual information but encrypted information is becoming exposed.

▸ Keyword : Privacy, Tracking, Gray Code, Hash, RFID protocol

• 제1저자 : 오기욱 교신저자 : 박미옥
• 투고일 : 2010. 05. 13, 심사일 : 2010. 06. 01, 게재확정일 : 2010. 06. 13.
* 안양대학교 교양학부 조교수 ** 성결대학교 컴퓨터공학부 전임강사

Ⅰ. 서 론

RFID 기술은 자동인식 및 데이터획득(Automatic Identification and Data Capture)의 근본 기술이며, 바코드를 대체하여 객체 식별에 널리 사용되는 유비쿼터스 컴퓨팅에 필요한 기술이다[1]. 바코드 대용으로 사용하는 RFID 시스템은 바코드보다 많은 저장능력을 가지고 있고, 저비용 무선인식 메모리 태그를 사용하며, 물리적 접촉 없이 사용하기에 사용 편리성과 유지 우수성으로 인해 사용이 확대되어가고 있다. 그러나 RFID는 RF 신호를 이용하기 때문에 태그와 리더간의 불법적인 정보획득이 가능하며, 획득한 정보를 위치추적과 프라이버시의 침해를 목적으로 사용 할 수 있다.

RFID 시스템에서 사용하는 태그의 종류는 능동형(Active) 태그와 준 수동형(Semi-Passive) 태그 그리고 수동형(Passive) 태그로 분류한다[2]. 능동형 태그는 자체 전원을 가지고 있고, 보다 복잡한 보안 알고리즘을 적용하고 있으며, 전파 전달 범위도 가장 넓다. 준 수동형 태그도 자체 전원을 갖고 있으며, 전파 전달 범위는 액티브 태그보다는 짧지만 수동형 태그와 같은 방식을 이용한다. 그러나 수동형 태그는 리더로부터 전원을 받으며, 전파전달 범위는 가장 짧다. 따라서 수동형 태그는 바코드 대용으로 널리 사용하며, 값이 매우 싸기 때문에 보다 복잡한 보안 알고리즘을 적용하기 어렵다[3].

RFID 시스템에서 발생할 수 있는 공격으로는 태그와 리더간의 도청이며, 도청된 통신내용 분석하는 방법과 태그의 위치변화를 추적하는 위치 트래킹, 정당하지 않는 개체를 속여 인증과정을 통과하는 위장(Spoofing) 및 정상적으로 RFID 시스템이 작동하지 못하도록 하는 서비스 거부 그리고 태그와 리더간의 일부 메시지 유실과 같은 방법이 있다.

RFID 프라이버시에 대한 연구 중 대표적인 것이 Kill 명령을 이용하는 방식과 해쉬락 프로토콜, 확장된 해쉬락 프로토콜 그리고 해쉬 체인에 기반한 방식과 본 저자가 제안한 그레이코드를 이용한 RFDI 보안 프로토콜과 시스템 설계등 많은 연구가 있다[4,5,6,7]. 그러나 기존의 연구들의 단점들은 첫째로 태그에서 리더로 전송되는 정보가 고정되어 전송되므로 트래킹을 할 수 있으며, 둘째로 태그의 인증에 다른부분에서 많은 계산이 필요하며, 셋째로 현실적으로 구현하기 힘들다.

RFID 시스템은 RF 통신을 사용하는 특성 때문에 태그의 정보를 쉽게 획득할 수 있고 실제로 허가 받지 않고 정보 획득이 가능하다. 따라서 리더와 태그는 암호화된 정보 교환이 필요하기에 태그와 리더간의 교환되는 정보가 누출되더라도 비 인가자들이 사용하지 못하도록 암호화 되어있어야 한다.

본 논문의 제안 시스템은 Gray Code를 이용하여 실제 태그의 계산용량을 줄임에도 불구하고, 다른 보호기법보다 간단하고 안전하게 사용자 프라이버시를 보호할 수 있다. 태그는 많은 계산과 정보를 담고 있지 못하기에 태그의 계산을 간단하게 하면서 많은 계산은 후방시스템에서 하도록 하였으며, Gray Code를 이용하여 프라이버시를 보호하며 실제 정보를 간단하고 안전하게 획득할 수 있도록 하였다.

제안 시스템은 태그에서 리더로 전송되는 정보가 고정되어 있지 않으므로 악의적인 공격자의 트래킹이 불가능하며, 악의적인 방법을 통해 태그의 실제정보를 획득하더라도 실제 정보가 아닌 암호화된 정보가 노출되기에 사용자의 프라이버시를 보호한다.

Ⅱ. 관련연구

1947년 벨 연구소에 의해서 개발된 그레이 코드는 Frank Gray에 의해 컴퓨터에 사용하도록 개발되었다. 연속되는 일련의 숫자비트를 하나의 비트만 변화하여 새로운 코드를 생성하며, 입력코드로 사용하면 오차가 적어지는 그레이 코드의 특징과 구조를 RFID 시스템의 보안 프로토콜로 이용하여 RFID 시스템에서 프라이버시 보호를 위한 보안 프로토콜로 이용한다.

RFID 시스템에서 프라이버시를 해결하기 위한 연구로는 물리적인 보호기법과 암호학적 보호기법으로 나눈다. 물리적 보호기법으로는 Kill Tag, Faraday cage, active jamming, Blocker Tag와 같은 물리적인 형태를 취함으로 프라이버시를 보호하는 기법을 말한다. 그것에 반하여 암호학적, 즉 소프트웨어적인 보호 기법으로는 해쉬락, 확장된 해쉬락, 해쉬 기반 아이디 번형 프로토콜, 해쉬체인 프로토콜, 재암호화, 경량화 암호 프로토콜등이 있다[8, 9, 10].

2.1 RFID 시스템 기본구조

RFID 시스템의 기본 구조는 그림 1과 같이 태그와 리더 그리고 후위시스템(Back-End System)으로 구성되어 있다[1]. 후위 시스템은 데이터처리 시스템과 데이터베이스를 가진 시스템을 통칭한다. 태그는 바코드를 대신하여 실제 상품의 정보를 담고 있는 장치로 리더가 안테나를 통해 전원을 공급하고 태그의 정보를 요구하면 리더는 그 요구에 자신의 정보를 태그에게 전달한다. 리더는 안테나를 통해 태그로부터 획득한 정보와 리더가 갖는 검증 코드를 후위 시스템으로 보낸다. 리더로부터 전달받은 정보를 후위시스템의 데이터베이스와 데이터 처리 시스템을 통해 획득한 정보를 다시 리더로 전송하고 리더는 가공 처리된 해당 정보를 태그로 전송한다.

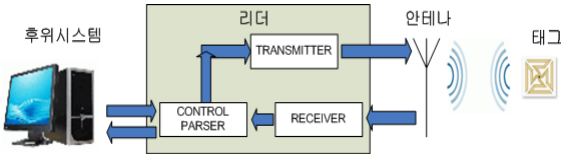

그림 1. RFID 시스템 구조
Figure 1. RFID System Structure

태그는 전원의 공급에 따라 수동형 태그와 준능동형 태그 그리고 능동형 태그로 구분하며, 자체 전원을 가지고 있으며, 많은 계산을 할 수 있고 값이 비싼 단점을 갖는 태그가 능동형태그이다.

2.2 그레이코드(Gray Code)

Emile Baudot에 의해 개발된 그레이코드를 Frank Gray는 컴퓨터에 적합하게 사용하도록 개발하였다[4,11]. 그레이코드는 이웃한 이진수와 해밍거리(Hamming Distance)가 항상 1인 코드이며, 대표적인 것이 BRGC(Binary Reflected Gray Code)로 n 비트의 코드는 n! 만큼 존재한다. 그레이 코드의 함수는 gc : N → seq{0,1} 로 나타내며, 속성은 아래와 같다.

① 2진수로는 gc 0 = ⟨0⟩ , gc 1 = ⟨1⟩ 로 나타내고 gc n = gc(n / 2) ⧺ ⟨d⟩ d 는 0 혹은 1 로 표현하거나 fr gc n = gc(n / 2) 로 표시한다.

② gc(n) 과 gc(n+1)은 모든 n 에 대해서 위치가 한 개가 다르다.

①의 속성은 이진수와 그레이코드 모두에 적용할 수 있으나 ②의 속성은 그레이코드 속성에만 적용한다. 그레이 코드로의 변환은 처음 숫자가 "0" 인 경우에 무조건 "0"으로 시작하며, "1"인 경우는 "1"로 시작한다. 따라서 처음 숫자 n 과 다음숫자 n+1을 xor하여 계산한다. 이와 같이 그레이 코드는 이해와 사용이 쉽다. 즉, 한 번에 단일 출력이 변환되는 절약적인 형태(Power saving)를 갖고 있다. 또 그레이 코드는 xor를 이용하기 때문에 인가된 사용자는 쉽게 입력 값을 찾을 수 있는 장점을 가지고 있다.

그레이 코드의 계산 알고리즘 방식은 되부름(Recursive) 방법과 반복(iterative)방법이 있으며, 알고리즘도 단순하다. 아래 그림은 되부름(Recursive)방법의 알고리즘이다.

```
def prepend(prefix, array)
    array.collect{|item|prefix +item}
end
def grayCodes(bits)
    if (bits == 1) ["0", "1"]
    else
    begin
        prepend("0", grayCodes(bits-1)) +1
        prepend("1", grayCodes(bits-1)).reverse
    end
end
puts grayCode(4)
```

그림 2. 되부름 그레이코드 생성 알고리즘
Figure 2. Recursive Gray Code Generation Algorithm

2.3 해쉬락과 확장된 해쉬락

해쉬락 프로토콜은 태그와 리더간의 통신이 되면 "Locked" 상태를 유지하면서 태그의 metaID를 리더에게 전달한다. 이때 다른 태그의 정보를 리더가 읽지 못하고 오직 "Locked" 걸린 태그의 metaID를 획득한다. metaID = hash(key)이면, 리더는 metaID를 이용하여 데이터베이스에서 실제 ID를 전송받으며 태그는 "Unlocked"상태를 유지한다. 단방향 해쉬함수의 역함수 계산의 어려운 점을 기반한 해쉬락 프로토콜은 "Unlocked" 상태에서만 실제 ID를 전송하기에 사용자 데이터의 프라이버시를 보호하지만 위치 프라이버시와 위장(Spoofing)을 방지하지 못하고 재전송공격에 취약하며 사용자 추적의 위험이 존재한다[12].

확장된 해쉬락 프로토콜은 해쉬락 기법에서 난수발생기(PRNG)를 이용하여 랜덤변수를 이용하여 사용자의 추적을 방지하는 프로토콜로써, 랜덤화된 해쉬락 프로토콜이라고도 한다. 태그를 "lock" 상태를 만들 때는 프로토콜이 필요 없으나 "Unlocked"상태로 전이할 때는 프로토콜이 필요하다. 실제 ID 전달 과정을 보면, 리더가 태그에게 질의를 보내면 태그는 랜덤한 수 R 을 생성하고 hash(ID || R)값을 계산한다. 태그는 (R, hash(ID || R))을 리더에게 전송하고, 리더는 ID_i 값에 대해 hash(ID_i || R)을 계산한다. hash(ID || R) = hash(ID_i || R) 한 값을 찾으면, 리더는 태그에게 ID_i를 전송하고, ID_i와 ID가 일치하면 태그는 "Unlocked" 상태에서 빠져 나온다. 이론적으론 미흡하지만 현실적으로 가능한 방법으로, PRF(Pseudo Random Function) 앙상블을 지원한다면, ID 비트 노출 방지가 가능하지만 구현상 PRF

앙상블을 대칭키 암호화보다 아주 적은 자원으로 가능한가에 대한 문제가 발생한다.

2.4 해쉬기반 아이디 변형 프로토콜

S. Weis의 해쉬락 프로토콜과 유사하게 Muller의 해쉬기반 ID 변형 프로토콜의 작동방법을 그림 3에서 보여준다. 해쉬기반 ID 변형 프로토콜은 해쉬에 기반하여 ID를 갱신하고, 도청, 스푸핑, 재공격, 수정과 같은 방법으로 읽기를 시도할 때마다 태그의 ID를 변경하므로 사용자 데이터 프라이버시와 위치 트래킹 공격을 방지하여 위치 프라이버시를 지원한다. 그러나 인증이 완료될 경우 ID가 갱신되므로 위치트래킹에 안전하지만 비정상적인 인증 때는 태그는 항상 동일한 h(ID)로 응답하므로 위치 트래킹이 가능하며 스푸핑 공격에도 안전하지 못하다[10]. 그러나 장점으로는 후위(Back-end)에서 접근 제어 구조를 현재의 요구에 맞게 쉽게 변형할 수 있으며, 그 구조는 간단하다. 따라서 다른 응용의 제약 없이 쉽고 간단하게 위치 프라이버시 증진이 가능하다. 이 프로토콜의 단점은 스푸핑을 당할 수 있고, 태그에서 계산하는 계산량이 많으며, 후위 시스템에서 트래킹이 가능하다.

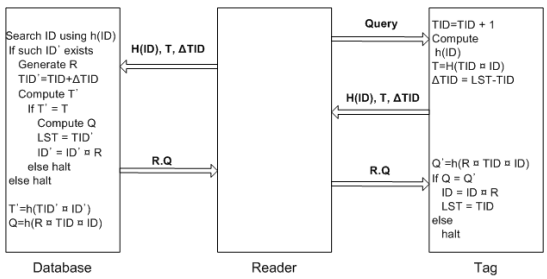

그림 3. 해쉬기반 ID 변형 프로토콜
Figure 3. Hash-Based ID Variation Protocol

2.5 해쉬체인 프로토콜

Okubo등에 의해 제안된 프로토콜로 두 개의 해쉬체인 함수를 이용하여 리더의 질의(Query)에 대해 태그가 매 세션마다 서로 다른 응답을 전송하고 인증하는 방법으로, 그림 4는 해쉬체인 프로토콜이다[2].

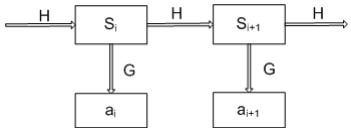

그림 4. 해쉬체인 프로토콜
Figure 4. Hash-Chain Protocol

해쉬 체인 프로토콜은 위치트래킹 공격에 안전하며, 태그 S_i 값에 대해 단방향 해쉬함수를 이용하여 도청이나 물리적인 공격으로 a_i 값을 알아도 다음 해쉬 결과 값인 S_{i+1} 값을 알아내는 것이 불가능한 전방위 보안성(Forward Security)을 지원한다. 태그별로 n 번의 해쉬연산을 수행하기 때문에 태그 수가 많아지고 해쉬 연산이 많아짐에 따라 후위에서 태그 판별 시간이 급격하게 길어지며 계산 복잡도는 $O(mn)$ 이다. 또 후위 시스템의 데이터베이스에는 태그의 실제 ID 값들이 저장되어 트래킹이 가능하며, 태그로부터 잘못된 값을 전달 받으면 후위 시스템의 데이터베이스가 갖는 모든 ID에 대해 해쉬를 수행할 수 있는 단점을 갖는다.

III. 제안 프로토콜

본 논문에서 제안하는 프로토콜은 보안이 안전하지 못한(Insecure)부분이고 적은 자원을 가진 태그에서 계산을 많이 하지 않고, 보안(Secure)이 안전하고 많은 자원을 가진 부분에서 계산을 하는 프로토콜로 리더에서 태그로 보내는 기본 값을 그레이 코드를 이용하여 변형하고, 변형된 값을 리더에서 생성한 토큰(Token) 값과 태그에서 변형하여 생성한 값을 후위 시스템에 전달한다. 전달한 값을 역으로 계산하여 실제 태그에서 계산한 값이 맞는지를 계산한다. 계산된 값이 틀리면 태그로부터 다른 정보를 전송받고 전송된 값이 맞으면, 계산된 값으로 실제 필요한 정보를 획득하는 프로토콜이다[7].

기존 해쉬 프로토콜들과 비교하면 그레이 코드를 이용하는 제안 프로토콜은 해쉬를 이용하는 프로토콜보다 복잡하지 않고 간편한 장점을 갖는다. 또 태그의 계산능력이 작은 수동형 태그를 감안하면 태그에서 많은 계산과 저장능력의 한계를 극복하는 시스템으로 바코드를 대신하여 사용이 가능하다. 제안한 프로토콜은 복잡하지 않는 그레이코드를 이용하기에 실제 구현이 어렵지 않고 사용자 프라이버시, 상호인증, 통신내용분석, 스푸핑과 위치 트래킹등을 지원한다.

제안 RFID 프로토콜은 그레이 코드를 이용하여 RFID 시스템에서 발생할 수 있는 공격으로부터 안전한 프로토콜이다. 제안한 프로토콜에서 태그와 리더간의 메시지 도청을 통한 도청 메시지 내용을 분석할 수 없으며, 또 태그는 리더의 질의에 대해 매번 다른 내용의 메시지로 응답하므로 공격자는 위치 트래킹을 할 수 없다. 정당하지 않는 개체를 속여 인증과정을 통과하는 위장(Spoofing)을 하였더라도 후위시스템의 랜덤 값과 그레이코드를 이용하여 변환한 값을 xor를 이용하므로 인가된 사용자의 정당한 정보획득을 공격자가 갖지 못한다.

3.1 제안 시스템의 구조

시스템의 구조는 태그와 리더 그리고 후위 시스템으로 구성된다. 제안한 프로토콜은 그림 5와 같이 후위시스템에서 그레이코드로 암호화한 랜덤 값을 리더를 통해 태그로 보낸다. 이때 악의적인 도청자는 후위시스템에서 그레이코드로 암호화한 난수 값만을 받게 되기 때문에 유용하지 못한 정보만 받는다. 태그는 리더로부터 전달받은 그레이코드로 암호화한 난수 값을 받고, 태그 자체가 가지고 있는 태그_아이디(T_ID)를 그레이코드로 암호화하고, 태그 아이디를 오른쪽 이동(Shift)한 값과 태그에 존재하는 카운터 값을 증가하여 이 모든 일련의 값 모두를 xor 하여 실제 아이디 값을 생성한다. 이렇게 생성된 값으로 인해 실제 태그 값과 그레이코드로 변형한 값을 알 수 없으며, 실제 태그에서 생성한 값을 리더를 통해 후위시스템으로 보내어 보내진 값들에 대한 정보계산의 많은 부분을 후위시스템에서 하도록 구성하고 있다. 이와 같이 암호화한 값과 완전한 정보를 중간에 가로채기 공격으로 악의적으로 획득하여도 암호화한 정보나 완전치 못한 정보를 획득하였기 때문에 공격자는 실제의 완전한 정보를 알 수 가 없다.

보내진 값들을 정확하게 해석하려면 태그아이디와 리더로부터 제공받은 그레이코드로 암호화한 난수 값을 알아야만하고, 태그에서 전달하는 태그아이디를 오른쪽으로 이동한 값을 알아야만 가능하기 때문에 사용자의 프라이버시를 제공할 수 있으며, 후위시스템에서 계속적으로 난수 값이 변화하고 변화된 난수 값을 그레이코드로 암호화하여 전달하기 때문에 트래킹도 불가능하다. 만약 난수 값만을 보내거나 순차적인 증분을 거친 값을 보내어도 크게 상관은 없으나 순차적 증분은 도청이나 스푸핑으로 보내지는 값을 추론할 수 있다면, 이러한 행위를 하지 못하게 하는 난수 값을 생성하여 그레이코드로 암호화하여 보내는 값은 매우 유용하다.

그림 5는 전반적인 제안 시스템의 프로토콜 구조를 순차 다이어그램으로 표현하였다.

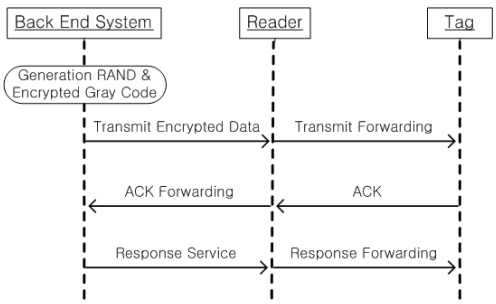

그림 5. 전반적인 프로토콜 순차 다이어그램
Figure 5. Overview Protocol Sequence Diagram

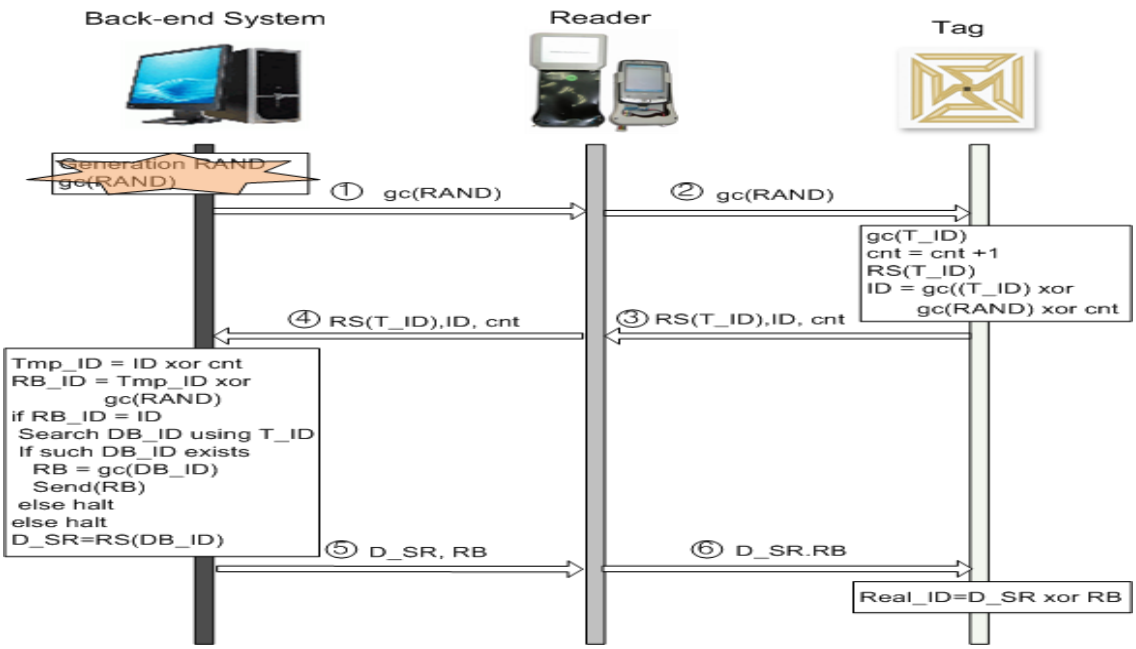

그림 6. 그레이코드를 이용한 제안 RFID 프로토콜
Figure 6. Propose RFID Protocol using Gray Code

3.2 제안 프로토콜 인증과정

제안 프로토콜의 인증과정을 그림 6과 같이 나타내었다. 우선 인증과정의 ①과 같이 후위시스템에서 난수 값을 생성하고 이 값을 그레이코드로 암호화한다. 암호화한 값을 ②와 같이 리더를 통해 태그로 전달하고 태그에 있는 태그아이디를 그레이 코드로 암호화하고 카운터를 증가한다. 그리고 전달받은 그레이코드로 암호화한 난수 값과 카운터 그리고 그레이코드로 암호화한 태그 아이디 값 모두를 xor 을 통해 아이디로 암호화하며, 태그아이디를 오른쪽 이동하여 값을 생성하고 이렇게 암호화 한 값과 오른쪽 이동하여 생성한 태그 아이디 값을 ③④ 과 같이 리더를 통해 후위 시스템에 전달한다. 전달하는 값들은 오른쪽 이동한 태그 아이디 값과 xor 을 통해 암호화한 값 그리고 카운터이다.

후위시스템은 리더를 통해 전달 받은 아이디와 카운터 그리고 오른쪽 이동한 태그 아이디 값을 가지고 계산을 수행한다. 임시 아이디에 리더를 통해 전달 받은 아이디와 카운터를 xor을 수행하여 저장하고, 이 값을 그레이코드로 암호화한 난수 값과 xor을 수행하여 비교인증 아이디(CA_ID) 값을 생성한다. 생성된 비교인증 아이디 값과 리더를 통해 전달되어진 아이디 값을 비교하여 그 값이 틀리면, 후위시스템에서 그레이코드로 난수 값을 암호화한 값이 제대로 태그에 전달되지 않았거나 태그에 존재하는 태그아이디의 값, 그레이코드로 암호화한 태그 아이디 값 혹은 xor을 이용하여 암호화한 아이디 값들이 맞지 않기에 다시 후위시스템에서 난수 값을 생성하여 그레이코드로 암호화한 후 리더를 통해 태그로 재전송을 한다. 그러나 후위시스템에서 생성한 비교인증 아이디 값과 태그에서 xor을 이용하여 생성한 아이디 값이 같으면, 후위시스템에서 그레이코드로 암호화한 값과 이 값을 태그에서 이용하여 재 암호화한 값 모두가 맞는 값이기에 후위시스템에서 계속하여 계산 및 실제 아이디에 맞는 정보처리 절차를 수행을 한다.

태그아이디를 이용하여 데이터베이스에서 사용할 수 있는 데이터베이스 아이디를 검색하여 데이터베이스 아이디가 존재하지 않으면 후위시스템에서 존재하지 않는 정보를 갖고 있기 때문에 전체 시스템을 정지하고 처음부터 새로운 난수를 생성하여 그레이코드로 암호화하고 리더를 통해 태그로 전송하는 절차를 다시 수행한다. 그러나 데이터베이스 아이디가 존재하면, 데이터베이스 아이디를 그레이코드로 암호화하여 복귀값(RB)으로 저장하고 이 값을 리더를 통해 태그로 보낸다. 그리고 데이터베이스 아이디 값을 오른쪽이동을 하여 이동된 목적 값(D-SR)로 저장하고 이 값도 리더를 통해 태그로 전송한다, 태그는 리더를 통해 후위 시스템에서 전송된 복귀 값(RB)와 이동된 목적 값(D_SR)을 xor 연산을 통해 실제 필요한 값(Real_ID)을 추출하는 연산과정을 수행한다. 표 1은 이와 같은 일련의 연산과정에 대한 알고리즘을 나타낸 것으로 리더와 후위시스템에서 이루어지는 모든 과정이다.

표1. 알고리즘
Table 1. Algorithm

```
// Back-End System_Oriented
1. Generation RAND   // 난수값 생성
2. gc(RAND)    // 그레이코드로 난수값을 암호화

// Tag_Oriented
3. gc(ID)
4. cnt = cnt + 1
5. RD(T_ID)  // 오른쪽이동(T_ID)
6. ID = gc(T_ID) xor gc(RAND) xor cnt

7. TO Back-End System Transfer
   RS(T_ID), ID, cnt

// Back-End System_Oriented
8. Tmp_ID = ID xor cnt
9  CA_ID = Tmp_ID xor gc(RAND)
10 if CA_ID  <> ID
11   Search DB_ID using T_ID
12   if such DB_ID exists
13     RB = gc(DB_ID)
14     Send(RB)
15   else
16     halt
   else
     halt
17 D_SR = RS(DB_ID)
18 Send(D_SR)

19 TO Tag Transfer
   RB, D_SR

// Tag_Oriented
19. Real_ID = D_SR xor RB
```

Ⅳ. 성능평가

기존 RFID 보안 프로토콜과 그레이코드를 이용한 제안 프로토콜간의 사용자 프라이버시, 상호인증, 통신내용분석, 스푸핑과 위치 트래킹등과 같은 항목을 비교 평가 하였으며, 제안 시스템의 보안 안전성에 대한 평가와 성능 분석을 하였다.

4.1 제안 시스템의 안전성(Safety)

RFID 시스템은 RF을 이용하기 때문에 많은 위협을 가지고 있다. 이러한 위협은 도청, 도청분석, 위치 트래킹, 사용자 프라이버시, 스푸핑 , 그리고 메시지 유실과 같은 부분에 안전하지 못하다. 그러나 제안 시스템은 태그의 계산용량을 현저하게 줄였을 뿐만 아니라 위에 지적한 단점을 극복한 효율적인 시스템으로, 기존의 해쉬함수를 이용한 보안 프로토콜의 갖는 장점을 수용하면서 프로토콜의 복잡도도 줄였다.

① 사용자 프라이버시(User Privacy)

후위시스템에서 토큰인 난수를 발생하여 이 값을 그레이코드를 이용하여 암호화하여 리더를 통해 태그에게 전달하고 태그는 이 값과 자신이 갖는 카운터와 xor 을 통해 암호호한 값을 리더를 통해 후위 시스템에 전달하면 전달 받은 받은 값과 후위 시스템에서 재계산하여 계산한 값과 비교를 하여 후위시스템에서 전달한 값이 맞는지 검증한다. 맞으면 일련의 검색 알고리즘을 통해 실제 데이터베이스의 실제 값을 다시 태그로 전송하지 않고 검색된 값을 다시 그레이 코드를 이용하여 변환한 후 리더를 통해 태그로 전송한다. 따라서 공격자의 공격에 의해 값들이 노출되더라도 실제 전송된 값이 무엇을 의미하는지 알 수 없다. 이러한 일련의 과정을 통해 상품의 실제 정보가 알려지지 않기 때문에 상품의 정보나 구매자의 상품 내역을 알 수 없으며, 개인의 정보가 유출되지 않기 때문에 사용자 프라이버시를 지킬 수 있다

② 상호인증(Cross Certificate)

후위시스템엣 그레이코드를 이용하여 생성한 토큰인 난수 값을 태그에게 전달하면, 태그는 이 값과 자신의 고유한 값 모두를 그레이코드와 xor 을 이용하여 계산하여 다시 후위 시스템으로 전달한다. 이렇게 전달한 값들을 후위 시스템에서 태그로부터 그레이 코드로 변환된 값과 비교하여 같은 태그로부터 전달 받은 것을 검증하여 상호 인증을 한다.

③ 도청(Eavesdrop)

후위시스템에서 토큰인 그레이코드로 암호화한 난수 값을 리더와 태그로 전달할 때 도청을 하고 태그에서 실제 암호화한 값 모두를 도청하더라도 이 값의 실제의미를 알 수가 없으며, 조합을 통해서도 풀 수가 없다. 근본인 난수 값을 그레이코드로 암호화하여 전달하기 때문에 해독을 할 수가 없기 때문이다. 따라서 전송되는 모든 값을 도청을 통해 알아내더라도 그레이코드로 변환된 실제의 값을 파악하지 못하기 때문에 실제 내용을 파악하는 것이 불가능하다.

④ 통신내용 분석(Content Analysis)

후위시스템과 리더 그리고 리더와 태그간의 통신 내용 값을 분석하려면, 실제 그레이 코드를 이용하여 변환된 값의 의미를 알거나 변환하기전의 실제 값을 추론할 수 있어야 한다. 그러나 후위시스템에서 생성한 토큰인 난수는 원래의 난수 값에 그레이코드를 이용하여 암호화한 값을 리더로 전달하고 리더에서 태그로 전달하기 때문에 공격자가 통신내용을 분석하더라도 실제의 값들이 뜻하는 의미를 파악하는 것은 불가능하다.

⑤ 재전송(Replay Transmit)

후위시스템에서 토큰을 생성하여 리더를 통해 태그로 전달할 때, 리더에서 태그로 재전송을 요구하면, 태그는 자신의 암호화를 통해 계산된 값을 리더로 재전송한다. 그러나 태그에서는 카운터가 있어 리더에서 재전송을 요구할 때 마다 카운터의 값이 증분하기 때문에 실제 재전송되는 값들은 매번 다른 계산된 값이 보내진다. 그리고 리더에서 후위시스템에게 재전송을 요구할 경우도 마찬가지고 후위시스템에서 생성된 난수가 매번 다른 값을 생성하여 리더로 보내고 이 값이 태그로 전달된다. 따라서 후위시스템과 리더의 재전송 공격에도 매번 다른 값이 전달되고, 리더와 태그간의 재전송 공격에도 매번 다른 값이 계속하여 생성되어 전달되기 때문에 재전송 공격에 안전하다.

⑥ 스푸핑(Spoofing)

공격자가 리더를 속이기 위해 태그로 가장하여 정보를 요구를 하더라도 요구된 정보를 이용하여 실제 값을 추출할 수 없다. 후위 시스템에서 계속적인 난수 값을 생성하고 생성된 값을 그레이코드를 이용하여 암호화를 통하여 전달하기 때문에 리더를 통해 태그에서 생성한 값이 리더를 통해 다시 후위 시스템에 전달되더라도 계산을 통해 생성되는 난수 값이 아니고 실제 후위 시스템에서 발생시킨 토큰인 난수 값이므로 스푸핑을 통해서 값들을 알아낼 수가 없다.

실제 태그에서는 후위시스템에서 발생한 토큰을 이용하여 태그 자신의 아이디와 카운터를 조합하여 자신이 가지고 있는 정보를 후위시스템에서 재차 확인 작업을 거친 후 옳게 검증이 되면 실제 정보를 추출하는 작업을 통하게 시스템이 구성되어 있다. 따라서 리더로 가장하여 후위시스템의 정보와 태그에서 생성된 모든 정보를 획득하더라도 후위시스템에서 생성한 난수값을 알지 못하면 후위 시스템에서 계산된 결과 값과 태그에서 리더로 전달되어 후위 시스템으로 전달된 값이 다르기 때문에 시스템은 정지되며, 스푸핑을 통해서 태그와 데이터베이스에 저장된 값을 알아내는 것은 불가능하다. 따라서 스푸핑을 이용하여 유용한 정보를 획득하는 것은 불가능하다.

⑦ 트래킹(Tracking)

태그가 계속적으로 리더에게 동일한 값을 전달한다면, 태그의 위치를 쉽게 파악하며, 상품의 이동경로를 쉽게 파악할 수 있다. 그러나 태그가 리더의 요청마다 다른 값으로 정보를 보내면, 공격자들은 같은 태그에서 정보를 보내는 것을 판별하기 힘들며, 위치 트래킹을 하기 어렵다. 제안 프로토콜 시스템의 후위시스템과 리더간의 통신에서 요청마다 계속적인 변화된 값을 주고 또 태그와 리더간의 통신에서도 리더에서

같은 태그에 변화된 값을 전송하게 되므로 요청 시 하나의 값을 전달하여 파악할 수 있는 상황이 이루어 지지 않는다. 따라서 한 태그가 계속적으로 같은 정보를 보내는 것이 아니고 태그에서 카운터 값이 증분되어 계속적으로 다른 정보 값을 반송하기 때문에 트래킹에 안전하다.

⑧ 추적 가능성(Traceability)

태그의 아이디는 태그에 존재하지만 실제 그레이코드로 암호화한 태그 아이디를 후위 시스템에 전송하려면 후위 시스템에서 발생시킨 토큰인 난수를 그레이 코드로 암호화한 이후 이 값과 태그에 있는 카운터의 값 모두를 xor 연산을 통하여 후위 시스템에 전송한다. 따라서 도청, 스푸핑등의 공격으로 획득하였다 하더라도 후위시스템에서 검증을 단계를 수행하기 때문에 실제 값들을 알 수 없지만 인가된 후위시스템 관리자는 실제의 정보의 흐름을 모두 알 수 있으며, 필요한 경우 추적을 통해 관리를 할 수 있다. 이러한 관리 기능이 추적가능성이다.

안전성 항목의 사용자프라이버시, 상호인증, 도청, 통신내용분석, 재전송, 스푸핑, 트래킹, 추적가능성에 대한 부분을 해쉬함수를 이용하는 기존 프로토콜과 제안 프로토콜간의 비교는 표 2와 같다.

표 2. 기존 프로토콜과 제안 프로토콜의 안전성항목 비교
Table 2. Safety factor of Compare to Preexistence Protocol and Propose Protocol

	해시락 프로토콜	확장된 해시락	해시체인 프로토콜	제안 프로토콜
사용자프라이버시	X	X	O	O
상호인증	O	O	O	O
도청	X	O	O	O
통신내용분석	O	O	O	O
재전송	X	O	O	O
스푸핑	X	X	O	O
트래킹	X	O	O	O
추적가능성	X	-	-	O

4.2 프로토콜간의 성능비교

태그와 리더간의 성능분석을 통하여 어느 보안 프로토콜이 가장 우수한지 평가하였다. 실험 성능 분석은 표 3과 같이 계산요소에 따른 계산 오버헤드와 저장요소에 따른 저장 오버헤드 그리고 상호인증을 위한 통신오버헤드로 구분하여 평가하였다.

표3. 제안 프로토콜과 기존 프로토콜간의 성능비교
Table 3. Performance Compare to Preexistence Protocol and Propose Protocol

기능	구분	개수				
		해쉬락	확장된 해쉬락	해쉬기반 ID변형	해쉬 체인	제안 프로토콜
태그메모리		256	128	192	128	128

DB 메모리		384	128	448	256	256
메세지크기		128	144	288	128	128
해쉬함수 갯수	T	1	1	1	2	gc(2)
	R		1		-	-
	BS			2	-	gc(2)
난수생성기	T		1		-	-
	R				-	-
	BS				-	1
XOR 연산	T		1	4	-	3
	R				-	-
	BS		1	3	-	2
|| 연산	T				-	-
	R		1		-	-
	BS				-	-
인증스텝수		6	5	5	5	6

태그 : T 리더 : R
후위 시스템 : BS gc : Gray Code 암호화

계산 오버헤드를 계산하기 위한 프로토콜별 인증 스텝수를 보면, 해쉬락은 6번의 인증단계를 수행해야만 한 번의 인증이 완성되며, 확장된 해쉬락은 5번의 인증 단계를 거쳐야만 한 번의 인증이 완성되고 제안된 프로토콜은 6번의 인증 단계를 수행해야만 한 번의 완성된 인증이 수행된다. 그러나 해쉬함수 구현하기 위해 사용한 MD5는 라운딩을 5번 수행해야만 한 번의 완성된 해쉬함수가 구현되므로 해쉬함수 사용은 xor 연산을 5번수행한 것으로 계산하였다. 따라서 확장된 해쉬락과 해쉬기반 ID 변형 프로토콜과 제안 프로토콜의 계산 오버헤드를 보면, 확장된 해쉬락 프로토콜은 해쉬함수를 태그와 리더에서 사용했으므로 XOR 계산을 10번 수행하였고, 난수발생기 한번과 XOR 연산 2번 그리고 연접(||)연산 1번을 수행하였기 때문에 모두 14번의 인증스텝을 수행해야만 하나의 태그를 인증하고, 해쉬기번 ID 변형 프로토콜은 22번의 인증스텝을 거쳐야 하며, 제안 프로토콜은 10번의 인증 스텝을 거쳐야 하나의 태그를 완전하게 인증단계를 수행한다. 그림 7은 태그 수에 따른 인증 계산수를 보여준다.

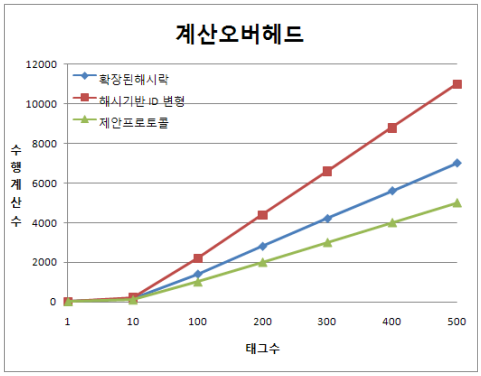

그림 7. 태그에 따른 계산오버헤드
Figure 7. Tags Computation Overhead

V. 결론

RFID 기술은 자동인식 및 데이터 획득의 근본 기술이며, 바코드보다 빠르고 많은 정보를 저장할 수 있어 바코드를 대체하여 사용되고 있다. 그러나 태그와 리더간의 RF를 이용하기 때문에 불법적인 정보획득이 가능하며, 획득한 정보를 이용하여 위치추적이나 개인 프라이버시 침해가 가능하다.

제안 프로토콜 시스템은 자체 전원을 가지고 많은 자원을 활용하며 많은 계산을 할 수 있는 액티브 태그보다는 태그의 계산능력과 한정된 자원 및 자체 전원을 갖지 못하는 수동형 태그에 적합하다.

본 논문은 태그에서 리더로 전송되는 정보를 태그와 후위 시스템에서 그레이 코드를 이용하여 쉽고 안전하게 전달할 수 있는 시스템으로 안전성의 항목들인 사용자 프라이버시, 도청, 상호인증, 위장공격, 스푸핑, 통신내용분석, 트래킹등에 안전한 보안 프로토콜을 제안하였다.

기존에 해쉬를 이용한 보안 프로토콜에 비해 태그에서 계산능력을 줄임에도 불구하고 안정성이 향상된 보안 프로토콜로 태그의 부하를 줄임으로 바코드를 대신하는 수동형 태그에 안정적인 RFID 보안 인증 프로토콜 시스템에 쉽게 적용 가능하다.

참고문헌

〔1〕 Sarma, S. et al., "RFID Systems and Security and Privacy Implications, Workshop on Cryptographic Hardware and Embedded Systems," pages 454-470, Lecture Notes in Computer Society, pp. 149 - 153. Computer Science, 2002

〔2〕 Weis, S. et al., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," First Intern. Conference on Security in Pervasive Computing (SPC), 2003

〔3〕 Kabatianski, Smeets, Johansson, "On the cardinality of systematic authentification codes via error correcting codes." In IEEE Trans on Info TheoryIT42, pp. 566-578, 1996.

〔4〕 Moshe Schwartz and Tuvi Etzion, "The Structure of Single-Track Gray Codes," IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 45, NO. 7, Nov. 1999.

〔5〕 Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," 1st International Conference on Security in Pervasive

〔6〕 남용택, 장종수, 손승원, "유비쿼터스 환경에서의 개인정보보호기술," 전자통신동향분석, 제 20권 제1호 2005년 2월

〔7〕 오기욱, "*그레이코드를 이용한 RFID 보안 프로토콜과 시스템 설계*," 숭실대학교 박사학위논문, 2007년

〔8〕 B. J. Feder, "Delta to Invest in radio Tags for Luggage at Airports," The New York Times, July 1, 2004. packages, CNET, 2003

〔9〕 Blum, A., Kalai, A., and Wasserman, H. "Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model." Journal of the ACM 50, 4, pp 506-519, July 2003.

〔10〕 Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A., and Szydlo, M., "Security Analysis of a Cryptographically-Enabled RFID Device." In USENIX Security (2005).

〔11〕 Yagni_Home, *http://yagni.com/graycode/index.html*

〔12〕 강전일, 박주성, 양대헌, "RFID 시스템에서 프러이버시 보호기술," 정보보호학회지, 제 14권 제 6호, 2004년 12월.

저 자 소 개

오 기 욱

1993년: 숭실대학교 컴퓨터학과 공학석사

2007년: 숭실대학교 컴퓨터학과 공학박사

2008년: 강원관광대학 컴퓨터정보과 조교수

현재: 안양대학교 교양학부 조교수

박 미 옥

1993년: 숭실대학교 컴퓨터학과 공학석사

2004년: 숭실대학교 컴퓨터학과 공학박사

2005년~현재: 성결대학교 컴퓨터공학부 전임강사